Contents

1 Summary

A major breakthrough for the multiplication in extensions of finite fields is the algorithm of Chudnovsky and Chudnovsky (1988), by evaluation-interpolation on algebraic curves. Indeed its complexity is linear in the size of the extension.

$\rightarrow$ Our first contribution, Theorem A, generalizes the formulas providing the best known asymptotic bounds for the bilinear complexity of multiplication. It improves the state of the art, and also corrects gaps in several results in the litterature.

We then target the most important parameter, i.e. the choice of the curve. Indeed Cascudo, Cramer, Xing et Yang showed in 2012 that the following folklore "Conjecture Y" would enable to cut by half the bilinear complexity in extensions of small characteristic p :

For p prime and $t' = 2t$ even, does there exist a family of curves $(X_i)_i$ over the extension of degree $2t$ of $\mathbf{F}_p$, such that :

(i) the genera g_i tend to infinity, with consecutive ratios tending to one (density condition)

(ii) the family $(X_i)_i$ has an optimal ratio of points of degree one (bound of Drinfeld-Vladuts)

(iii) the curves descend over $\mathbf{F}_p$?

Firstly we give counterexamples in V.5.6 that invalidate a recent published proof of the conjecture. The issue is the field of definition of Shimura curves (that are moduli spaces of abelian varieties).

$\rightarrow$ Our second contribution, Theorem B, provides an explicit solution to the conjecture in the particular case ($p = 3$ and $2t = 6$). The construction, done in VI, consists in intertwinning towers of Shimura curves then to descend their field of definition. The same techniques also provide a new curve with a record number of points (VI.4).

Theorems A and B enable to cut down the best known asymptotic bounds in small characteristic, nearly by half (in Table I.2.2).

We finally optimize in VII the effective construction of algorithms on a given curve: firstly in small algebras, then in extensions of cryptographic size.

2 Acknowledgements

My first thanks go to my advisor Hugues Randriam, who had the goodwill to always leave his door open during these last four years. His insights enabled to overcome many issues, as a text search for his name in the thesis will easily account for. It has been a great pleasure to follow his intuition of 2013 that Shimura curves would soon bring effective results.

Which did happen: Jeroen Sijsling and John Voight have since developped tremendous tools for canonical models, quaternionic modular forms, Hecke operators, Fuchsian groups, and endomorphisms of hyperelliptic curves. Hence the exchanges with them during the last two years were decisive for this project.

Noam D. Elkies had finally the key role of launching this project in August 2015. He then gave the crucial ideas of intertwinning modular towers, and that triangle groups were friendly for descent.

On a more personal side, I am indebted to Gérard Cohen and Virgile Ducet for their constant goodwill and support.

It is then a pleasure to thank all the people that closely followed this work and demonstrated their interest.

Firstly, David Madore offered his contradiction and way of thinking during my regular presentations these last four years. Stéphane Ballet and Julia Pieltant encouraged me to contribute to their joint work, which proved to be very useful for what followed. Julia moreover suggested that the bounds of [CCXY] could be improved: along with encouragements of Gérard Memmi, this motivated the search for Theorem A. Bertrand Meyer shared his knowledge and advices during many discussions, and it was a pleasure to exchange with all the other participants of the workgroups Vaches and Bac (with a special mention to Jean-Pierre Flori and Jérôme Plût).

This wonderful opportunity of research would have never been possible without the renewed confidence and support of the people representing the Infres department, the Telecom ParisTech school and the ministry of finance.

More widely, being part of the welcoming family of Mathematics & Cryptography is a great satisfaction.

Indeed, the possibility to meet remote colleagues and to learn new topics without immediate purpose is the best possible incentive to carry on a research activity. This is firstly made possible by the top academic specialists

who dedicate semesters to learn, teach, expose and write on subjects which are not necessarily theirs. With a personal gratitude to: A. Arabia, J. Barge, P. Clark, J.-F. Dat, J. Duval, D. Harari, L. Illusie, B. Kahn, B. Klingler, Z. Mebkhout, J.S Milne and M. Romagny.

Closer to this work, the contributions of many other people were a central thread to this thesis: I. Cascudo & al., R. Rolland, M. Tukumuli & al., T. Hasegawa, P. Zimmermann & al., Cenk–Özbudak, L. Dembélé, F. Hess, W. Stein & all the other contributors to Sage and Magma.

This is why the constant travel and computational support of the national grant Manta and the team Grace was indispensable for this work. I am equally indebted to S. Mesnager, J. Stankiewicz, H. Chen, C. Ritzenthaler, E. Howe, P. Loidreau, M. Perret, E. Hallouin, D. Augot and P. Lebacque for organizing very enrichening meetings.

This community feeling has been especially vivid last July, when Alp Bassa and Peeter Beelen gifted Hugues Randriam and I with an extraordinary result on the descent of Drinfeld curves.

It was finally a great honor that busy people like Serge Vladuts and Chaoping Xing immediatly accepted the huge work to review this thesis, and that Irene Bouw, Jean-Marc Couveignes, David Kohel and Gérard Cohen happily decided to escape from their responsibilities and sacrifice their week-end to participate to the jury. It was especially a great emotion to learn that Emmanuel Hallouin and John Voight had thoroughly read the thesis project and made many corrections.

All this makes me eager to continue giving back to the community what I have received.

I am grateful to John Voight for having always believed in this project.

Chapter I

Summary and Main results

1 Introduction

1.1 Motivation: the bilinear complexity of multiplication in finite fields

Let K be a field and $\mathcal{A}$ a finite-dimensional (associative, commutative and unitary) K-algebra. The multiplication law in $\mathcal{A}$, $m_{\mathcal{A}}$, is seen as a K-bilinear map:

$$m_{\mathcal{A}} : \quad \begin{array}{c} \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A} \\ (X, Y) \longmapsto X \cdot Y \end{array} \tag{1.1}$$

Definition 1.1. Let n be an integer, a *(possibly asymmetric) multiplication algorithm of length n in $\mathcal{A}$* is the data of $2n$ linear forms $(\phi_i)_{i=1,\dots n}$, $(\phi'_i)_{i=1,\dots n}$ on $\mathcal{A}$, along with n elements $(w_1, \dots, w_n)$ of $\mathcal{A}$, such that $m_{\mathcal{A}}$ is equal to

$$m_{\mathcal{A}} : (x, y) \longmapsto \sum_{i=1}^{n} \phi_i(x) \cdot \phi'_i(y) \cdot w_i \ . \tag{1.2}$$

The algorithm is furthermore *symmetric* if and only if $\phi_i = \phi'_i$ for all i.

The *bilinear complexity* of the multiplication $m_{\mathcal{A}}$ in $\mathcal{A}$, denoted $\mu(\mathcal{A}/K)$, is the lowest integer n, such that there exists a (possibly asymmetric) multiplication algorithm of length n. The *symmetric bilinear complexity* $\mu^{\mathrm{sym}}(\mathcal{A}/K)$ is defined likewise.

Definition 1.2. Let q be a prime power and n a positive integer. Let $\mathbf{F}_{q^n}[y]/y^l$ be the polynomial algebra over $\mathbf{F}_{q^n}$ modulo y^l.

The symmetric bilinear complexity of multiplication in the algebra $\mathbf{F}_{q^n}[y]/y^l$ over $\mathbf{F}_q$ is denoted $\mu_q^{\mathrm{sym}}(n,l)$, and $\mu_q(n,l)$ stands for the bilinear complexity.

In particular,

$$\mu_q^{\mathrm{sym}}(n) = \mu_q^{\mathrm{sym}}(n,1)$$

is the *symmetric bilinear complexity of the multiplication in the extension of finite fields* $\mathbf{F}_{q^n}/\mathbf{F}_q$, and $\mu_q(n)$ stands for the bilinear complexity.

Definition 1.3. If q is a prime power, we let

$$m_q = \liminf_{n\to\infty} \frac{1}{n}\mu_q(n)$$
$$M_q = \limsup_{n\to\infty} \frac{1}{n}\mu_q(n)$$

and their symmetric counterparts m_q^{sym} and M_q^{sym} are defined likewise.

Other complexity measures are possible, especially over the field $\mathbf{F}_2$. For example, one could count both the bitwise additions and multiplications. Or even take into account the possibility to perform computer-elementary operations on groups of 32 or 64-bits.

1.2 The interpolation method of Chudnovsky and Chudnovsky

The interpolation method of [Ch^2] provides algorithms that have today's lowest known bilinear complexities for extensions of finite fields of degree approximately greater than 20.

In the symmetric framework, the construction can be summarized as follows. It will be formalized more precisely in §1.1. Suppose that we want to compute the multiplication in $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$. Start with an algebraic curve X over $\mathbf{F}_q$, equipped with a point Q of degree m, and convenient divisors D and G. For instance, let G be a collection of points of degree one $P_1 \dots P_n$.

Assuming the injectivity and surjectivity of the maps as represented in the diagram below, the multiplication of any x and y in $\mathbf{F}_{q^m}$ can be performed with the following five steps:

① *lift* x and y to some functions f_x and f_y, in the space of global sections $L(D)$, so that $f_x(Q) = x$ and $f_y(Q) = y$.

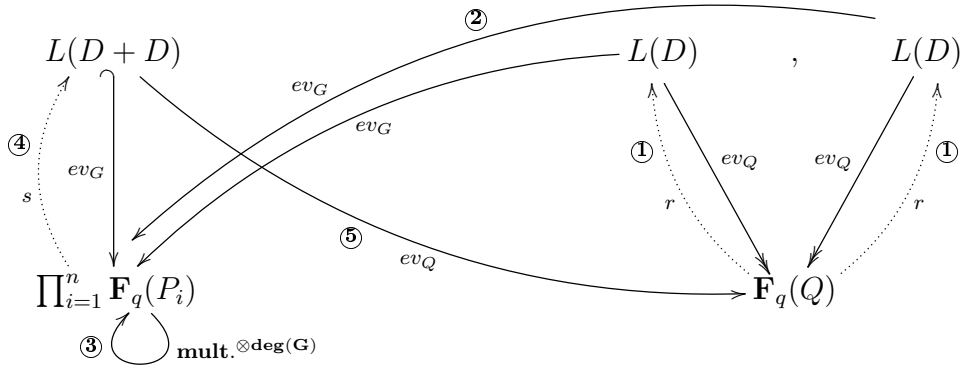
② *evaluate* f_x and f_y, separately, on each point P_i of the divisor G.

③ *compute*, for each P_i, the product of the two evaluations : $a_i = f_x(P_i).f_y(P_i)$. This is the critical step : here we perform $\deg G$ two-variables multiplications. We obtain the vector of values $(a_1, \cdots, a_n)$.

④ *interpolate* this vector to the *unique* function $g \in L(D+D)$ having values a_i at the P_i;

⑤ *evaluate* g at Q to find the product of x and y.

(1.3)



2 Main results and further conjectures

2.1 Theorem A for asymptotic upper bounds

Since we are mainly interested by the upper-limit complexity M_q, it is necessary to use sufficiently many different curves so as to deal with the worst cases. So let us give a name to the following requirement, formalized in [STV, Claim p163]:

Definition 2.1. Let X_s/k be a family of curves over a field k with genera g_s. We say that the family $(X_s)_s$ is *dense* iff the genera g_s tend to infinity and the ratio of two successive genera g_{s+1}/g_s tends to 1.

On the contrary, approaching the lower-limit m_q doesn't require dense families of curves (see II.3.3).

The asymptotic ratios β_r of the number of places of degree r divided by the genus, are quantities investigated in number fields (see [Leb] and [LZ] for

recent progress). Analogously, multiplication algorithms by interpolation on algebraic curves often require many points of higher degree $r \geq 2$. Hence the following definition for the best possible asymptotic ratio β_r.

Definition 2.2. Let $r \geq 1$ be an integer and q a prime power. For X a curve over $\mathbf{F}_q$, let $B_r(X)$ denote the number of closed points of degree r. Define $A_r(q)$ and $\widetilde{A}_r(q)$ as the sup of real numbers β_r and $\widetilde{\beta}_r$ such that there exists a family (respectively a *dense* family) of curves X_s over $\mathbf{F}_q$, of genera g_s going to infinity, that satisfies:

$$\lim_{s\to\infty} \frac{B_r(X_s)}{g_s} = \beta_r \text{ (respectively } \widetilde{\beta}_r)$$

Example 2.3. To start with, $A_1(q) = A(q)$ is the Ihara constant. See table II.2.2 and Theorem II.2.5 for recent results for non-square values of q.

More generally, Cascudo–Cramer–Xing–Yang showed that the generalized bound of Drinfeld–Vladuts implies the majoration (see Theorem 2.1):

$$\widetilde{A}_r(q) \leq A_r(q) \leq \frac{\sqrt{q^r} - 1}{r}$$

Examples 2.4. The towers of Garcia–Stichtenoth being actually defined over their prime field $\mathbf{F}_p$, they provide an example of towers reaching the previous bound (see II.2.2):

$$A_r(q) = \frac{\sqrt{q^r} - 1}{r} \text{ as long as } q^r \text{ is a square.} \tag{2.1}$$

For all the values of q that will be needed, Shimura curves provide dense families over finite fields $\mathbf{F}_q$ with many points in the quadratic extension $\mathbf{F}_{q^2}$: see II.2.3. The same holds for Drinfeld modular curves: see [Gek, 8-9] (and [Gek$_2$, Th. 2.16] for the supersingular argument needed when q is even). Their ratio matches the bound of Drinfeld–Vladuts over $\mathbf{F}_{q^2}$, which reads:

$$\widetilde{A}_1(q^2) = q - 1 \tag{2.2}$$

But actually one can say more. As will be re-stated in Corollary II.2.6, taking into consideration that the curves above are defined over $\mathbf{F}_q$ —and not only $\mathbf{F}_{q^2}$—, and by the consequence of the generalized bound of Drinfeld–Vladuts above, this implies :

$$\widetilde{A}_2(q) = \frac{q-1}{2} \tag{2.3}$$

Note that the dense families of classical modular curves over prime fields $\mathbf{F}_p$ are a particular case of Shimura curves.

Our following omnibus theorem generalizes essentially all the known formulas providing the current best upper-limit asymptotic bounds.

Theorem A. *Let q a prime power and $r \geq 1$, $l \geq 1$ be two positive integers. Then, as long as the respective denominators are positive, one has*

(a)
$$M_q \leq \frac{2\mu_q(r,l)}{rl}\left(1 + \frac{1}{rl\widetilde{A}_r(q) - 1}\right).$$

(a') *Moreover under any of the following two cases :*

(i) *$r = 1$ and q is such that $\widetilde{A}_1(q) > 5$;*

(ii) *let p be a prime number such that Conjecture Z holds for p. In addition one requires: $\{q = p$ and $r = 2\}$ or $\{q = p^2$ and $r = 1\}$;*

then the above bound is actually symmetric *:*
$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1 + \frac{1}{rl\widetilde{A}_r(q) - 1}\right).$$

(b)
$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1 + \frac{2}{rl\widetilde{A}_r(q) - 2}\right).$$

(c) *if $2|q$*
$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1 + \frac{1 + \log_q(2)}{rl\widetilde{A}_r(q) - 1 - \log_q(2)}\right).$$

(c') *if $2 \nmid q$*
$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1 + \frac{1 + 2\log_q(2)}{rl\widetilde{A}_r(q) - 1 - 2\log_q(2)}\right).$$

Remarks 2.5. In comparison to the known results :

- (c) and (c') allow from now on evaluation on points of odd degree r in Theorem 5.18 of [CCX$_2$]. All the arguments are actually available in the proof of the original theorem;
- (b) allows evaluation on points of arbitrary degree compared to [BCP, Proposition 11];
- finally, derived evaluations are now considered in all the results. These additional tools were actually known since [Ar], [CO$_1$] and [Ran$_1$].

2.2 Theorem B and dense families with many points of higher degree

A record curve with many points

The family of our main Theorem B below, arises from recursive towers of Shimura curves. Studying another tower, this time over the field $\mathbf{Q}(\sqrt{3})$ of narrow class number two, also leads to the good surprise described in §VI.4. Indeed the fourth step of this tower, of genus five, has a greater number of points in $\mathbf{F}_{5^4}$: **871** than the previous value of 868 recorded in the tables of manypoints.org[1]at the time it was found. As a bonus we obtained *explicit equations for the curve, that are furthermore defined over* $\mathbf{F}_5$.

Conjecture Y and its recent history

The following folklore conjecture asks for *dense families defined over their prime field, and matching the (optimal) Ihara constant for their number of points after a given even field extension.* It is stated as in [CCXY, Lemma IV.4], under a form essentially equivalent to the following:

Conjecture Y. *Let p be a prime number and $2t \geq 2$ an even integer*[2]*. Does this equality hold:*

$$\widetilde{A}_{2t}(p) = \frac{p^t - 1}{2t} \quad ? \tag{2.4}$$

[1] S.E. Fischer simultaneously submitted a record curve with an even simpler equation.

[2] Notice that the cases where $2t = 2$ are actually statisfied with classical modular curves : see [Mo] §5.6 for a demonstration. Whereas the cases for $2t = 6$ are dealt with the (new) theorem B below, and Conjecture X.

Equivalently (by Theorem 2.1): does there exist a family $(X_s/\mathbf{F}_{p^{2t}})_{s\geq 1}$ *of curves with genera* g_s *tending to infinity, such that:*

(i) X_s *is, actually,* defined over the prime field $\mathbf{F}_p$*;*

(ii) $g_{s+1}/g_s \xrightarrow[s\to\infty]{} 1$ *(*"density" *of* $(X_s)_s$*)*

(iii) $|X_s(\mathbf{F}_{p^{2t}})|/g_s \xrightarrow[s\to\infty]{} p^t - 1$ *(*Ihara constant over $\mathbf{F}_{p^{2t}}$*)* *?*

The first contributions towards the conjecture were to make Garcia–Stichtenoth towers more dense. It started with [Bal_2], then [BR] also dealt with the field of definition issue, and finally [BBR] proved a descent theorem. This last one uses the full power of Proposition A.1.2 (rediscovered by Randriam).

A previous attempt was [CCXY, Lemma IV.4], which proposes to solve it by using Shimura curves defined on the rationals. The problem is that the curves considered curves proposed do not necessarily descend over the rationals. This issue was first noticed by S. Ballet when he reviewed [CCXY], in a preliminary version. The paper was then accepted with another proof, and the result later used as a theorem, in: [CCX_2, Lemma 5.17] and [PR, Lemma 5.2].

Several people independently noticed that the final proof still contained the issue of Shimura curves that do not necessarily descend over the rationals. More nastily, *even canonical models with field of moduli equal to* $\mathbf{Q}$ *sometimes don't descend over* $\mathbf{Q}$. Three such counterexamples are described in §V.5.6. They were initially brought up in our joint work [BPRS, §3], out of the curves studied in [Sij_1]. In particular H. Randriam and J. Voight should be thanked for their contribution.

Anyway, the proposition of [CCXY] to use Shimura curves turned out to be the good idea. Indeed we could provide an explicit solution to the conjecture for the case ($p = 3$ and $2t = 6$), (and possibly $p = 5$): Theorem B in the next paragraph.

The conjecture has just been given an existential proof in early July 2017. Bassa–Beelen proved that Drinfeld modular curves modulo T over $\mathbf{F}_q$ with levels in $\mathbf{F}_p[T]$, descend to $\mathbf{F}_p$. From Gekeler's genus formulae, Randriam deduces the density of such curves (we further densified the families to match the growth rate of intertwinned towers of Shimura curves).

Our particular solution

Theorem B. *We have:*

$$\widetilde{A}_6(3) = \frac{3^3-1}{6}. \tag{2.5}$$

Said otherwise : there exists a family X_s of curves over $\mathbf{F}_3$ *with (increasing) genera g_s tending to infinity such that*

(i) $$\frac{g_{s+1}}{g_s} \xrightarrow[s\to\infty]{} 1 \text{ (density } \textit{condition}\text{)}$$

(ii) $$\frac{|X_s(\mathbf{F}_{3^6})|}{g_s} \xrightarrow[s\to\infty]{} 3^3-1 \text{ (optimal number of points of degree 6)}$$

We also explicit a solution in the case ($p = 5$ and $2t = 6$): intertwin the tower of equations VI.(6.10), with the reduction of the tower of Theorem VI of VI.6. But our verification of the next level did not terminate yet.

The key insight is due to N.D. Elkies, that one can *intertwin* two recursive modular towers into a dense family, see VI.5.3. A lookup in the table [Voi$_4$] of Shimura curves with small genera, filtered with the conditions on B, $\mathfrak{p}$ and $\mathfrak{N}$ from the Theorem V.5.4 brought up by V. Ducet's thesis, ends up with the following promising candidates.

Proof Consider the Riemann surfaces $X_0(\mathfrak{p}_2^i\mathfrak{p}_7^j)$ described in IV.2.5, where their genera are shown to be dense.

By the general theory (Theorem V.5.4), these curves have canonical models over the field $F = \mathbf{Q}(\cos(2\pi/3))$ that have good reduction modulo the inert (3). These reductions take place over $\mathbf{F}_{3^3}$ and have many points in the quadratic extension $\mathbf{F}_{3^6}$.

But to show that they descend over $\mathbf{F}_3$ requires to *construct explicitly these canonical models.*

The two towers $X_0(\mathfrak{p}_2^i)$ and $X_0(\mathfrak{p}_7^j)$ being recursive by §VI.3, *their determination relies essentially on the knowledge of the two canonical Belyi maps of genus one* $X_0(\mathfrak{p}_7^2) \to X_0(\mathfrak{p}_7)$ and $X_0(\mathfrak{p}_2^2) \to X_0(\mathfrak{p}_7)$ of degrees 7 and 8. Their monodromy are computed in Examples V.3.4 and 3.6. By the second statement of our Theorem V.5.14, these Belyi maps are characterized by their sole topological monodromy above $X(1)$. The previous arguments are given a detailed Leitfaden in VI.1.

The Belyi maps are computed in VI.5 and summarized in Theorem C of VI.6. The reduction of these covers are then *descended over* $\mathbf{F}_3$.

As a sanity check we could finally compute the next steps of each tower, $X_0(\mathfrak{p}_7^3)$ and $X_0(\mathfrak{p}_2^3)$, of genera five and seven. And compare their number of points in $\mathbf{F}_{3^3}$ and $\mathbf{F}_{3^6}$ —28; 1000 for $X_0(\mathfrak{p}_7^3)$ and 24; 1760 for $X_0(\mathfrak{p}_2^3)$—with those predicted from the traces of Hecke operators (Theorem V.5.5). □

Remark 2.6. the canonical model $X_0(\mathfrak{p}_2^i)$ of genus one has no rational point (cf. Remark VI.5.2). So we computed the cover over a quadratic extension $\mathbf{Q}(\sqrt{-7})$, where it acquires a rational ramification point. So, even if the reductions of our covers do descend to $\mathbf{F}_3$, they are only proven to be isomorphic to the canonical models *after a quadratic extension by* $\sqrt{-7}$. Fortunately, since we are interested by the number of points after a quadratic extension, this doesn't impeed the validity of the result.

Remark 2.7. chapter V takes a long time to prove the first statement of Theorem V.5.14, about descent of canonical covers over $\mathbf{Q}$. This general statement is not stricly necessary in the proof of Theorem B but gives very helpful hints for the computations of VI.5. It uses the general theory of descent of arithmetic covers, and builds on the results of Doi–Naganuma,

As a conclusion, for all primes different from $p = 2$ and 7, and inert in the field $\mathbf{Q}(\cos \pi/7)$ of the canonical models, the curves considered $X_0(\mathfrak{p}_2^i\mathfrak{p}_7^j)$ have also *potential good over* $\mathbf{F}_{p^3}$ and many points in $\mathbf{F}_{p^6}$. So of course, a general argument that would conclude for *good reduction* over any of these primes p (as we did explicitly for $p = 3$) would be highly welcome.

The remaining Conjectures X $\leq$ Y and Z

To deal with the remaining case $p = 2$, one needs another tower $X_0(\mathfrak{p}^k)$ over the same base $X_0(1)$ as in Theorem B, descends over $\mathbf{F}_2$. Indeed one could then intertwin this tower $X_0(\mathfrak{p}^k)_{\mathbf{F}_2}$ with the smooth tower $X_0(\mathfrak{p}_7^j)_{\mathbf{F}_2}$ found in Theorem B (see VI.(5.12)). And thus produce a dense family.

A good candidate is the tower $X_0(\mathfrak{p}_3^i)$, where $\mathfrak{p}_3$ is the prime (3). By the general theory it has a good reduction modulo the inert (2): $X_0(\mathfrak{p}_3^i)_{\mathbf{F}_{2^3}}$, that has many points in $\mathbf{F}_{2^6}$. But we don't know if this reduction descends to $\mathbf{F}_2$. By recursivity of the tower, this would be implied by the following conjecture.

Conjecture X. *Let B the quaternion algebra over the number field $F = \mathbf{Q}\big(\cos(2\pi/7)\big)$, which is ramified exactly at two of the three real places and no finite place. Let $\mathfrak{p}_3$ be the ideal above the inert prime (3), and $X_0(\mathfrak{p}_3^2)$ the Shimura curve over F defined by the group $\Gamma_0(\mathfrak{p}_3^2)$ of norm one units of the Eichler order of level $\mathfrak{p}_3^2$.*

Then the following morphisms descend to $\mathbf{F}_2$:

- *the canonical branched cover $X_0(\mathfrak{p}_3^2)_{\mathbf{F}_{2^3}} \to X_0(\mathfrak{p}_3)_{\mathbf{F}_{2^3}}$,*
- *and the Atkin–Lehner involution on $X_0(\mathfrak{p}_3^2)_{\mathbf{F}_{2^3}}$.*

Although this is part of an ongoing work, we describe the computations leading to the Atkin–Lehner quotient $X_0(\mathfrak{p}_3^2)^*$ of genus two in II.4. Indeed they illustrate the general theory and some recent algorithms.

The last conjecture, as proposed in [Ran_0, Conjecture A] plus the density condition, could close the gap between symmetric and asymmetric bounds for larger prime values of q, in the cases where modular curves are used (see Theorem A, case (a')(ii)).

Conjecture Z. *Let $p > 2$ be an odd prime. Does there exist a sequence of numbers $(N_s)_s$, with $N_{s+1}/N_s \xrightarrow[s\to\infty]{} 1$ (density condition), such that the Hecke operator $T_p(N_s)$ acting on the space of weight 2 cusp forms $S_2(\Gamma_0(N_s))$, has an odd determinant ?*

The following consequence was singled out in [Ran_0]. Let p be a prime, N a positive integer prime to p and $X_0(N)$ the classical modular curve over the rationals with the Hecke operator T_p acting on the space of weight 2 cusp forms $S_0(\Gamma_0(N))$. Then the congruence relation of Eichler–Shimura implies (see II.5 for a proof) :

$$|J_0(N)(\mathbf{F}_{p^2})| = \det(p^2 + 1 - T_p(N)^2) \tag{2.6}$$

In particular, considering the rational subgroup of 2-torsion points gives :

$$\dim J_0(N)(\mathbf{F}_{p^2})[2] \leq \mathrm{ord}_2\left(\det(p^2 + 1 - T_p(N)^2)\right)$$

where ord_2 is the 2-adic valuation. The prime p being odd, the left-hand side determinant has the same parity as $\det(T_p(N))$. Thus, the conjecture would have as a consequence the following weaker conjecture:

Conjecture 2.8. *Does there exist a dense family of curves* $(X_0(N_s)/\mathbf{F}_p)_s$ *such that:*

$$(J_0(N)(\mathbf{F}_{p^2}))\,[2] = \{0\} \text{ for all } N_s?$$

Remarks 2.9. Notice that our density condition says that $N_{s+1}/N_s \xrightarrow[s\to\infty]{} 1$, which *does not* imply that the set of numbers $\{N_s\}_s$ has a positive Dirichlet density (take $(N_s^2)_s$). The opposite implication is also false (introduce very sparse gaps in the harmonic series).

Removing this additional density requirement would only benefit to lower-limit symmetric bounds:

- for the values of q in table 2.3: the only effect of Conjecture Z would then be to close the gap between the symmetric and asymmetric bounds for $q = 25$. Indeed, in the three other cases where the asymmetric bounds are better than their symmetric counterparts, the families used are not modular curves.

- for larger values of q: Conjecture Z would only benefit to values for which the condition (a').(i) of Theorem A ($\widetilde{A}_1(q) > 5$) is not known to be satisfied. So only large primes q would be concerned, because interpolation on points of degree two of classical modular curves would be needed.

2.3 New bounds for bilinear multiplication

Symmetric multiplication in small binary algebras

The generalized interpolation method of Chudnovsky and Chudnovsky handles pointwise evaluations that live in small algebras (see the beginning of §1.1). It is thus useful to improve the bilinear algorithms in those algebras.

In Table 2.1 below are recapitulated the best known upper and lower bounds for the symmetric bilinear complexities $\mu_2^{\mathrm{sym}}(m,l)$ of the multiplication in the small $\mathbf{F}_2$-algebras $\mathbf{F}_{2^m}[x]/x^l$. Each pair of lower–upper bound is given as "L–U". When the upper bound U is in fact optimal (so L=U), then one single value is displayed.

The three new upper bounds are displayed in bold. Whereas the two new lower bounds (for $\mu_2^{\mathrm{sym}}(2,2)$ and $\mu_2^{\mathrm{sym}}(2,3)$, in addition to the exact value of $\mu_2^{\mathrm{sym}}(3,2)$) are just emphasized in Table II.3.1.

The values of the upper-bounds are justified in Table II.3.1 of II.3.1, and the new formulas in the annex A.2. The methods employed are described in §VII.2.

However most of the lower bounds are not given further justification. In particular the three new ones mentionned above arize from the exhaustivity of the search method described below Observation VII.2.2. The other unjustified lower bounds are merely deduced from the general [Ran_1, Lemma 1.9], or from the lower bound of a subalgebra.

Table 2.1: Lower–Upper bounds on the complexities $\mu_2^{\mathrm{sym}}(m,l)$

$l \backslash m$	1	2	3	4	5	6	7	8	9	10
1	1	3	6	9	13	15	$16-22$	$16-24$	$17-30$	$19-33$
2	3	9	**16**	$16-24$	.	.	.	.	.	.
3	5	15	$16-30$	.	.	.	.	.	.	.
4	8	$8-$ **21**	.	.	.	.	.	.	.	.
5	11	$11-$ **30**	.	.	.	.	.	.	.	.
6	14	.	.	.	.	.	.	.	.	.
7	$16-18$	.	.	.	.	.	.	.	.	.
8	$16-22$	.	.	.	.	.	.	.	.	.
9	$16-27$	.	.	.	.	.	.	.	.	.
10	$16-31$	.	.	.	.	.	.	.	.	.

Asymptotic upper-limit bounds in finite fields extensions

The values appearing in Table 2.2 below are justified in Table II.3.2. The first line accounts for the state of the art, the second one adding the contribution of Theorem A, the third one adds the new values of the $\widetilde{A}_r(q)$ allowed by Theorem B. The fourth and last one add gradually the values of the $\widetilde{A}_r(q)$ implied by Conjectures X and the more general Conjecture Y. Conversely, the line assuming Conjecture Z needs not assuming any of the previous new values (neither Theorem B nor the two previous conjectures)

Remark 2.10. Notice that we did not state some bounds appearing in the litterature in the lines "(Repaired) published bounds" part of table 2.2. The

Table 2.2: (new)-Upper bounds for M_q^{sym} and M_q

Results used \ q		2	3	4	5	7
(Repaired) Bounds	Sym	$15,2$ [BP_2]	$7,73$ [BP_2]	6.00	$5,61$	$4,20$
	Asym	8.59	$6,00$	$4,50$	$4,00$	$3,60$
Using Th. A and Tab. 2.1	Sym	**10,0**	**7,50**	**5,33**	**5,21**	**4,08**
	Asym	**7,00**	—	—	—	—
Adding Th. B	Sym	—	**5,42**	—	*4,74*	—
	Asym	—	**5,20**	—	—	—
Conj. X	Sym	7	—	4.24	—	—
	Asym	$5,83$	—	$3,89$	—	—
Conj. Y	Sym	$6,92$	$5,39$	—	$4,34$	3.63
	Asym	—	$5,14$	—	—	$3,57$
Conj. Z	Sym	—	—	—	*4,00*	$3,60$

Results used \ q		8	9	11	5^2
(Repaired) published bounds	Sym	3.71	3.77	3.56	3
	Asym	3,50	3,43	3,33	2,67
Using Th. A and Tab. 2.1	Sym	—	—	—	—
	Asym	—	—	—	—
Adding Th. B	Sym	—	**3.56**	—	—
	Asym	—	—	—	—
Conj. X	Sym	—	—	—	—
	Asym	—	—	—	—
Conj. Y	Sym	3.58	—	3.55	—
	Asym	—	—	—	—
Conj. Z	Sym	—	—	$3,33$	$2,67$

reason being that they actually cannot be considered as proven. They appear in [CCXY, Theorem IV.6, Theorem IV.7, Corollary IV.8], [CCX_2, Theorem 5.18, Corollary 5.19] and [PR, Theorem 5.3, Corollary 5.4, Corollary 5.5].

Indeed they rely on Conjecture Y, which would imply many values of $\widetilde{A}_r(q)$.

Nevertheless we have already tried to take into account the theoretical improvements made by these articles in the lines "published bounds", which explains the adjective "repaired". So we re-used as much as possible the proven statements in the aforementionned articles[3]. And applied these statements with the parameters allowed by[4] (2.2) and (2.3).

Remark 2.11. There seems to be room for immediate improvement of the bound $M_2^{\mathrm{sym}} \leq 10,0$. Indeed if the following conjectural upper-bound did hold : $\mu_2(2,6) \leq 39$ (instead of 42), then the criterion (b) of Theorem A applied to $(r,l) = (2,6)$ would imply $M_2 \leq 9,75$. Our reason to believe the above conjectural bound to be accessible, is the fact that it could be deduced from a conjectural $\mu_4(1,6) \leq 13$ (instead of 14), which is in the range of exhaustive-search methods. Moreover the value 14 is also an upper bound for the harder complexities $\mu_2(1,6)$ and $\mu_4(6,1)$. So the conjectural upper-bound seems credible.

Remark 2.12. The additional column for $q = 5^2$ emphasizes the record of longevity of the published symmetric bound (which still holds). Indeed, although it had never been stated numerically, the bound can be directly deduced from a formula of Ballet–Pieltant, which is based on an argument as old as 1999. This exception will be discussed in remark II.3.2.

Asymptotic lower-limit bounds in finite fields extensions

The following table gathers both (i) the best known upper bounds for the lower-limit symmetric complexities m_q^{sym}, for small values of q (see [CCX_2], V, table II), and (ii) in certain cases, proposes slightly better asymmetric counterparts (in bold)[5]:

[3] but without the additional generalities enabled by Theorem A in the cases the results were not stated as such

[4] Arising from the well-known dense families of Shimura curves recalled in II.2.3. Which include the classical modular curves over prime fields as a special case

[5] Use the towers of Theorem II.2.5 for $q = 27$ and $q = 32$, and Shimura curves for $q = 16$.

Table 2.3: (new)-Upper bounds for m_q and m_q^{sym}

q	2	3	4	5	8
m_q^{sym}	$5,834$	$5,143$	$3,889$	$3,903$	$3,500$
m_q	$5,834$	$5,143$	$3,889$	$3,903$	$3,500$
q	9	16	25	27	32
m_q^{sym}	$3,429$	$3,026$	$2,779$	$3,120$	$2,667$
m_q	$3,429$	$\mathbf{3,000}$	$\mathbf{2,667}$	$\mathbf{2,909}$	$\mathbf{2,625}$

The fact that the symmetric bounds are close to the asymmetric ones, is due to the versatility of the lower-limit measure (or, said otherwise, its low accuracy), that enables it to be computed on fewer (and more advantageous values) : see II.3.3. However there is still room for improvement :

Remark 2.13. Suppose that one could bring down to 17 (or 18) the upper bound for $\mu_2(7,1)$ (the bilinear complexity of multiplication in $\mathbf{F}_{2^7}$), which is so far known to be somewhere between 17 and 22. Then the upper bound for the asymmetric complexity m_2 would be brought down to $5,426$ (or, resp., $5,745$). This would follow from the use of the Bassa & al. [BBGS] tower over $\mathbf{F}_{2^7}$ (using the trick of Lemma II.3.4).

2.4 Effective aspects

Consider a fixed extension of finite fields with a small prime field, e.g. $\mathbf{F}_{2^m}/\mathbf{F}_2$ —with m not too small—and a fixed curve X of genus g. Then the equation (1.11) (in the §1.3 below) implies that there exists a multiplication algorithm by interpolation on the curve X, that uses $2m+2g+3$ interpolation points (with degrees and multiplicities).

In practice one can expect that fewer points are needed —and thus to get a smaller algorithm—for the same degree m. To start with, Proposition VII.3.4 states that one cannot expect an algorithm with fewer interpolation points than $2m+g-1$.

Then the search algorithm of Proposition VII.3.6 enables to construct such an optimal multiplication algorithm, whenever it exists.

And it does exist in practice, at least always on the examples that we dealt with. The following Table 2.4 compare the previous bounds of [BBT] for the

bilinear multiplication in the binary extensions of [NIST], with our bounds obtained with the classical modular curves. The data is a compression of Tables VII.4.1 and VII.4.1.

Table 2.4: New effective upper bounds in the NIST extensions $\mathbf{F}_{2^m}/\mathbf{F}_2$

m	163	233	283	409	571
before	906	1340	1668	2495	3566
after	**900**	**1335**	**1654**	**2486**	**3555**

As pointed in the final paragraph of VII.4.2, these computations date back from 2014. They could be improved today by using quotients of Atkin–Lehner and also one of our Shimura curves from Theorem B.

Chapter II

Proofs of Theorem A and numerical bounds, more on Conjectures X and Z

1 Proof of Theorem A

1.1 Reminder of the general multiplication algorithm

Framework

Let us formalize the objects involved in the description of §1.2. A *curve* X will always be assumed projective, smooth and geometrically irreducible over $\mathbf{F}_q$ (here often $\mathbf{F}_p$ with p prime). Given a divisor D on X, let $\mathcal{O}(D)$ be the sheaf of sections of D. Let $l(D)$ and $i(D)$ (the *index of specialty of* D) be the dimensions of the $\mathbf{F}_q$-vector spaces, of global sections $H^0(X, \mathcal{O}(D))$, and of $H^1(X, \mathcal{O}(D))$. So that the theorem of Riemann–Roch states itself as : $l(D) - i(D) = \deg D + 1 - g$, where g is the genus of X.

More particularly, given P a closed point of X of degree n, D a divisor and l a positive integer, we will need the following map : the *evaluation of a global section of the line bundle* $\mathcal{O}(D)$ *at the thickened point* $P^{[l]}$, which takes values in $\mathbf{F}_{q^n}[y]/y^l$. Let t_P be a local parameter at P : multiplication by $t_P^{v_P(D)}$ provides a local trivialization of $\mathcal{O}(D)$ at P, and thus an evaluation

map[1]:

$$\begin{aligned} ev_Q : L(D) &\longrightarrow \mathcal{O}_{X,P}/(t_P^l) \\ f &\longrightarrow t_P^{v_P(D)} f_P \bmod (t_P^l) \end{aligned} \tag{1.1}$$

The target space maps itself isomorphically to the $\mathbf{F}_q$-algebra $\mathbf{F}_{q^n}[y]/y^l$.

The general algorithm

The following theorem states sufficient conditions for the algorithm of §1.2 to hold, and draws the consequences on the symmetric bilinear complexity of multiplication in finite fields.

Theorem 1.1 ([Ran$_1$], Theorem 3.5)**.** *Let X be a curve of genus g over $\mathbf{F}_q$, and let $m, l \geq 1$ be two integers. Suppose that X admits a closed point Q of degree $\deg Q = m$. Let G be an effective divisor on X, and write*

$$G = u_1 P_1 + \cdots + u_n P_n$$

where the P_i are pairwise distinct closed points, of degree $\deg P_i = d_i$. Suppose that there exist two divisors D_1, D_2 on X such that:

(i) *The natural evaluation map*

$$L(D_1 + D_2) \longrightarrow \prod_{i=1}^{n} \mathcal{O}_X(D_1 + D_2)|_{P_i^{[u_i]}}$$

is injective.

(ii) *The natural evaluation maps*

$$L(D_1) \longrightarrow \mathcal{O}_X(D_1)|_{Q^{[l]}} \qquad L(D_2) \longrightarrow \mathcal{O}_X(D_2)|_{Q^{[l]}}$$

are surjective.

Then

$$\mu_q(m, l) \leq \sum_{i=1}^{n} \mu_q(d_i, u_i). \tag{1.2}$$

[1] This map was first built, at least for the purpose, in its full generality in [Ran$_1$, remarks 3.4-3.6]. We just corrected the signs of $t_P^{-v_P(D)}$ in the reference.

In fact we also have $\mu_q(m,l) \leq \mu(\prod_{i=1}^n \mathcal{A}_q(d_i,u_i)/\mathbf{F}_q)$. *Moreover, if* $D_1 = D_2$, *all these inequalities also hold for the symmetric bilinear complexity* μ^{sym}.

Sufficient numerical criteria for the hypotheses above to hold can be given as follows. A sufficient condition for the existence of Q *of degree* m *on* X *is that* $2g+1 \leq q^{(m-1)/2}(q^{1/2}-1)$, *while sufficient conditions for (i) and (ii) are:*

(i') *The divisor* $D_1 + D_2 - G$ *is zero-dimensional:*

$$l(D_1 + D_2 - G) = 0.$$

(ii') *The divisors* $D_1 - lQ$ *and* $D_2 - lQ$ *are non-special:*

$$i(D_1 - lQ) = i(D_2 - lQ) = 0.$$

More precisely, (i) and (i') are equivalent, while (ii') only implies (ii) a priori.

Interesting particular situations

The first corollary is straightforward :

Corollary 1.2 ([Ran$_1$, Proposition 5.1])**.** *Let* X *be a curve of genus* g *over* $\mathbf{F}_q$, *and let* $m \geq 1$ *an integer.*

Suppose that X *admits a closed point* Q *of degree* $\deg Q = m$ *(a sufficient condition for this is* $2g+1 \leq q^{(m-1)/2}(q^{1/2}-1)$*).*

Suppose also that X *admits a non-special divisor* S, *of degree* $g+e-1$, *for an integer* e *as small as possible (hence* $e \leq g$ *by the Riemann-Roch theorem).*

Consider now a collection of integers $n_{d,u} \geq 0$ *(for* $d,u \geq 1$*), such that almost all of them are zero, and that for any* d,

$$n_d = \sum_u n_{d,u} \leq B_d(X/\mathbf{F}_q).$$

Then, provided

$$\sum_{d,u} n_{d,u} du \geq 2m + 2e + 2g - 1$$

we have

$$\mu_q(m) \leq \sum_{d,u} n_{d,u} \mu_q(d,u)$$

and likewise

$$\mu_q^{sym}(m) \leq \sum_{d,u} n_{d,u} \mu_q^{sym}(d,u).$$

The next criterion is both sharper, and the proof actually provides an explicit construction of such a symmetric multiplication algorithm.

Theorem 1.3 ([Ran$_1$, Proposition 5.2 c)]). *Let X be a curve of genus g over $\mathbf{F}_q$, and let $m \geq 1$ an integer.*

Suppose that X admits a closed point Q of degree $\deg Q = m$ (a sufficient condition for this is $2g+1 \leq q^{(m-1)/2}(q^{1/2}-1)$).

Consider now a collection of integers $n_{d,u} \geq 0$ (for $d, u \geq 1$), such that almost all of them are zero, and that for any d,

$$n_d = \sum_u n_{d,u} \leq B_d(X/\mathbf{F}_q).$$

Suppose also

$$\sum_{d,u} n_{d,u} du \geq 2m + g - 1.$$

Then: if $|X(\mathbf{F}_q)| > 5g$, we have

$$\mu_q^{sym}(m) \leq \sum_{d,u} n_{d,u} \mu_q^{sym}(d,u).$$

Moreover, suppose X and Q are given explicitly, that $5g+1$ points of degree 1 on X are given explicitly, and, for any d, that n_d points of degree d on X are given explicitly. Suppose also that for each d, u such that $n_{d,u} > 0$, we are given explicitly a symmetric multiplication algorithm of length $l_{d,u}$ for $\mathcal{A}_q(d,u)$. Then, after at most $5g^2$ computations of Riemann-Roch spaces on X, we can construct explicitly a symmetric multiplication algorithm of length $\sum_{d,u} n_{d,u} l_{d,u}$ for $\mathcal{A}_q(m)$.

Remark 1.4. Although the previous criterion requires many points of degree one , it seems in practice that only one or two points of degree one are needed to build the divisor D (see the example in §VII.4.2). So it would be interesting to quantify the fact that the "favorable cases form a dense subset of points".

The following criterion states the existence of an asymmetric algorithm on every given curve X, such that this bilinear algorithm is essentially the best that one could expect from this given curve X, by Proposition VII.3.4.

Theorem 1.5 ([Ran$_1$, Proposition 5.7]). *Let X be a curve of genus $g \geq 2$ over $\mathbf{F}_q$, where $q \geq 2$ is any prime power, and let $m, l \geq 1$ be two integers.*

Suppose that X admits a closed point Q of degree $\deg Q = m$ (a sufficient condition for this is $2g + 1 \leq q^{(m-1)/2}(q^{1/2} - 1)$).

(Fix $e_q = 2$ in the original statement, for simplicity).

Consider now a collection of integers $n_{d,u} \geq 0$ (for $d, u \geq 1$), such that almost all of them are zero, and that for any d,

$$n_d = \sum_u n_{d,u} \leq B_d(X/\mathbf{F}_q).$$

Then, provided

$$\sum_{d,u} n_{d,u} du \geq 2m + g + 5,$$

we have

$$\mu_q(m) \leq \sum_{d,u} n_{d,u} \mu_q(d, u).$$

1.2 Generalizing in Theorem A the existential criterions of Shparlinsky–Tsfasman–Vladuts–Ballet and Cascudo–Cramer–Xing

The next two consequences state the existence of a symmetric algorithm, by an existential argument for divisors D satisfying (i') and (ii') of Theorem 1.1. See the introduction of [Ran$_2$] and [CCX, §4 Theorem 6] for a general discussion on such systems of divisorial equations.

The first one was stated by [STV, Claim p159-160], and later [Bal$_1$, Prop 2.1] gave an elementary proof as (but with the additional assumption that $q \geq 7$). However, as first noticed in Cascudo's PhD thesis, both arguments actually require that the divisor group has *no 2-torsion* (in order for the map $D \to 2D$ to be injective).

Theorem 1.6. *Let q a prime power and $m > 1$ an integer. Suppose we are given a curve X of genus $g \geq 2$ over $\mathbf{F}_q$, with Jacobian $J \widehat{=} \mathrm{Cl}_0(X)$, such that the rational class group $J(\mathbf{F}_q)$ contains* no rational divisor of 2-torsion.

Consider now a collection of integers $n_{d,u} \geq 0$ (for $d, u \geq 1$), such that almost all of them are zero, and that for any d,

$$n_d = \sum_u n_{d,u} \leq B_d(X).$$

Then, provided

$$\sum_{d,u} n_{d,u} du \geq 2m + g - 1,$$

we have

$$\mu_q(m) \leq \sum_{d,u} n_{d,u} \mu_q(d,u).$$

We skip the proof, because it can be seen as a particular case of the proof of the next theorem [set $(\mathrm{Cl}_0 X)(\mathbf{F}_q)[2]$ to zero and (instead of using Proposition 1.8(iii) for degree $i = g-1$ as in [Bal$_1$] Prop 2.1) remove the $\log_q(2)$ term in R, to be able to conclude even when $q < 7$].

The following theorem does control for 2-torsion in the worst case. It is a straight generalization of [CCX$_2$, Theorem 5.18]. The parameters will be specified in the next paragraph to derive criterions for asymptotic bounds, then further specified in §3.2 [2].

Theorem 1.7. *Let X be a curve of genus g over $\mathbf{F}_q$, where $q \geq 2$ is any prime power, and let $m \geq 1$ be an integer.*

Suppose that X admits a closed point Q of degree $\deg Q = m$ *(a sufficient condition for this is $2g + 1 \leq q^{(m-1)/2}(q^{1/2} - 1)$).*

Consider now a collection of integers $n_{d,u} \geq 0$ (for $d, u \geq 1$), such that almost all of them are zero, and that for any d,

$$n_d = \sum_u n_{d,u} \leq B_d(X).$$

Let R the smallest integer *such that*

$$R \geq g(1 + \log_q(2)) + 2m + 3log_q\left(\frac{3qg}{(\sqrt{q}-1)^2}\right) + 2 \text{ (if } 2|q) \tag{1.3}$$

$$R \geq g(1 + 2\log_q(2)) + 2m + 3log_q\left(\frac{3qg}{(\sqrt{q}-1)^2}\right) + 2 \text{ (otherwise).} \tag{1.4}$$

Then, provided

$$\sum_{d,u} n_{d,u} du \geq R \tag{1.5}$$

[2] This presentation also avoids the choice of parameters used in the original theorem because they are not always proven to be valid (see the comments after Conjecture Y)

we have

$$\mu_q(m) \leq \sum_{d,u} n_{d,u}\mu_q(d,u).$$

The following proposition gathers the upper-bounding made in the proof. The first two follow from [M, p. 39 (or p. 64)]. Whereas the third one is borrowed from [CCX$_2$, Proposition 3.4].

Proposition 1.8. *Let $\mathbf{F}_q$ be a finite field and X a curve over $\mathbf{F}_q$ of genus $g \geq 1$. Let J be the Jacobian of X and $J(\mathbf{F}_q)$ the rational class group.*

(i) *If q is odd, then $J(\mathbf{F}_q)[2] \leq 2^{2g}$*

(ii) *If q is even, then $J(\mathbf{F}_q)[2] \leq 2^g$*

(iii) *Let h be the class number of X and, for any integer i with $0 \leq i \leq g-1$, A_i the number of $\mathbf{F}_q$-rational effective divisors of degree r. Then*

$$\frac{A_i}{h} \leq \frac{g}{q^{g-i-1}(\sqrt{q}-1)^2}$$

Let us now follow the original proof of the theorem [only in the case q even, the odd case being identic modulo using upper-bound (i) instead of (ii)]. Adding the terms $-\log_q\left(\frac{3qg}{(\sqrt{q}-1)^2}\right)$ and $2g(1-\log_q(2))$ to both sides of the inequality (1.3) reads :

$$2g + 2m + 2\log_q\left(\frac{3qg}{(\sqrt{q}-1)^2}\right) \leq g(1-\log_q(2)) + R - \log_q\left(\frac{3qg}{\sqrt{q}-1)^2}\right) - 2$$

Thus there exists an even integer $2d$ between the two sides of the previous inequality. Raising q to the inequalities $LHS \leq 2d$ and $2d \leq RHS$ respectively gives:

$$\frac{g}{q^{g-(2g-d+m)-1}(\sqrt{q}-1)^2} \leq \frac{1}{3} \tag{1.6}$$

$$\frac{g2^g}{q^{g-(2d-R)-1}(\sqrt{q}-1)^2} \leq \frac{1}{3} \tag{1.7}$$

Using the upper-bound (ii) in the previous proposition, and combining the two inequalities (1.6) and (1.7) above with the upper-bound (iii), yields

$$h > \frac{2}{3}h \geq A_{2g-d+m} + J(\mathbf{F}_q)[2]A_{2d-R} \tag{1.8}$$

Now let us choose a collection of pairwise distinct thickened points $\{P\}$ on the curve X such that, for each (d,u), there are exactly $n_{d,u}$ points among them of degree d and multiplicity u (this is possible by assumption). Let G be their divisorial sum and Q a closed point of degree m as in the assumption. G being of degree greater than R by assumption (1.5), the general criterion of [CCX, §4 Theorem 6] along with the inequality (1.8) imply the existence of a divisor $D = X$ of degree d that satisfies the following system of Riemann-Roch spaces vanishing conditions (with K being the canonical divisor of X):

$$l(K - X + Q) = 0 \tag{1.9}$$

$$l(2X - G) = 0 \tag{1.10}$$

Thus criterions (i') and (ii') of Theorem 1.1 are satisfied with the divisors G and D.

1.3 Generalizing the bounds of Ballet: (a')(ii)–Pieltant: (b), Randriam: (a) - (a')(i) and Cascudo–Cramer–Xing: (c) - (c')

Let $(X_s)_s$ be a dense sequence of curves over $\mathbf{F}_q$ with genera g_s growing to infinity, and a ratio of points of degree r matching $\widetilde{A}_r(q)$. Noting $\widetilde{A}_r = \widetilde{A}_r(q)$, this reads :

$$g_s \xrightarrow[s\to\infty]{} \infty \tag{d1}$$

$$B_r(X_s) = \widetilde{A}_r g_s + o(g_s) \tag{d2}$$

$$g_s = g_{s-1} + o(g_s) \tag{d3}$$

Let us prove first the bound (b), which generalizes [BCP, Proposition 11], but whose arguments were already introduced in [BP, Theorem 3.2]. Given an integer n, let $s(n)$ be the smallest integer such that

$$rlB_r(X_{s(n)}) - 2g_{s(n)} \geq 2n + 3. \tag{1.11}$$

(d2) makes clear (or anyway it will be in the following equivalences), that such an integer $s(n)$ exists as soon as the denominator in the criterion (b) of Theorem A is strictly positive.

Moreover g being large enough, [BRR, Proposition 4.3 and Remark 4.4] state in general the existence of a zero-dimensional divisor of degree $g-5$ on $X_{s(n)}$. Thus the existence of a non-special divisor R of degree (lower than) $g+3$.

Therefore, Corollary 1.2 applies to (1.11). Taking all $n_{d,u}$ null except $n_{r,l}$ equal to $B_r(X_{s(n)})$, this reads :

$$\mu_q^{\mathrm{sym}}(n) \leq \mu_q^{\mathrm{sym}}(r,l)B_r(X_{s(n)}). \tag{1.12}$$

Let us now tie the asymptotics behaviors of $g_{s(n)}$ and $B_r(X_{s(n)})$. The minimality of $s(n)$ satisfying (1.11) implies :

$$rlB_r(X_{s(n)}) - 2g_{s(n)} \geq 2n+3 > rlB_r(X_{s(n)-1}) - 2g_{s(n)-1}$$

Dividing the two inequalities by $g_{s(n)-1}$, and applying the asymptotic equivalences (d2) and (d3) (and (d1)) yields :

$$rl\widetilde{A}_r - 2 + o(n) \geq \frac{2n}{g_{s(n)}} + o(1) > rl\widetilde{A}_r - 2 + o(n)$$

hence the asymptotic equivalence :

$$2n + o(n) = (rl\widetilde{A}_r - 2)g_{s(n)} + o(g_{s(n)})$$

(which implies in particular that $o(n) = o(g_{s(n)})$). One can now divide both sides of the upper-bound (1.12) by the previous equality :

$$\frac{\mu_q^{\mathrm{sym}}(n)}{n} \leq \mu_q^{\mathrm{sym}}(r,l).2\left(\frac{\widetilde{A}_r g_{s(n)} + o(n)}{(rl\widetilde{A}_r - 2)g_{s(n)} + o(n)}\right)$$

Multiplying and dividing the RHS parenthesis by rl, then subtracting and adding $2g_{s(n)}$ to the numerator of the RHS, gives the result by letting n tend to infinity.

The asymmetric (a), and symmetric bounds : (a'), (c) & (c') are derived similarly from the other generalized criterions stated above. Indeed, given

an integer n, consider $s(n)$ be the smallest integer such that, respectively :

(1.13)
$$rlB_r(X_{s(n)}) - g_{s(n)} \geq 2n + 5 \text{ for (a)}$$

(1.14)
$$rlB_r(X_{s(n)}) - g_{s(n)} \geq 2n + 1 \text{ under either condition (a').(i) or (a').(ii)}$$

(1.15)
$$rlB_r(X_{s(n)}) - (1 + \log_q 2)g_{s(n)} \geq 2n + 3log_q\left(\frac{3qg_{s(n)}}{(\sqrt{q}-1)^2}\right) + 3 \text{ if } 2|q \text{ for (c)}$$

(1.16)
$$rlB_r(X_{s(n)}) - (1 + 2\log_q 2)g_{s(n)} \geq 2n + 3log_q\left(\frac{3qg_{s(n)}}{(\sqrt{q}-1)^2}\right) + 3 \text{ otherwise for (c')}$$

Similarly, such integers $s(n)$ exist as soon as the respective denominators in equations (a), (a'), (c) and (c') are strictly positive. Then apply the following criterions with all the $n_{d,u}$ null excepted $n_{r,l} = B_r(X_{s(n)})$:

Th. 1.5 for upper-bound (1.13), Th. 1.3 for upper-bound (1.14)(i), Th. 1.6 for (1.14)(ii), and Th. 1.7 for both (1.15) and (1.16).

2 Known asymptotic ratios of closed points

2.1 Many $\mathbf{F}_{q^r}$-points means many points of degree r

The following fact is possibly well-known. The proof given here reproduces the arguments of [CCXY].

Theorem 2.1. *Let $(X_s/\mathbf{F}_q)$ be a family of curves over a finite field $\mathbf{F}_q$, with genera g_s tending to infinity. Let $r \geq 1$ be an integer, and $B_r(X_s)$ the number of closed points of degree r. Then the following assertions are equivalent :*

(i) $$\frac{|X_s(F_{q^r})|}{g_s} \xrightarrow[s\to\infty]{} \sqrt{q^r} - 1$$

(ii) $$\frac{B_r(X_s)}{g_s} \xrightarrow[s\to\infty]{} \frac{\sqrt{q^r}-1}{r}$$

The demonstration is based on the following lemma, which itself is a consequence of the generalization by Tsfasman of the bound of Drinfeld–Vladuts.

Lemma 2.2 ([CCXY, Lemma IV.3]). *Let $(X_s/\mathbf{F}_q)_s$ be a family of curves over a finite field $\mathbf{F}_q$, with genera g_s tending to infinity. If for some $m \geq 1$, one has*

$$\lim_{s\to\infty} \frac{1}{g_s} \sum_{i=1}^{m} \frac{iB_i(X_s)}{q^{m/2}-1} \geq 1 \tag{2.1}$$

then

$$\lim_{s\to\infty} \frac{mB_m(X_s)}{g_s} = q^{m/2}-1 \tag{2.2}$$

Now, let $(X_s)_s$ a family satisfying the hypotheses of the theorem. By the identity $X_s(\mathbf{F}_{q^r}) = \sum_{i|r} iB_i(X_s)$, one gets

$$\lim_{s\to\infty} \frac{1}{g_s} \sum_{i=1}^{r} \frac{iB_i(X_s)}{q^{r/2}-1} \geq \lim_{s\to\infty} \frac{1}{g_s} \sum_{i|r} \frac{iB_i(X_s)}{q^{r/2}-1} = \lim_{g_s\to\infty} \frac{X_s(\mathbf{F}_{q^r})}{g_s(q^{r/2}-1)} = 1 \tag{2.3}$$

Thus, the inequality (2.1) of the previous lemma is satisfied, so the conclusion of the theorem follows.

2.2 Non-necessarily dense families

Being defined with equations in the prime field, the tower of Garcia-Stichtenoth naturally descends :

Theorem 2.3 (Garcia-Stichtenoth [GS], descended over the prime field). *Let $q = p^r$ be a prime power and $F_1 = \mathbf{F}_p(x_1)$ be the rational function field over $\mathbf{F}_p$. For $n \geq 1$, we set*

$$F_{n+1} = F_n(z_{n+1})$$

where z_{n+1} satisfies the equation

$$z_{n+1}^q + z_{n+1} = x_n^{q+1} \tag{2.4}$$

with

$$x_n := z_n/x_{n-1} \in F_n \text{ (for } n \geq 2 \text{)}$$

Then (F_n) is a sequence of function fields such that when n tends to infinity,

$$|F_n(\mathbf{F}_{p^{2r}})| / g(F_n) \longrightarrow p^r - 1$$

Proof Let K be the field $\mathbf{F}_{q^2}$ and $(K.F_n)$ the tower of fields with constant field K defined by equation (2.4). These are the fields considered in [GS] (definition 0.1), whose asymptotic ratio of K-points equal to $p^r - 1$ (corollary 3.2).

What remains to be checked is that for each n, the extension degrees $|F_{n+1}/F_n|$ are preserved after constant field extension by K. But the reccurence argument of loc. cit. done in Lemma 2.1 and Prop 1.1 (and concluded in Lemma 2.2), shows in particular that for each n, the polynomial of equation (2.4) : $z_{n+1}^q + z_{n+1} - x_n^{q+1}$ is irreducible over $K.F_n$. Thus is also irreducible over F_n. □

By Lemma 2.2, the previous theorem implies that

Corollary 2.4. *For all prime power q and r an integer such that q^r is a square, one has*

$$A_r(q) = \frac{\sqrt{q^r} - 1}{r}$$

When q^r is not a square, the values of $A_r(q)$ as still unknown. But lower-bounds benefited from recent progress: on the one hand for prime fields $q = p$ and points of degree one (see [HS] for a survey):

Table 2.1: Lower bounds for $A_1(p)$

p	2 [DM]	3 [DM]	5 [AM]	7 [HS]	11 [HS]	13 [LM]
$A_1(p)$	$0,317$	$0,493$	$0,727$	$0,923$	$1,14$	1.33

On the other hand for any odd prime power $q = p^{2m+1}$ such that $m \geq 1$, Bassa–Beelen–Garcia–Stichtenoth produced an explicit tower that sets a new lower bound for the number of points of degree one :

Theorem 2.5 ([BBGS])**.**

$$A_1(p^{2m+1}) \geq 2\frac{p^{m+1} - 1}{p + 1 + \epsilon} \text{ with } \epsilon = \frac{p-1}{p^m - 1} \tag{2.5}$$

Notice that the case $q = p^3$ had been firstly announced by Zink [Zi].

2.3 Dense families

[Iha$_2$] showed that Shimura curves do provide, for any finite field, dense families of curves with many points over a quadratic extension. For our purpose, the explicit work [Duc] provides at least all the equalities $\widetilde{A}_2(q) = (q-1)/2$ needed in Tables 2.2:

Theorem 2.6. *For any prime power q such that : { there exists a number field F and a principal prime ideal $\mathfrak{p}$ in F above p, generated by a totally positive element, of norm $q = N(\mathfrak{p})$ }. Then*

$$\widetilde{A}_2(q) = \frac{q-1}{2}$$

Proof The existence of a family over $\mathbf{F}_q$, with an asymptotic ratio of $\mathbf{F}_{q^2}$-points equal to $q-1$, will be stated in theorem V.5.4. Theorem 2.1 thus implies that the ratio of points of degree two is $(q-1)/2$.

The density of the family will be stated in Corollary IV.2.2 (avoiding here the negligible set of disciminants and levels divided by $\mathfrak{p}$). □

3 About the new numerical bounds

3.1 For small binary algebras, in Table 2.1 of §2.3

In the following Table 3.1, we attempt to give references or explanations for some bounds of Table 2.1 in §2.3. We do not claim to always giving credit to the first discoverer, nor to the most efficient method. In particular, the inequality $\mu_q^{\mathrm{sym}}(m,l) \leq \mu_{q^d}^{\mathrm{sym}}(e,l)\mu_q(d)$ (see *e.g.* [Ran$_1$, Lemma 4.6]) is often used. For the upper and lower bounds that are new, up to our knowledge, we provide more details about how they were established in VII.2.

The exact formulas for the three new upper bounds used here are given in the annex A.2 : for $\mu_2(3,2)$, $\mu_4(1,4)$ and $\mu_4(1,5)$.

Remark 3.1. We would like to point here an error in our article [Ra, Table 1] in which these bounds were first published. The best known upper-bound for $\mu_2^{\mathrm{sym}}(1,10)$ is actually still 31 as in [CO$_2$, Table 2], not 30 as claimed. The new bound being actually $\mu_2^{\mathrm{sym}}(2,5) \leq \mu_4^{\mathrm{sym}}(1,5)\mu_2(2,1)^{\mathrm{sym}} = 10.3 = 30$, with our contribution being the exact value $\mu_4^{\mathrm{sym}}(1,5) = 10$. This value was already claimed in [Ra, Table 2] at entry (1,10), although the upper-bounding in which it was used was then grossly false.

Table 3.1: Origins of the bounds for $\mu_2(m,l)$ in Table 2.1

$\mu_2^{\mathrm{sym}}(m,l)$	Upper bound	Lower bound
$(5,1)$	[Mon]	[BDEZ]
$(6,1)$	$\leq \mu_4^{\mathrm{sym}}(3)\mu_2^{\mathrm{sym}}(2)$ (first factor : by interpolation over $\boldsymbol{P}^1_{\mathbf{F}_4}$)	[BDEZ]
$(7,1)$	[Mon]	[BDEZ]
$(8,1)$	$\leq \mu_4^{\mathrm{sym}}(4)\mu_2^{\mathrm{sym}}(2)$ (first factor: $[\mathrm{CO}_0]$ but unknown original contributor)	.
$(9,1)$	$[\mathrm{CO}_0]$	.
$(10,1)$	$\leq \mu_4^{\mathrm{sym}}(5)\mu_2^{\mathrm{sym}}(2)$ (first factor: $[\mathrm{CO}_0]$ but unknown original contributor)	.
$(1,5)$	[Oce]	[BDEZ]
$(1,6)$	[Oce]	[BDEZ]
$(1,7)$	[Oce] (proved valid over a general ring, in $[\mathrm{CO}_2]$)	[BDEZ]
$(1,8)$	$[\mathrm{CO}_2]$	[BDEZ]
$(1,9)$	$[\mathrm{CO}_2]$	[BDEZ]
$\mathbf{(1,10)}$	$\leq \boldsymbol{\mu_4^{\mathrm{sym}}(1,5)}\mu_2^{\mathrm{sym}}(2)$, the first factor being ***equal to* 10**: c.f. A.2	.
$(2,2)$	$\leq \mu_4^{\mathrm{sym}}(1,2)\mu_2^{\mathrm{sym}}(2)$	**new**
$(2,3)$	$\leq \mu_4^{\mathrm{sym}}(1,3)\mu_2^{\mathrm{sym}}(2)$	**new**
$\mathbf{(3,2)}$	**new**	**new**
$\mathbf{(2,4)}$	$\leq \boldsymbol{\mu_4^{\mathrm{sym}}(1,4)}\mu_2^{\mathrm{sym}}(2)$, the first factor being ***equal to* 7**: c.f. A.2	.
$(4,2)$	$[\mathrm{Ran}_1]$, inequality (94)	.
$(3,3)$	$\mu_8^{\mathrm{sym}}(1,3)\mu_2(3)$	.

3.2 The upper limit bounds M_q in Table 2.2 of I.2.3

The table 3.2 below justifies the upper bounds for the M_q stated in table 2.2. The explanation consists in the criterion of Theorem A used, along with the parameters (r, l) chosen. These parameters are chosen:

- within the previously known values for dense families (see section §2.3) in the lines "published bounds" and "Theorem A";
- whereas more parameters are allowed in the lines below (the new values stated by Theorem B, then by Conjecture X and finally under the more general Conjecture Y);
- The line assuming Conjecture Z needs not assuming any of the previous new values (neither Theorem B nor the two previous conjectures).

Remark 3.2. On the face of it, the symmetric bound for $q = 5^2$ directly results from the formula of the proposition 10 in [BCP]. Although the authors themselves did not compute it numerically. It seems that they thought that it would be beaten by the bounds of [CCX_2] (see the discussion of the authors following theorem 14, where they only mention the cases $q > 5$).

But actually, the proposition 10 actually relies on results from 1999 ([Bal_1]: lem 2.2=>1.1=>cor 2.1). They are based on a coding-theoretic argument. It consists in removing points from the interpolation divisor G, while still preserving injectivity of the evaluation map $\mathcal{L}(2D) \to \mathcal{L}(2D - G)$. So this trick only works for points of degree 1 and multiplicity 1, and does not seem cheaply generalizable.

Finally this upper-bound runs between the drops of every further improvements. First because the value of $25 = p^2$ is below the threshold of $p^2 \geq 49$ of Theorem A (a'), that would ensure an even lower complexity. Last because q is odd [so the 2-torsion rank of the Jacobian is only upper-bounded by q^{2g} in A (c')][3]. Nevertheless, solving conjecture Z for $p = 5$ could remove the problem of 2-torsion and enable to improve the bound.

3.3 The lower-limit bounds m_q in Table 2.3 of §2.3

Remark 3.3. The morals of this part is that *the lower-limit measure mostly ignores both the issues of two-torsion, and of the field of definition of the*

[3] To illustrate this point, observe that if 25 were even, then the torsion upper-bounding q^g would provide the slightly better bound $2,87$ for M_{25}

Table 3.2: Origins of the bounds for M_q in table 2.2

Results used \q		2	3	4	5
(Repaired) Bounds	Sym	[BP_2]	[BP_2]	(c) (2,1)	(c') (2,1)
	Asym	[PR] Prop 5.1	[PR] Prop 5.1	(a) (2,1)	(a) (2,1)
Th. A and Tab. 2.1	Sym	(b) (2,5)	(b) (2,3)	(c) (2,2)	(c') (2,2)
	Asym	(a) (2,4)	—	—	—
Adding Th. B	Sym	—	(b) (6,1)	—	(c') (6,1)
	Asym	—	(a) (6,1)	—	—
Conjecture X	Sym	(b) (6,1)	—	(c) (3,1)	—
	Asym	(b) (6,1)	—	(a) (3,1)	—
Conjecture Y	Sym	(b) (8,1)	(b) (8,1)	—	(c') (4,1)
	Asym	—	(a) (4,1)	—	—
Conjecture Z	Sym		—	—	(a') (2,1)

Results used \q	7	8	9	11	5^2
(Repaired) Bounds	(c') (2,1)	(c) (2,1)	(c') (2,1)	(c') (2,1)	[BP_2, Prop. 10] (1,1)
	(a) (2,1)	(a) (2,1)	(a) (2,1)	(a) (2,1)	(a) (1,1)
Th. A and Tab. 2.1	(c') (2,2)	—	—	—	—
	—	—	—	—	—
Adding Th. B	—	—	(c') (3,1)	—	—
	—	—	—	—	—
Conjecture X	—	—	—	—	—
	—	—	—	—	—
Conjecture Y	(c') (4,1)	(c) (4,1)	—	(c') (4,1)	—
	(a) (4,1)	—	—	—	—
Conjecture Z	(a') (2,1)	—	—	(a') (2,1)	(a') (2,1)

curves. Indeed, suppose that we have painfully found a family of curves defined over a small field $\mathbf{F}_q$, with controled two-torsion, and having many points of degree r. Then the lower-limit can actually equally be computed:

- using the closed points of degree (say r) on these curves;
- or, after a base-field extension of degree r, using the closed points of degree 1. And moreover, [Ran_1, Theorem 6.3]) then allows to ignore the two-torsion.

The explanation lies in the following property for m_q [explained by the fact that the lim inf can be evaluated on fewer –so more advantageous– values].

Lemma 3.4 ([STV] Corollary 1.3)**.** *For any positive integer r, and prime power q,*

$$m_q^{\mathrm{sym}} \leq \frac{\mu_q^{\mathrm{sym}}(r)}{r} m_{q^r}^{\mathrm{sym}} \tag{3.1}$$

$$M_q^{\mathrm{sym}} \leq \mu_q^{\mathrm{sym}}(r).M_{q^r}^{\mathrm{sym}}, \tag{3.2}$$

The asymmetric counterparts also hold (removing all the symbols sym *above).*

Using the previous lemma, the criterions (a) and (a')(i) (relaxing the density condition) can then be respectively be applied to q^r. Which implies the following (apparent) generalization :

Theorem 3.5. *Let q be a prime power and $r \geq 1$ a positive integer. If $A_1(q^r) > 1$, then*

$$m_q \leq \frac{\mu_q(r)}{r}\left(1 + \frac{1}{A_1(q^r) - 1}\right).$$

Moreover, if $A_1(q^r) > 5$, then also $m_q^{\mathrm{sym}} \leq \frac{\mu_q^{\mathrm{sym}}(r)}{r}\left(1 + \frac{1}{A_1(q^r)-1}\right)$.

The last statement is used by [CCX_2], V, table II to provide most of the symmetric bounds in table 2.3. Whereas for the asymmetric bounds, the first statement is enough.

4 About Conjecture X

Consider $F = \mathbf{Q}(\cos(2\pi/7))$ and "the" quaternion algebra ramified exactly at two of the three real places (the three possible choices lead to isomorphic models). Recall the canonical models over F:

- $X_0(1)$ is uniformized by the (2,3,7) triangle group,
- $X_0(\mathfrak{p}_3)$ was computed in [Elk06] and is the elliptic curve 147.c1 ([LMFDB] labels).
- $X_0(\mathfrak{p}_3^2)$ is of genus 10 and still unknown. By the first statement of Theorem V.5.14 it descends over $\mathbf{Q}$.

Among the dimension 10 vector space of Hilbert modular forms associated to $X_0(\mathfrak{p}_3^2)$, the Atkin–Lehner stable are of dimension 2 and can be decomposed into

- the old form of level $\mathfrak{p}_3$, associated to the elliptic curve $X_0(\mathfrak{p}_3)$: 147.c1
- a new form of level $\mathfrak{p}_3^2$, associated to the isogeny class of the elliptic curve 441.d2

Now, it is possible to compute the Atkin–Lehner quotient $X_0(\mathfrak{p}_3^2)^*$, of genus 2, with the algorithm of Klug–Voight–Willis for modular forms arising from Fuchsian groups. It has equation:

$$y^2 = x^6+84*x^5+4876*x^4+163296x^3+8726544/7x^2-20500672x+10355021120/49$$

which is isomorphic over $\mathbf{Q}$ to:

$$y^2 + (x^3 + x^2 + x + 1)y = x^6 + 6x^5 + 11x^4 + 9x^3 + 11x^2 + 6x + 1$$

We check with the algorithm of [CMSV]—[BSSVY] that the Jacobian of this curve is, as expected, $\mathbf{Q}$-isogenous to the product of

- 147.c2, itself $\mathbf{Q}$-isogenous to 147.c1,
- and 441.d2.

5 About conjecture Z

Here is a sketch of proof of equation (2.6) (we follow the arguments of [Sh_3, §7.5], see also [Duc, Prop IV 2.6] for the general case with Shimura curves).

Proof Let p be a prime, N a positive integer prime to p, $X_0(N)$ the classical modular curve over the rationals, endowed with the Hecke correspondence T_p on divisors. Then Igusa's theorem states that there exists a good reduction $\widetilde{X_0(N)}$ over $\mathbf{F}_p$, compatible with the moduli interpretations. The relation of Eichler–Shimura [DS, §8.7 and exercice 8.7.2] states that the correspondence T_p reduces to a divisorial correspondence $\widetilde{T}_p$ on $\widetilde{X_0(N)}$, which can be expressed as follows. Let σ_p be the geometric Frobenius divisorial correspondence $\widetilde{X_0(N)}$ and σ_p^* its transpose. Then

$$\widetilde{T}_p = \sigma_p + \sigma_p^*.$$

Let us remind some general curve-theoretic results:

(i) by the construction of the Jacobian, the correspondence σ_p induces the geometric Frobenius endomorphism $\sigma_{J,p}$ on $\widetilde{J} = \mathrm{Jac}(\widetilde{X_0(N)})$. Similarly, the transposed correspondence σ_p^* induces the Rosati-dual of the previous $\sigma_{J,p}^\dagger$.

(ii) the composition $\sigma_{J,p}^\dagger \circ \sigma_{J,p}$ equals the endomorphism $[p]$ of multiplication by p.

(iii) the cardinality of $\left|\widetilde{J}(\mathbf{F}_{p^2})\right|$ is equal to the degree of the endomorphism $\mathrm{Id} - \sigma_{J,p}^2$ (see the proof of [MilAV, II Th. 1.1]). Letting $l \neq p$ be any prime distinct from p, $\widetilde{T}_l$ be the Tate ($2g$-dimensional $\mathbf{Z}_l$-) module of $\widetilde{J}$ and $\sigma_{l,p}$ the induced morphism on $\widetilde{T}_l$, then by the general relation [M, §19 th. 4], the degree considered above is equal to the determinant $\det(\mathrm{Id} - \sigma_{l,p}^2 | \widetilde{T}_l)$. So :

$$\left|\widetilde{J}(\mathbf{F}_{p^2})\right| = \det(\mathrm{Id} - \sigma_{l,p}^2 | \widetilde{T}_l).$$

(iv) The following modular forms-theoretic result will be used. Let $T_{n,H}$ be the complex endomorphism of the homology $H_1(X_0(N), \mathbf{C})$ induced by the Hecke correspondence T_n. And $T_{n,0}$ the induced endomorphism acting on the –twice smaller– space of level 2 cuspforms $S_0(\Gamma_0(N), \mathbf{C})$. Then it is possible to choose a basis of $S_0(\Gamma_0(N), \mathbf{C})$ (made of cusp forms with rational

coefficients) such that the matrix of $T_{n,0}$ has *rational* coefficients [Ste, Lem. 3.25].

(v) Noting $T_{n,J}$ the endomorphism induced by the correspondence T_n on the Jacobian $J = \mathrm{Jac}(X_0(N))$, then the $\mathbf{Z}_l$-linear endomorphism $T_{n,l}$ induced on the Tate module $T_l(J)$ actually coincides with the rational representation of $T_{n,J}$. In particular up to a base change, its matrix is equal to the direct sum of the matrix of $T_{n,J}$ and its conjugate. Both summands are equal, when choosing a rational basis as in (iv). Moreover the $\mathbf{Z}_l$-linear endomorphism $\widetilde{T_{n,l}}$, induced on the Tate module $\widetilde{T}_l$ by the reduced endomorphism $\widetilde{T_{n,J}}$, is actually equal to $T_{n,l}$ by [Sh_4, §11 Prop 14].

We can now prove (2.6). Let α_i be the $2g$ eigenvalues of $\sigma_{l,p}$. Let $T_{l,p}$ be the morphism induced by T_p on the Tate module $T_l(X_0(N))$ (an unfortunate notation), and its counterpart for the reduced Jacobian : $\widetilde{T_{l,p}}$ the morphism induced by $\widetilde{T}_p$ on $\widetilde{T}_l$. By (5), it suffices to prove the equality :

$$\det\big(p^2 - T_p + 1 | S_0(\Gamma_0(N))\big) = \det\big(1 - \sigma_{l,p}^2 | \widetilde{T}_l\big).$$

Firstly, the relation (5), the identification (i), formula (ii) and property (iii) immediatly imply :

$$\det(1-\sigma_{l,p}^2)\det(1-(\sigma_{l,p}^\dagger)^2) = \det(1+p^2-\widetilde{T_{l,p}}^2 | \widetilde{T}_l)$$

But (a) the caracteristic polynomials of $\sigma_{l,p}$ and of its Rosati-dual $\sigma_{p,l}^*$ being equal, and (b) the $\mathbf{Z}_l$-adic endomorphism $\widetilde{T_{l,p}}$ actually being equal to the direct sum of the rational morphism $T_{p,0}$ (on the space $S_0(\Gamma_0(N), \mathbf{C})$) with itself [by (iv) and (v)], one obtains the square of equation (5) :

$$\det(1-\sigma_{l,p}^2)^2 = \det\big(1+p^2-T_{p,0}^2 | S_0(\Gamma_0(N), \mathbf{C})\big)^2.$$

□

Chapter III

Conditions for friendly quaternion algebras and Shimura curves

1 Goals and conventions

1.1 Goals

Although this chapter contains essentially well-known facts on quaternion algebras, its purpose is to clarify some points:

- The two connected Shimura curves $X_0^+(\mathfrak{N})$ and $X_0(\mathfrak{N})$ coincide only when the narrow class number of F is one (Proposition 3.2). Only the former is known to have a canonical model with many points (see VI.4 for an interesting example where they do not coincide). Whereas the latter, although being more computational-friendly as a complex curve, has in general several possible canonical models (see [Sij_1, below Prop 3.2.4]).
- The group of Atkin–Lehner is defined by equation (4.4). The issue of §III.4.2 is that in the setting of this thesis, the group boils down to equation (4.3).

  On the contrary in the general case (without the narrow class number one assumption), the group of Atkin–Lehner can be strictly bigger. This is described in the references given in Footnote 3 in Proposition 4.1. This extra-complexity can happen even if the Eichler order is of level a power of a prime ideal;
- Corollary 2.5 gives a sufficient criterion for all Eichler levels of given

level to be conjugate (see [Sij$_1$, Proposition 2.6.2] for a thinner classification). This allows the descent data of Theorem V.5.11.

- The purpose of this last section, about §III.5. is threefold:

  - to explain how the $\mathrm{PSL}_2(R)$ of a finite localdef:narrow ring R acts on the set $\mathbf{P}^1(R)$: Lemma 5.2. This is the key to the monodromy computations of §V.3.2;

  - to provide the index-counting results Propositions 5.4 and Corollary 5.6. Notice that the latter could actually be obtained immediatly from strong approximation;

  - and to stress that the congruence subgroup that has a Galoisian meaning: $\Gamma'(\mathfrak{N})$, can be strictly bigger than the classical principal congruence subgroup $\Gamma(\mathfrak{N})$. This happens when the norm of $\mathfrak{N}$ is even.

    Stressing this fact is the sole purpose of Proposition III.5.7, which is not used anywhere else in the thesis.

1.2 Conventions

Definitions are done with the defined object on the left-hand side of the equality defining it. A superscript dot to an algebra A, e.g. $A^\bullet$, stands for the subgroup of invertible elements for the multiplication. The cardinality of a set X is noted $|X|$.

Let F be a number field with ring of integers $\mathbf{Z}_F$ and P_F the set of finite places of F. The norm of an

Let B be a quaternion algebra with center F. Every element $x \in B$ has a *trace* $t(x)$ and a *norm* $n(x)$, the former being additive and the latter multiplicative.

For example in the interesting case for this work where B is a (non-commutative) field, every element $x \in B$ lies in a quadratic subfield $F \subset L \subset B$, so has a *minimal polynomial* over F, such that the standard involution $x \to \overline{x}$ swaps its roots. The trace and norm in L/F coincide with the previous.

Let B_v be the completion of B at a place v of F. Let $\mathfrak{D}$ be the finite discriminant of B, i.e. the product of the finite places $\mathfrak{p}$ which *ramify* B, i.e. for which $B_\mathfrak{p}$ is a field. Recall that the total number of ramified places is

even, by the reciprocity law for the Hilbert symbol ([Vig, Propriété II p75] or [Voi$_5$, Theorem 14.6.1]).

An *ideal* is a $\mathbf{Z}_F$-lattice of B. A ($\mathbf{Z}_F$-) *order* $\mathcal{O}$ is an ideal which is a ring or, equivalently, an ideal integral over $\mathbf{Z}_F$ (see also [Voi$_1$, Lemma 10.3.7]).

An ideal I is *invertible* if and only if the completions $I_\mathfrak{p}$ at each finite place $\mathfrak{p}$ are locally principal, generated by an invertible element $\alpha_\mathfrak{p}$ (see [Voi$_5$, Main Theorem 16.6.1]). An ideal I is *two-sided* if and only if it has the same left and right order $\mathcal{O}$. An *Eichler order* is the intersection of two maximal orders. The completion $\mathcal{O}_\mathfrak{p}$ of an Eichler order $\mathcal{O}$ at $\mathfrak{p}|\mathfrak{D}$ being equal to the unique maximal order of $B_\mathfrak{p}$, the level $\mathfrak{N}$ of $\mathcal{O}$ is automatically prime to $\mathfrak{D}$.

Definition 1.1. Let $\infty_\mathbf{R}$ be the set of infinite real places of F, ∞_B the subset of real places which ramify B and $\mathcal{O}$ an order. Define:

- the *totally positive subgroups* $F^+ \subset F^\bullet$ and $\mathbf{Z}_{F,+} \subset \mathbf{Z}_F^\bullet$, and the larger groups F_B and $\mathbf{Z}_{F,B}$, which are the invertible elements which are totally positive at $\infty_\mathbf{R}$, respectively at ∞_B;
- the *narrow class groups* $\mathrm{Cl}(\infty_\mathbf{R})$ and $\mathrm{Cl}(\infty_B)$ of ideals modulo the principal ideals generated by elements in F^+, respectively in F_B;
- the *narrow class number* $h^+ = |\mathrm{Cl}(\infty_\mathbf{R})|$;
- the *narrow class field* $F_\infty = F(\infty_\mathbf{R})$, which is the corresponding abelian extension;
- the *totally positive subgroups* B^+ and $\mathcal{O}^+$, of invertible elements, respectively units, of norm in F^+;
- the *narrow classes of ideals* $\mathrm{Cl}^+(\mathcal{O})$ and $\mathrm{Cl}^+_\mathrm{R}(\mathcal{O})$, as quotients of: invertible two sided $\mathcal{O}$-ideals, respectively invertible right $\mathcal{O}$-ideals, modulo principal ideals generated by elements in B^+;
- the *subgroups of norm one* B^1 and $\mathcal{O}^1$.

It is assumed that B has at least one split infinite place v.

2 Classes of Eichler orders and of ideals

2.1 Global adelic dictionnary

The split infinite place condition is not necessary here.

Let $\mathcal{O}$ be any $\mathbf{Z}_F$-order and define:

$$\widehat{\mathcal{O}} = \prod_{\mathfrak{p} \in P_F} \mathcal{O}_\mathfrak{p} \ ,$$

This is an additive subgroup of the following: let $\widehat{F}$ be the ring of finite adèles of F, then the *ring of finite adèles of* B:

$$\widehat{B} = B \otimes_F \widehat{F}$$

is in fact equal to the restricted product of the locally compact groups $B_{\mathfrak{p}}$ with respect to the compact subgroups $\mathcal{O}_{\mathfrak{p}}$ ([Vig, 3) p60]).

The lattices in B over $\mathbf{Z}_F$ are determined by their completions at the finite places of F:

Lemma 2.1 ([Vig, Proposition III.5.1])**.** *Let X be any fixed $\mathbf{Z}_F$-lattice of B. Then one has the following bijection of sets:*

$$\left\{\mathbf{Z}_F\text{-lattices } Y \text{ of } B\right\} \longleftrightarrow \left\{\left(Y_{\mathfrak{p}}\right)_{\mathfrak{p}\in P_F},\ Y_{\mathfrak{p}} \text{ lattices of } B_{\mathfrak{p}} \text{ such that } Y_{\mathfrak{p}} = X_{\mathfrak{p}} \text{ for almost every } \mathfrak{p}\right\}$$

$$Y \longmapsto \left(Y_{\mathfrak{p}}\right)_{\mathfrak{p}}$$

$$Y = \{y \in B,\ y \in Y_{\mathfrak{p}} \text{ for all } \mathfrak{p}\} \longmapsfrom \left(Y_{\mathfrak{p}}\right)_{\mathfrak{p}}$$

Fixing an order $\mathcal{O}$, the properties of being an ideal or a two-sided ideal for $\mathcal{O}$ are local, so the bijection also restricts to ideals and two-sided ideals.

Finally, let $\mathcal{O}$ be an order in a (possibly local) quaternion algebra B, and $N_{B^\bullet}(\mathcal{O})$ be the normalizer of $\mathcal{O}$ in $B^\bullet$. Then the principal two sided $\mathcal{O}$-ideals $\mathrm{PIdl}(\mathcal{O})$, and likewise the principal $\mathcal{O}$-ideals on the right $\mathrm{PIdl}_{\mathrm{R}}(\mathcal{O})$, are seen to be given by the following exact sequences ([Voi$_1$, 18.5.2]):

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}^\bullet & \longrightarrow & N_{B^\bullet}(\mathcal{O}) & \longrightarrow & \mathrm{PIdl}(\mathcal{O}) & \longrightarrow & 1 \\ & & & & \alpha & \longmapsto & \alpha\mathcal{O} = \mathcal{O}\alpha = \mathcal{O}\alpha\mathcal{O} & & \\ 1 & \longrightarrow & \mathcal{O}^\bullet & \longrightarrow & B^\bullet & \longrightarrow & \mathrm{PIdl}_{\mathrm{R}}(\mathcal{O}) & \longrightarrow & 1 \\ & & & & \alpha & \longmapsto & \alpha\mathcal{O} & & \end{array} \tag{2.1}$$

This enables to give an idelic description of invertible ideals and of their classes:

Lemma 2.2. *Let $\mathcal{O}$ be a fixed order. Then one has the following bijections*

of sets:

$$\begin{array}{ccc} \{\textit{Invertible right } \mathcal{O}\textit{-ideals}\} & & \widehat{B}^\bullet/\widehat{\mathcal{O}}^\bullet \\ I \textit{ such that } I_\mathfrak{p} = \alpha_\mathfrak{p}\mathcal{O}_\mathfrak{p} & \longleftarrow\!\shortmid & (\alpha_\mathfrak{p})_\mathfrak{p} \\ \mathrm{Cl}^+_{\mathrm{R}}(\mathcal{O}) & & B^+\backslash\widehat{B}^\bullet/\widehat{\mathcal{O}}^\bullet \\ \{\textit{Invertible two-sided } \mathcal{O}\textit{-ideals}\} & & N_{\widehat{B}^\bullet}(\widehat{\mathcal{O}}^\bullet)/\widehat{\mathcal{O}}^\bullet \\ I \textit{ such that } I_\mathfrak{p} = \alpha_\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}\alpha_p = \mathcal{O}_\mathfrak{p}\alpha_\mathfrak{p}\mathcal{O}_\mathfrak{p} & \longleftarrow\!\shortmid & (\alpha_\mathfrak{p})_\mathfrak{p} \\ \mathrm{Cl}^+(\mathcal{O}) & & N_{B^+}(\mathcal{O}^\bullet)\backslash N_{\widehat{B}^\bullet}(\widehat{\mathcal{O}}^\bullet)/\widehat{\mathcal{O}}^\bullet \end{array}$$

Likewise, the property of being integral over $\mathbf{Z}_F$ is local so the bijection of Lemma 2.1 restricts to orders. Furthermore Lemma 2.1 also shows that the property of being a maximal order is local, so the bijection also restricts to Eichler orders. In addition, all the Eichler orders of given level in local quaternion algebras being conjugate, one can describe the bijection in terms of local conjugates of a fixed Eichler order:

Lemma 2.3. *Let $\mathcal{O}(\mathfrak{N})$ be any fixed Eichler order of level $\mathfrak{N}$ and $N(\widehat{\mathcal{O}(\mathfrak{N})})$ the normalizer of $\widehat{\mathcal{O}(\mathfrak{N})}$ in $\widehat{B}^\bullet$. Then one has the following bijections of sets:*

$$\begin{array}{ccc} \{\textit{Eichler orders of level } \mathfrak{N}\} & & \widehat{B}^\bullet/N(\widehat{\mathcal{O}(\mathfrak{N})}) \\ \mathcal{O}' \textit{ such that } \mathcal{O}'_\mathfrak{p} = y_\mathfrak{p}^{-1}\mathcal{O}(\mathfrak{N})_\mathfrak{p}y_\mathfrak{p} & \longleftarrow\!\shortmid & (y_v)_v \in \widehat{B}^\bullet \\ \left\{\begin{array}{c}\textit{Conjugacy classes of}\\ \textit{Eichler orders of level } \mathfrak{N}\end{array}\right\} & & B^\bullet\backslash\widehat{B}^\bullet/N(\widehat{\mathcal{O}(\mathfrak{N})}) \end{array}$$

2.2 The norm isomorphisms

The cardinality of the previous double quotients can themselves be computed as class numbers of F:

Proposition 2.4. *Let $\mathfrak{N}$ be an ideal of F, let $\mathcal{O}$ be an Eichler order of level $\mathfrak{N}$. Let $F_B^\bullet$ be the group of elements of F which are of positive norms at ∞_B. Then the norm induces the bijections:*

$$n : \mathrm{Cl}^+_{\mathrm{R}}(\mathcal{O}) = B^+\backslash\widehat{B}^\bullet/\widehat{\mathcal{O}}^\bullet \longrightarrow F^+\backslash\widehat{F}^\bullet/n(\widehat{\mathcal{O}}^\bullet) \tag{2.2}$$

$$n : B^\bullet\backslash\widehat{B}^\bullet/N(\widehat{\mathcal{O}}) \longrightarrow F_B^\bullet\backslash\widehat{F}^\bullet/n\big(N(\widehat{\mathcal{O}})\big) \tag{2.3}$$

Proof We deal with the second statement, the first one being analogous (done in [Voi$_5$, Corollary 28.4.24]).

Firstly, the norm map remains well defined after quotienting on the left because by the easy way of the norm theorem, $n(B) \subset F_B$.

The surjectivity at any finite place $\mathfrak{p}$ follows from the image of the central term: $n(B_\mathfrak{p}^\bullet) = F_\mathfrak{p}^\bullet$. Let us prove this:

- if $\mathfrak{p}$ splits B it is immediate;
- if $B_\mathfrak{p}$ is a division algebra, it suffices to show that it contains a ramified quadratic extension $K/F_\mathfrak{p}$. Indeed the norm n of $B_\mathfrak{p}$ extends that of K, so this implies that:

$$n(B_\mathfrak{p}^\bullet) \supset n(K^\bullet) = F_\mathfrak{p}^\bullet.$$

  The existence of $K \subset B_\mathfrak{p}$ ramified comes from the fact that $B_\mathfrak{p}$ contains at least two quadratic subfields, and that $F_\mathfrak{p}$ has only one unique quadratic unramified extension by [Se$_0$, III.§5 th 2].

For the injectivity, notice that we are dealing with a mere map of sets. Suppose that $n(\widehat{\alpha}) = f.n(\widehat{\beta})n(h)$, with $f \in F_B$ and $h \in N(\widehat{\mathcal{O}})$. The (hard way of the) norm theorem [Vig, III.4.1] states that there exists $b \in B^\bullet$ of norm f. So up to multiplying x on the left by b, and on the right by h, one can assume that $n(\widehat{\alpha}) = n(\widehat{\beta})$.

Following [Voi$_5$, Lemma 28.3.6], let us conclude that there exists $z \in B^\bullet$ such that $\widehat{\alpha}\widehat{\mathcal{O}}^\bullet = z\widehat{\beta}\widehat{\mathcal{O}}^\bullet$. Which will be enough, $\widehat{\mathcal{O}}^\bullet$ being itself included in the normalizer $N(\widehat{\mathcal{O}})$.

Claim: There exists $z \in B^\bullet$ and $\widehat{\mu} \in \widehat{\mathcal{O}}^\bullet$ such that $\widehat{\alpha}\widehat{\beta}^{-1}\mathcal{O}' = z(\widehat{\beta}\widehat{\mu}\widehat{\beta}^{-1})$.

End of the proof: thus $\widehat{\alpha}\widehat{\mathcal{O}} = z\widehat{\beta}\widehat{\mu}\widehat{\mathcal{O}} = z\widehat{\beta}\widehat{\mathcal{O}}$.

Proof of the claim: consider the Eichler order $\mathcal{O}' = B \cap \widehat{\beta}\widehat{\mathcal{O}}\widehat{\beta}^{-1}$, $\widehat{B}^1$ the group of idèles of norm one, and B^1 seen in $\widehat{B}^1$ by the diagonal embedding. The subgroup $\widehat{\mathcal{O}'}^\bullet$ being (compact) open in the group of idèles $\widehat{B}^\bullet$ (see [Vig, Définition p59 2)]), the strong approximation theorem ([Vig, III.4.3]) states that B^1 is dense in $\widehat{B}^1$. One thus has the open cover:

$$B^1\widehat{\mathcal{O}'}^\bullet \supset \widehat{B}^1 \ .$$

The element $\widehat{\alpha}\widehat{\beta}^{-1}$ being of norm one, the inclusion above implies the existence of $z \in B^1$ and of $\widehat{\mu}' \in \widehat{\mathcal{O}'}^\bullet$ such that $\widehat{\alpha}\widehat{\beta}^{-1} = z\widehat{\mu}'$. Conclude with $\widehat{\mu} = \widehat{\beta}^{-1}\widehat{\mu}'\widehat{\beta}$. □

Corollary 2.5 ([Vig, exercice III.5.5] or [Sij$_1$, 2.6.1]). *Under the same assumptions, if h^+ is odd, then there is only one conjugacy class of Eichler orders of level $\mathfrak{N}$ in B.*

Firstly, the RHS of the isomorphism (2.3) is a quotient of $\mathrm{Cl}(\infty_B)$, itself quotient of $\mathrm{Cl}(\infty_{\mathbf{R}})$. Thus its cardinality divides h^+. Finally we claim that the cardinality of the RHS is a power of two, which implies the conclusion. The claim comes from the fact that $\widehat{F}^\bullet \subset N(\widehat{\mathcal{O}})$, hence $\widehat{F}^{\bullet 2} \subset n(N(\widehat{\mathcal{O}}))$.

3 Totally positive units

If $\mathcal{O}$ is an Eichler order, then its local description implies that $n(\widehat{\mathcal{O}}) = \widehat{\mathbf{Z}_F}$. The leap from local to global then results from the two key theorems of quaternions algebras, Eichler's norm theorem and the strong approximation theorem:

Theorem 3.1 ([Voi$_5$, Corollaries 28.4.20 & 31.1.11][1]). *Let $\mathcal{O}$ be an Eichler order, and $\mathbf{Z}_{F,B}$ the integers of F that are positive at the ramified places of B. Then*

$$n(\mathcal{O}) = \mathbf{Z}_{F,B}.$$

Let $\mathcal{O}$ be an Eichler order and $\mathcal{O}^+$ (respectively $\mathbf{Z}_F^+$) the subgroups of units of totally positive norm. Let $PB = B^\bullet/F^\bullet$ and $P\mathcal{O}^+ = F^\bullet\mathcal{O}^+/F^\bullet$, (respectively $P\mathcal{O}^1 = F^\bullet\mathcal{O}^1/F^\bullet$) be the images in PB of the groups $\mathcal{O}^+$ and $\mathcal{O}^1$.

Proposition 3.2 ([Sij$_1$, Prop 3.2.1 modified]). *The reduced norm induces an isomorphism of quotient groups*

$$\left|\frac{P\mathcal{O}^+}{P\mathcal{O}^1}\right| \xrightarrow{\sim} \frac{\mathbf{Z}_F^+}{\mathbf{Z}_F^{\bullet 2}}$$

If furthermore F is a totally real field, then the cardinality of this quotient group is equal to the narrow class number h^+.

Proof Let recall that if G is a group, $K \lhd G$ a normal subgroup and $H \subset G$ any subgroup, then the inclusion $H \hookrightarrow HK$ induces the isomorphism of quotient groups $H/H \cap K \xrightarrow{\sim} HK/K$.

[1] See also [Vig, III.5.9]. But beware that the choice of $zu \in \mathcal{O}$, in the proof of III.5.8, is not obvious unless all Eichler orders are conjugate.

One considers the subgroups $H = \mathcal{O}^+$ (respectively $\mathcal{O}^1$) of $G = B^\bullet$. Their elements are integral over $\mathbf{Z}_F \subset F$, so the intersection of these subgroups with the normal subgroup $K = F^\bullet$ is equal to $\mathcal{O}^+ \cap \mathbf{Z}_F^\bullet$ (respectively $\mathcal{O}^1 \cap \mathbf{Z}_F^\bullet$). One deduces the isomorphisms of quotient groups:

$$PO^+ = \frac{F^\bullet \mathcal{O}^+}{F^\bullet} \cong \frac{\mathcal{O}^+}{\mathcal{O}^+ \cap \mathbf{Z}_F^\bullet} \cong \frac{\mathcal{O}^+ \mathbf{Z}_F^\bullet}{\mathbf{Z}_F^\bullet}$$

$$PO^1 = \frac{F^\bullet \mathcal{O}^1}{F^\bullet} \cong \frac{\mathcal{O}^1}{\mathcal{O}^1 \cap \mathbf{Z}_F^\bullet} \cong \frac{\mathcal{O}^1 \mathbf{Z}_F^\bullet}{\mathbf{Z}_F^\bullet}$$

that enable to express the LHS with the isomorphism:

$$\frac{P\mathcal{O}^+}{P\mathcal{O}^1} \xrightarrow{\sim} \frac{\mathcal{O}^+ \mathbf{Z}_F^\bullet}{\mathcal{O}^1 \mathbf{Z}_F^\bullet} \tag{3.1}$$

Let $\mathcal{O}^{(2)}$ be the group of units whose norm is in $\mathbf{Z}_F^{\bullet 2}$.

Claim: the natural surjection:

$$\mathcal{O}^+ \mathbf{Z}_F^\bullet \twoheadrightarrow \frac{\mathcal{O}^+ \mathbf{Z}_F^\bullet}{\mathcal{O}^1 \mathbf{Z}_F^\bullet}$$

has kernel $\mathcal{O}^{(2)} \mathbf{Z}_F^\bullet$. Proof :

- let $x = o.r \in \mathcal{O}^+ \mathbf{Z}_F^\bullet$ be an element of the kernel, with $o \in \mathcal{O}^1$ and $r \in \mathbf{Z}_F^\bullet$. Then its norm is in $\mathbf{Z}_F^{\bullet 2}$;
- conversely if $n(x) = z^2$ is a square in $\mathbf{Z}_F^\bullet$, then the element $x.1/z$ is both integral over $\mathbf{Z}_F$ (z being invertible in $\mathbf{Z}_F$) and of norm one. Thus the class of x in $\mathcal{O}^+ \mathbf{Z}_F^\bullet / \mathbf{Z}_F^\bullet$ is in $\mathcal{O}^1 \mathbf{Z}_F^\bullet / \mathbf{Z}_F^\bullet$.

From the claim and the previous lemma, the norm induces the isomorphism:

$$\frac{\mathcal{O}^+ \mathbf{Z}_F^\bullet}{\mathcal{O}^{(2)} \mathbf{Z}_F^\bullet} \xrightarrow[n]{\sim} \frac{\mathbf{Z}_F^+}{\mathbf{Z}_F^{\bullet 2}}, \tag{‡}$$

which proves the first statement.

For the last statement, let us show the equality of cardinalities:

$$\left| \frac{\mathbf{Z}_F^+}{\mathbf{Z}_F^{\bullet 2}} \right| = h^+ = |\mathrm{Ker}\big(\mathrm{Cl}(\infty) \to \mathrm{Cl}(1)\big)|$$

Firstly, the kernel of the projection $\mathrm{Cl}(\infty) \to \mathrm{Cl}(1)$, is equal to the set of the classes in $\mathrm{Cl}(\infty)$ of nonzero scalars $(F^\bullet)$. Letting r_1 be the number of real embeddings of F, a set of representative of these classes consists in a set of elements $(b_i)_i$ of $F^\bullet$, whose r_1-uples of signs $((--+\cdots+-))$ run over all the possible combinations. But the real places of F induce nonequivalent norms. Thus by the weak approximation theorem, the $(-1)^{r_1}$ possible combinations of signs are all reachable. Hence the kernel map:

$$\varphi : \{\pm 1\}^{r_1} \to \mathrm{Cl}(\infty),$$

that sends an r_1-uple $(--+\cdots+-)$ on the class $\overline{(b_i)}$ of the representative b_i that takes these signs.

Consider now the surjection

$$f : \frac{\mathbf{Z}_F^\bullet}{\mathbf{Z}_F^{\bullet 2}} \twoheadrightarrow \mathrm{Ker}\varphi \in \{\pm 1\}^{r_1}$$

in the previous kernel, that sends a unit on the r_1-uple of its signs. The kernel of f is equal to the generators of ideals with trivial class. I.e. to the (classes modulo $Z_F^{\bullet 2}$ of) totally positive units. Hence the exact sequence:

$$1 \to \frac{\mathbf{Z}_F^+}{\mathbf{Z}_F^{\bullet 2}} \xrightarrow{f} \frac{\mathbf{Z}_F^\bullet}{\mathbf{Z}_F^{\bullet 2}} \to \{\pm 1\}^{r_1} \to \mathrm{Ker}\left(\mathrm{Cl}(\infty) \to \mathrm{Cl}(1)\right) \to 1$$

One can conclude noticing that the two central terms of the sequence have the same cardinality[2] . Indeed by Dirichlet's units theorem:

$$\mathbf{Z}_F^\bullet / \mathbf{Z}_{F,\mathrm{tors}}^\bullet \cong \mathbf{Z}^{r_1 - 1},$$

the additional factor two needed coming from the equality $|\mathbf{Z}_{F,\mathrm{tors}}^\bullet / \mathbf{Z}_F^{\bullet 2}| = 2$. □

[2] In the case of a general number field F, letting $\mathbf{Z}_{F,\mathbf{R}}^\bullet$ be the totally real units, one still has $\left|\mathbf{Z}_{F,\mathbf{R}}^\bullet / \mathbf{Z}_{F,\mathbf{R}}^{\bullet 2}\right| = 2^{r_1}$. Indeed let i be the (logarithmic) embedding of $\mathbf{Z}_F^\bullet / \mathbf{Z}_{F,\mathrm{tors}}^\bullet$ onto a lattice in $\mathbf{R}^{r_1+r_2-1}$ (the vector subspace of elements whose sum of coordinates is zero). Let $H_{\mathbf{R}}$ be the vector subspace $\mathbf{R}^{r_1+r_2-1}$ of dimension $r_1 - 1$ of elements whose complex coordinates are zero. Then $\mathbf{Z}_{F,\mathbf{R}}^\bullet / \mathbf{Z}_{F,\mathrm{tors}}^\bullet$ is equal to the preimage of the following lattice of H: $i(\mathbf{Z}_F^\bullet / \mathbf{Z}_{F,\mathrm{tors}}^\bullet) \cap H$. In conclusion, the only roots of unity in $\mathbf{Z}_{F,\mathbf{R}}^\bullet$ being $\{\pm 1\}$, the cardinality of the quotient $\mathbf{Z}_{F,\mathbf{R}}^\bullet / \mathbf{Z}_{F,\mathbf{R}}^{\bullet 2}$ is equal to 2^{r_1}

4 Atkin–Lehner

4.1 The group of two-sided ideals

Let $\mathcal{O}$ be a $\mathbf{Z}_F$-order, one deduces from equation (2.1) that

$$N_{B^\bullet}(\mathcal{O})/(F^\bullet \mathcal{O}^\bullet) \xrightarrow{\sim} \mathrm{PIdl}(\mathcal{O})/\mathrm{PIdl}(R)\,. \tag{4.1}$$

Let us now describe the group of invertible two-sided ideals Idl when $\mathcal{O}$ is an Eichler order of level $\mathfrak{N}$. Let $\mathfrak{p}$ be a finite place, π an uniformizer of the discrete valuation of $\mathbf{Z}_{F,\mathfrak{p}}$ and $\mathcal{O}_\mathfrak{p}$ the completion at $\mathfrak{p}$. Recall that all two-sided invertible $\mathcal{O}_\mathfrak{p}$-ideals are principal. They are as follows:

- If $\boxed{\mathfrak{p} \nmid \mathfrak{N}}$ then one has the bijection ([Voi$_1$, (23.3.20)]):

  $$\begin{array}{ccc} \{\text{Prime two-sided invertible } \mathcal{O}_\mathfrak{p}\text{-ideals}\} & & \{\text{Prime ideals of } \mathbf{Z}_F\} \\ P & \longmapsto & P \cap \mathbf{Z}_F \end{array}$$

  - if $\mathfrak{p} \nmid \mathfrak{D}$: then $P = \mathfrak{p}\mathcal{O}_\mathfrak{p}$;
  - if $\mathfrak{p}|\mathfrak{D}$: then one has the two-sided prime ideal P with $P^2 = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ ("$\mathfrak{p}\mathcal{O}_\mathfrak{p}$ ramifies").

- For $\boxed{\mathfrak{p}^e || \mathfrak{N}}$ (see [Voi$_5$, Proposition 23.4.11]), one has $\mathcal{O}_\mathfrak{p} = \mathrm{M}_2(\mathbf{Z}_{F,\mathfrak{p}})$. Consider then $\omega_e = \begin{pmatrix} 0 & 1 \\ \pi_\mathfrak{p}^e & 0 \end{pmatrix}$: the group $\mathrm{Idl}(\mathcal{O}_\mathfrak{p})$ is abelian, generated by the –non obvious– two-sided ideal $J = \mathcal{O}_\mathfrak{p}\omega = \omega\mathcal{O}_\mathfrak{p}$ and $\mathfrak{p}\mathcal{O}_\mathfrak{p}$. With the single relation $J^2 = \mathfrak{p}^e\mathcal{O}_\mathfrak{p}$.

In particular, the previous classification and Lemma 2.1 imply the following exact sequence of abelian groups for the global Eichler order $\mathcal{O}$:

$$0 \to \mathrm{Idl}(\mathbf{Z}_F) \to \mathrm{Idl}(\mathcal{O}) \to \prod_{\mathfrak{p}|\mathfrak{D}\mathfrak{N}} \mathbf{Z}/2\mathbf{Z} \tag{4.2}$$

4.2 The groups of Atkin–Lehner involutions

Let again $\mathcal{O}$ be an Eichler order of level $\mathfrak{N}$. The following group is studied in [Rot, §4.1] (where it is shown to provide nearly all the automorphisms of the Shimura curve $X_0(\mathfrak{N})$):

$$W^1 = N_{B^+}(\mathcal{O})/(F^\bullet \mathcal{O}^1) \tag{4.3}$$

Proposition 4.1. *Assume that the narrow class number is one*[3]*. Then*

$$W^1 \cong \prod_{\mathfrak{p}|\mathfrak{D}\mathfrak{N}} \mathbf{Z}/2\mathbf{Z} \tag{4.4}$$

Proof Proposition 2.4.(2.2) implies in particular that every two-sided ideal is generated by a totally positive element. So the LHS of bijection (4.1) restricts to :

$$N_{B^+}(\mathcal{O})/(F^\bullet \mathcal{O}^+) \xrightarrow{\sim} \mathrm{PIdl}(\mathcal{O})/\mathrm{PIdl}(R)\,. \tag{4.5}$$

Next, $\mathcal{O}^+$ being equal to $\mathcal{O}^1$ by Proposition 3.2, the LHS is equal to W^1. Finally, every two-sided ideal being principal, the RHS is described by (4.2). □

5 Indices of congruence subgroups

5.1 Definitions

It is assumed for the commodity of the exposition that the (possibly non unique) split infinite place of B is *real*.

We fix in this section $\mathcal{O}$ a maximal order of B and $\mathfrak{N} = \prod_i \mathfrak{p}_i^{e_i}$ any ideal of F, *prime to the finite discriminant* $\mathfrak{D}$ of B, along with its decomposition in primes. For each prime $\mathfrak{p} = \mathfrak{p}_i$ dividing $\mathfrak{N}$, *choose* $\iota_\mathfrak{p}$ an embedding of B into its $\mathfrak{p}$-adic completion $B_\mathfrak{p} = \mathrm{M}_2(F_\mathfrak{p})$. The completion $\mathcal{O}_\mathfrak{p}$ of $\mathcal{O}$ is an order conjugate to the integral matrices $\mathrm{M}_2(\mathbf{Z}_{F,\mathfrak{p}})$. One then defines the *standard Eichler order* $\mathcal{O}(\mathfrak{N}) \subset \mathcal{O}$ of level $\mathfrak{N}$, equal to the elements $x \in \mathcal{O}$ such that their image in $\mathrm{M}_2(F_{\mathfrak{p}_i})$ is upper-triangular modulo $\mathfrak{p}^{e_i}$ for all i.

Let $\iota_v : F \hookrightarrow F_v = \mathbf{R}$ be the corresponding embedding. Choose $\iota_{B,v} : B \hookrightarrow \mathrm{M}_2(\mathbf{R})$ an extension of ι_v to B.

The groups $\mathcal{O}(\mathfrak{N})^1$ of units of norm one, and $\mathcal{O}(\mathfrak{N})^+$ of units of totally positive norm, are sent isomorphically by $\iota_{B,v}$ onto subgroups of $\mathrm{SL}_2(\mathbf{R})$ and $\mathrm{GL}_2^+(\mathbf{R})$.

Let $\bar{\iota} : B^+ \to \mathrm{PGL}_2(\mathbf{R})$ be the embedding $\iota_{B,v}$ followed by the quotient modulo scalar multiplications. Define the following subgroups of $\mathrm{PSL}_2(\mathbf{R})$:

[3] In the general case, the normalizer group $W = N_{B^\bullet}(\mathcal{O})/(F^\bullet \mathcal{O}^\bullet)$ is described correctly [Voi$_5$, Corollary 28.7.21]. The error in [Vig, Exercice III.5.4] was firstly fixed by [LV, Proposition 1.17], also described in detail in [Duc, Proposition III.3.14].

- the congruence subgroups of level $\mathfrak{N}$:

$$\Gamma_0(\mathfrak{N}) = \iota_{B,v}\big(\mathcal{O}^1(\mathfrak{N})\big) \tag{5.1}$$
$$\Gamma_0^+(\mathfrak{N}) = \iota_{B,v}\big(\mathcal{O}^+(\mathfrak{N})\big)\ ; \tag{5.2}$$

- the principal congruence groups –which pairwise coincide with the previous groups when $\mathfrak{N} = 1$:

$$\Gamma(\mathfrak{N}) = \iota_{B,v}\{\gamma \in \mathcal{O}^1, \gamma - 1 \in \mathfrak{N}\mathcal{O}^1\} \tag{5.3}$$
$$\Gamma^+(\mathfrak{N}) = \iota_{B,v}\{\gamma \in \mathcal{O}^+, \gamma - 1 \in \mathfrak{N}\mathcal{O}^+\}\ ; \tag{5.4}$$

- the kernel of the natural map (see also (5.6) below):

$$\Gamma'(\mathfrak{N}) = \mathrm{Ker}\big\{\Gamma(1) \longrightarrow \mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{N}\mathbf{Z}_F)\big\} \tag{5.5}$$

- and for every group $\Gamma \in \mathrm{SL}_2(\mathbf{R})$, define its image ([Miy, p 106]):

$$\overline{\Gamma} \cong P\Gamma = \Gamma/Z(\Gamma)$$

in $\mathrm{PSL}_2(\mathbf{R})$ the group of direct holomorphic automorphisms of the upper half plane.

In conclusion one has the inclusions:

$$\Gamma(\mathfrak{N}) \lhd \Gamma'(\mathfrak{N}) \lhd \Gamma_0(\mathfrak{N}) \subset \Gamma_0(1),$$

the two LHS groups being normal in everything because they are kernels (of the natural morphisms in $\mathrm{SL}_2(\mathfrak{N})$ and in $\mathrm{PSL}_2(\mathfrak{N})$). One of the purpose of this section is that, unlike for the classical modular groups, $\overline{\Gamma'(\mathfrak{N})}$ can be strictly bigger than $\overline{\Gamma(\mathfrak{N})}$: see Proposition 5.7.

5.2 Reduction and some cardinalities

Prop-Def 5.1 ([Be])**.** Let R be a finite local ring and $\mathfrak{p}$ its single maximal ideal. Define the set

$$\mathbf{P}^1(R) = \{(u, v),\ uR + vR = (1)\} / \sim$$

Where $\sim$ is the equivalence relation of simultaneous multiplication by an invertible $\lambda \in R^\bullet$.

Then in each couple, either u or v is invertible. Thus $\mathbf{P}^1(R)$ is the disjunct union of the two following subsets of classes :

(i) $\{(1,\beta),\ \beta \in R\}$
(ii) $\{(\alpha,1),\ \alpha \in R\backslash R^\bullet = \mathfrak{p}\}$

Proof Claim: in every couple (u,v), either u or v is invertible. Proof: if not, then they both would be in the maximal ideal $\mathfrak{p}$ so the ideal generated by u and v would be contained in $\mathfrak{p}$. The classification follows. □

Lemma 5.2. *The group* $\mathrm{PSL}_2(R)$ *acts transitively on* $\mathbf{P}^1(R)$.
The fixator subgroup of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *is* $\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{PSL}_2(R). \right\}$.
The following subgroup acts transitively on the following subset (ii) :

$$\Gamma_0(\mathfrak{p}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(R),\ c \in \mathfrak{p}. \right\}$$

Lemma 5.3. *Let* R *be a Dedekind domain and* $\mathfrak{p}$ *a maximal ideal of norm* $q = N(\mathfrak{p}) = |R/\mathfrak{p}|$. *Let* k *be a strictly positive integer, consider the finite local ring* $\overline{R} = R/\mathfrak{p}^k$, *its maximal ideal* $\overline{\mathfrak{p}} = \mathfrak{p}/\mathfrak{p}^k$ *is nilpotent of order* k. *Then:*

(i) $\left|\overline{\mathfrak{p}}\right| = q^{k-1}$ *and* $\left|\overline{R}\right| = q^k$

(ii) $\left|\mathrm{GL}_n(\overline{R})\right| = q^{n^2(k-1)}(q^n-1)\dots(q^n-q^{n-1})$

(iii) $\left|\mathrm{SL}_n(\overline{R})\right| = \left|\mathrm{GL}_n(R)\right|/(q^k-q^{k-1})$

(iv) $\mathrm{SL}_n(R/\mathfrak{N}) \cong \prod_{\mathfrak{p}} \mathrm{SL}_n(R/\mathfrak{p}^{e_{\mathfrak{p}}})$ *where* $\mathfrak{N} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$

(v) $\left|\mathrm{PSL}_2(\overline{R})\right| = \boxed{\text{if } \mathfrak{p} \nmid (2)}$: $\left|\mathrm{SL}_2(\overline{R})\right|/2$, $\boxed{\text{if } \mathfrak{p}|(2) \text{ and } k=2}$: $\left|\mathrm{SL}_2(\overline{R})\right|/q$.

Proof [(i)] The existence of a $\mathfrak{p}$-adic valuation yields an isomorphism $R/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^i/\mathfrak{p}^{i+1}$ for all i. Thus the nested quotients $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ are all of cardinality q. Composing their indices gives the two assertions.

[(ii)] For all $i \leq k-1$, the reduction map $\mathrm{GL}_n(\overline{R}/\mathfrak{p}^{i+1}) \to \mathrm{GL}_n(\overline{R}/\mathfrak{p}^i)$ is surjective. The kernel is equal to the subset of matrices congruent to the identity modulo $\overline{\mathfrak{p}^i} = \mathfrak{p}^i/\mathfrak{p}^{i+1}$. E.g. for $n=2$:

$$\left\{ \begin{pmatrix} 1+\overline{\mathfrak{p}^i} & \overline{\mathfrak{p}^i} \\ \overline{\mathfrak{p}^i} & 1+\overline{\mathfrak{p}^i} \end{pmatrix} \right\} \subset \mathrm{GL}_2(\overline{R}/\mathfrak{p}^{i+1}),$$

where all the ideals $\overline{\mathfrak{p}^i}$ are of cardinality q as seen in (i). At last the cardinality of the linear group over the field $R/\mathfrak{p}$ with q elements is classical.

[(iii)] The determinant map $\mathrm{GL}_n(\overline{R}) \to \overline{R}^*$ is surjective with kernel the subgroup $\mathrm{SL}_n(\overline{R})$. But $\left|\overline{R}^*\right| = \left|\overline{R}\right| - \left|\overline{\mathfrak{p}}\right|$

[(iv)] Follows from the Chinese remainder (Sun Tsu) theorem argument of [Miy, Lemma 4.2.3]

[(v)] If $\boxed{\mathfrak{p} \nmid (2)}$, then the polynomial $f = X^2 - 1$ has exactly two distinct roots (1 and -1) and a nonzero derivative in $R/\mathfrak{p}$. Thus by successive Hensel liftings, it has also exactly two distinct zeros in $\overline{R} = R/\mathfrak{p}^k$. Now if $\boxed{\mathfrak{p}|(2) \text{ and } k = 2}$, then let λ be an element of $\overline{R}$ such that $(1+\lambda)^2 = 1$. This implies that $\lambda^2 = -2\lambda$, which belongs to the maximal ideal $\overline{\mathfrak{p}}$. $\overline{\mathfrak{p}}$ being prime, λ itself belongs to $\overline{\mathfrak{p}}$. But then $\lambda^2 = -2\lambda \in \overline{\mathfrak{p}}^2 = 0$. Conclusion: any $\lambda \in \overline{\mathfrak{p}}$ suits, this set being of cardinality q. □

The link with congruence subgroups is first seen from the natural morphism of rings:

$$\mathcal{O}/\mathfrak{N}\mathcal{O} \xrightarrow{\sim} \mathrm{M}_2(\mathbf{Z}_F/\mathfrak{N}) \tag{5.6}$$

of reduction modulo $\mathfrak{N}$. Let us define it and verify in the same time that it is an isomorphism (although we won't need this actually). Indeed by the Chinese remainder (Sun Tsu) theorem, it suffices to prove it for $\mathfrak{N} = \mathfrak{p}^k$ a prime power. Then, recall that completion at $\mathfrak{p}$ commutes with quotienting by $\mathfrak{p}^k$. Finally:

$$\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^k\mathcal{O}_p = \mathrm{M}_2(\mathbf{Z}_{F,\mathfrak{p}}/\mathfrak{p}^k) = \mathrm{M}_2(\mathbf{Z}_F/\mathfrak{p}^k)\,.$$

Now, the following (hard) result shows that congruence (sub)groups surject onto their $\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{N})$ counterparts:

Proposition 5.4. *Let $\mathfrak{N}$ be an ideal prime to the discriminant $\mathfrak{D}$, then*

$$\Gamma(1)/\Gamma'(\mathfrak{N}) \xrightarrow{\sim} \mathrm{SL}_2(\mathbf{Z}_F/\mathfrak{N})\ ; \tag{5.7}$$

Proof Let us restrict the isomorphism (5.6) to the units of norm one to show (5.7). $\mathbf{Z}_F$ being a Dedekind domain, [Voi$_5$, Proposition 28.2.5] states the surjection:

$$\mathrm{SL}_2(\mathbf{Z}_F) \twoheadrightarrow \mathrm{SL}_2(\mathbf{Z}_F/\mathfrak{N})$$

So considering $\widetilde{\gamma} \in \mathrm{SL}_2(\mathbf{Z}_F/\mathfrak{N})$ and γ a lifting, the strong approximation states that there exists $b_1 \in B^1$ such that:

- at $\mathfrak{p} \nmid \mathfrak{N}$: $|b_1 - 1| \in \mathfrak{p}$, so b_1 is integral in $\mathcal{O}_{\mathfrak{p}}$;

- at $\mathfrak{p}$, $\mathfrak{p}^{e_\mathfrak{p}}||\mathfrak{N}$: $|b_1-\gamma|_\mathfrak{p} \in \mathfrak{p}^{e_\mathfrak{p}+1}$, so $b_1 \equiv \gamma \bmod \mathfrak{p}^{e_\mathfrak{p}}$ and b_1 is integral in $\mathcal{O}_\mathfrak{p}$.

Thus $b_1 \in \mathcal{O}^1$ and reduces to $\widetilde{\gamma}$ modulo $\mathfrak{N}$. □

This result enables one the recover in particular the *local* indices of inclusion of the units of norm one of Eichler orders, computed with Lemmas 5.2 and 5.3.(i):

$$[P\mathcal{O}^1_\mathfrak{p} : P\mathcal{O}(\mathfrak{p}^k)^1_\mathfrak{p}] = \left|\mathbf{P}^1(\mathbf{Z}_F/\mathfrak{p}^k)\right| = |\mathbf{Z}_F/\mathfrak{p}^k| + |\mathfrak{p}/\mathfrak{p}^k| = q^{k-1}(q+1). \tag{5.8}$$

5.3 Indices

Passing to the global indices requires the classical combination of Eichler's norms theorem (Theorem 3.1) and of the strong approximation theorem for quaternion algebras with a split real place:[4]

Proposition 5.5 ([Sij$_1$, Prop 2.5.3 (i)]). *Let $K' \subseteq K$ be two compact open subgroups of $\widehat{B}^\bullet$, $K^1_B = K \cap B^1$ and likewise $K^+_B = K \cap B^+$. Then:*

$$[K^1_B : K'^1_B] = \frac{[K:K']}{[n(K):n(K')]} \tag{5.9}$$

$$[K^+_B : K'^+_B] = \frac{h[K:K']}{[n(K):n(K')]}, \tag{5.10}$$

Where

$$h = \left|\frac{n(K) \cap \mathbf{Z}_{F,+}}{n(K')}\right|$$

And fortunately in the case of congruence groups from Eichler orders, the following corollary implies that the local and global indices coincide. Set the following functions [Duc, top of page 52], defined on the ideals of $\mathbf{Z}_F$ (noted here $\mathfrak{N}$ and $\mathfrak{D}$) and taking integer values :

$$\Phi(\mathfrak{D}) = |(\mathbf{Z}_F/\mathfrak{D})^\bullet| = N(\mathfrak{D}) \prod_{\mathfrak{p}|\mathfrak{D}} \left(1 - \frac{1}{N(\mathfrak{p})}\right) \tag{5.11}$$

$$\Psi(\mathfrak{N}) = N(\mathfrak{N}) \prod_{\mathfrak{p}|\mathfrak{N}} \left(1 + \frac{1}{N(\mathfrak{p})}\right) \tag{5.12}$$

[4] Is this additional argument really needed ? Indeed one can quotient everything by $\Gamma'(\mathfrak{N})$ and, thanks to Proposition 5.4, work with congruence subgroups of $\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{N})$

Corollary 5.6 ([Sij$_1$, Corollary 2.5.4]). *Let $\mathfrak{p}$ be a prime ideal of F of norm q, $\mathfrak{N}$ an ideal prime to the discriminant $\mathfrak{D}$ and $k \geq 1$, then:*

$$[\overline{\Gamma(1)} : \overline{\Gamma_0(\mathfrak{p}^k)}] = [\overline{\Gamma^+(1)} : \overline{\Gamma_0^+(\mathfrak{p}^k)}] = q^{k-1}(q+1)\ ; \tag{5.13}$$

$$[\overline{\Gamma(1)} : \overline{\Gamma_0(\mathfrak{N})}] = [\overline{\Gamma^+(1)} : \overline{\Gamma_0^+(\mathfrak{N})}] = \Psi(\mathfrak{N}) \tag{5.14}$$

Proof For both the indices $[\Gamma(1) : \Gamma_0(\mathfrak{p}^k)]$ and $[\Gamma^+(1) : \Gamma_0^+(\mathfrak{p}^k)]$, consider the compact open subgroups $K = \widehat{\mathcal{O}}^\bullet$ and $K' = \widehat{\mathcal{O}(\mathfrak{p}^k)}^\bullet$. The numerators of formulas (5.9) and (5.10) contain the index $[K : K']$. It is equal to the product of the local indices $[K_\mathfrak{p} : K'_\mathfrak{p}]$. They are all equal to one except at $\mathfrak{p}$, where it is $q^{k-1}(q+1)$ by (5.8).

Then the denominator $[n(K) : n(K')]$ equals one, by the local description of Eichler orders.

Finally the factor h equals one because it is a subgroup of the one-element group $[n(K) : n(K')]$.

In conclusion, $[\mathcal{O}^1 : \mathcal{O}(\mathfrak{p}^k)^1] = [\mathcal{O}^+ : \mathcal{O}(\mathfrak{p}^k)^+] = q^{k-1}(q+1)$. Finally, observe that by Theorem 3.1, the two groups appearing in each index have the same center: $\mathbf{Z}_F^1$ (respectively $\mathbf{Z}_F^+$). So the projective indices $[\overline{\Gamma(1)} : \overline{\Gamma_0(\mathfrak{p}^k)}]$ and $[\overline{\Gamma^+(1)} : \overline{\Gamma_0^+(\mathfrak{p}^k)}]$ are equal to the previous global indices.

Equation (5.14) results from the same argument, considering all the primes dividing $\mathfrak{N}$. □

Proposition 5.7. *Let $\mathfrak{p}$ be a prime ideal prime to the discriminant $\mathfrak{D}$. Then:*

$$[\overline{\Gamma'(\mathfrak{p}^k)} : \overline{\Gamma(\mathfrak{p}^k)}] = \boxed{\textit{if } \mathfrak{p} \nmid (2)} : 1 \tag{5.15}$$

$$\boxed{\textit{if } k = 2, \mathfrak{p}|(2) \textit{ and } \mathfrak{p}^2 \nmid (2)} : N(\mathfrak{p})/2 \tag{5.16}$$

$$\boxed{\textit{if } k = 2, \mathfrak{p}|(2) \textit{ and } \mathfrak{p}^2|(2)} : N(\mathfrak{p}) \tag{5.17}$$

Proof Firstly, if $\mathfrak{p} \nmid (2)$, then $\Gamma(\mathfrak{N}) = \Gamma'(\mathfrak{N})$ by the first case of the proof of Lemma 5.3 (v). So the projectivized groups also coincide.

Then if $\mathfrak{p}|(2)$ and $k = 2$, the last case of the proof of Lemma 5.3 (v) shows that:

$$\Gamma'(\mathfrak{p}^2) \subset \left\{ M \in \mathrm{SL}_2(\mathfrak{p}^2),\ M \equiv \begin{pmatrix} 1+\lambda & 0 \\ 0 & 1+\lambda \end{pmatrix} \bmod \mathfrak{p}^2,\ \lambda \in \mathfrak{p} \right\}, \tag{5.18}$$

so $[\Gamma'(\mathfrak{p}^2) : \Gamma(\mathfrak{p}^2)]$. The first subcase is when $\mathfrak{p}^2|(2)$, so that $\Gamma(\mathfrak{p}^2)$ also contains $-\mathrm{Id}$. In which case the projectivized indices are preserved. The other subcase is when this does not hold, so only $\Gamma'(\mathfrak{p}^2)$ contains $-\mathrm{Id}$. □

Chapter IV

A dense family of Riemann surfaces

The conventions are those laid in §III.1.2, and in §III.5.1 for the congruence subgroups. In particular $\mathcal{O}$ is a maximal order.

In addition it is assumed that the quaternion algebra B is a *field* and that *the split real place v is unique*.

1 Arithmetic groups

Theorem 1.1 ([Vig, IV 1.1 (1)]). *The image $\iota_{B,v}\big(\Gamma(\mathfrak{N})\big)$ is a discrete subgroup of $\mathrm{SL}_2(\mathbf{R})$. It is cocompact if and only if B is a division algebra*[1].

Definition 1.2 ([Vig, IV.1 5]). A subgroup of $\mathrm{SL}_2(\mathbf{R})$ which is commensurable to such a group $\iota_{B,v}\big(\Gamma(\mathfrak{N})\big)$ is called an *arithmetic group*.

[1] The reference states a second property in the case where B would have at least two infinite places. But the proof depends on the following general claim which I am not sure of. The second property would imply this very strong statement: suppose there are exactly two split infinite places (say v and w). Then the image $\iota_{B,v}(\mathcal{O}^1)$ (a priori a discrete group !) is dense in $\mathrm{SL}_2(\mathbf{R})$.

[Claim : Consider four topological subgroups of the ideles $B^1_{\mathbf{A}}$: (i) $G'' = B^1_w = (\mathrm{SL}_2)_w$ (the idelic factor at w). (ii) $U'(\widehat{=}G'.C)$, with component 1 at w, (iii) $\mathcal{O}^1$ and (iv) B^1_F. Suppose that $B^1_{\mathbf{A}} = B^1_F U$ and $B^1_F \cap U = \mathcal{O}^1$ (so that $B^1_A/B^1_F = U/\mathcal{O}^1$). The assumption made is that ("D'après III.4.3 : (2).."): $G''\mathcal{O}^1$ is dense in $U = U'G''$. From this the author deduces that (p105, "(2) l'image de..."): the projection of $\mathcal{O}^1$ is dense in U'.
But actually I can only deduce that $U \cap B^1_F G''$ is dense in U.]

Counterexample 1.3. Consider the rational non-division quaternion algebra $M_2(\mathbf{Q})$ (with discriminant 1). The unique class of maximal orders is $\mathcal{O} = M_2(\mathbf{Z})$, and the group of units $\mathcal{O}^1 = \mathrm{SL}_2(\mathbf{Z})$ acts on $\mathcal{H}$ via $\mathrm{PSL}_2(\mathbf{Z})$, which is the -non compact- triangle group $(2, 3, \infty)$

The following general theorems then imply that the previous groups have a bounded fundamental domain, framed by a finite number of arc of circles, and without vertices on the real line :

Proposition 1.4. *Let* Γ *be a subgroup of* $\mathrm{PSL}_2(\mathbf{R})$.

- Γ *is discrete if and only if it acts discontinuously on the upper-half plane* $\mathcal{H}$. Γ *is then called a* Fuchsian group.
- *[Kat, 4.1.1 and proof of 4.5.1 & 4.5.2]* Γ *is of finite covolume if and only if: every Dirichlet fundamental domain has a finite number of sides and no side included in* $\mathbf{P}^1_{\mathbf{R}}$. Γ *is then called a* Fuchsian group of the first kind.
- *[Kat, Cor 4.2.7] Let* Γ *be a* Fuchsian group of the first kind, *one says that* Γ *is* cocompact *if and only if* $\Gamma\backslash\mathcal{H}$ *is compact. This is also equivalent to the fact that (i) every Dirichlet domain is both of finite area, and (ii)* Γ *has no parabolic element.*

Definition 1.5 ([Kat, Formula (4.3.4)])**.** Let Γ be a Fuchsian group of the first kind. The *signature* of Γ is the data $(g; e_1, \ldots, e_r; s)$ of: the *genus* g of the quotient $\Gamma\backslash\mathcal{H}$, the *orders* e_i of the r inequivalent elliptic points and if any, the number s of parabolic points.

Let us see how to determine the signature of Γ a cocompact Fuchsian group of the first kind. An important case for this work is :

Prop-Def 1.6. Suppose that we are given a hyperbolic triangle ABC with angles α, β, γ (so $\alpha + \beta + \gamma < 1$, see [JS, 5.6.5-5.6.6, & p258]). Consider the group of reflexions through the sides, and let $\Gamma \subset \mathrm{PSL}_2(\mathbf{R})$ be the index two subgroup of direct isometries. Namely, Γ is generated by the rotations $\delta_a, \delta_b, \delta_c$, of angles $2\alpha, 2\beta, 2\gamma$, around the vertices A,B,C.

Suppose furthermore that there exists positive integers a, b, c, such that $\alpha = \pi/a$, $\beta = \pi/b$, $\gamma = \frac{\pi}{c}$. Then

- a fundamental domain F is made of the triangle ABC, joined with its symmetric through a side (say AC);

- Γ has the presentation :

$$\left\langle \delta_a, \delta_b\delta_c,\ \delta_a^a = \delta_b^b = \delta_c^c = 1 \text{ and } \delta_c\delta_b\delta_a = 1 \right\rangle \tag{1.1}$$

  [Notice that, possibly modulo taking inverses of the generators, the presentation of Γ given above still holds when reordering (a, b, c)].

- and the Riemann surface $\Gamma\backslash\mathcal{H}$ has genus 0.

Such a Fuchsian group is called a *cocompact triangle group*[2].

Proof The first statement follows from [Mag, II.5 Th. 2.8]. The difficulty consists in showing that the images of ABC under side reflections, fill the hyperbolic plane without gaps and overlappings.

The second is also stated in the result mentionned above. Or more generally follows from the proof of the theorem of Poincaré–Maskit (apply the presentation of [Kat, p98] with $g = 0$).

For the last : consider B' the symmetric of B through the side AC. Then from the first statement, a fundamental domain of Γ is the quadrilateral ABCB'. But the group Γ identifies the vertices B and B' (by the rotation 2α), and identifies the pairs of sides : BC with CB', and AB with AB'. This triangulation of F thus induces a triangulation of the Riemann surface $X = \Gamma\backslash\mathcal{H}$ into 3 vertices, 2 edges and 1 free side. Thus, by the formula of Euler–Poincaré [JS, 4.16.2], the genus g_X satisfies $2 - 2g_X = 3 - 2 + 1$. So is zero. □

Example 1.7. The list of all *arithmetic triangle groups* is stated in [Tak]. The Proposition 1 states furthermore that two such groups are commensurable in $\mathrm{PSL}_2(\mathbf{R})$ iff they arise from the same quaternion algebra.

Example 1.8. Let Δ be a *cocompact* triangle group with indices (a, b, c) and $\Gamma \subset \Delta$ a subgroup. Then the covering map of Riemann surfaces:

$$f : X(\Gamma) = \Gamma\backslash\mathcal{H} \to \mathbf{P}^1 = \Delta\backslash\mathcal{H} \tag{1.2}$$

has degree $d = |\Delta/\Gamma|$. It is called a *Belyi map* and X a *Belyi curve*. Consider (separately) two additional assumptions:

[2] We don't know if the following definition, given in [Sh$_1$] (3.18.2), is equivalent : a group of genus 0 with exactly three inequivalent elements. Namely, does a group with this definition necessarily have its Dirichlet domains equal to a quadrilateral ?

(a) *Suppose that* Γ *has no elliptic point*, then the genus g of X satisfies

$$g(X(\Gamma)) = 1 + \frac{d}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right). \tag{1.3}$$

[Proof : notice that all points in the preimage of the fixed point of δ_a have ramification index a by f, and so there are $\frac{d}{a}$ of them. Conclude by the formula of Riemann–Hurwitz].

(b) Suppose now that Γ is *normal* in Δ. Then by [Wol, Lem 1 & proof of Th. 6], there also exists another pair of groups $\Gamma' \triangleleft \Delta'$ such that Γ' has *no elliptic points* and

$$X(\Gamma') = X(\Gamma).$$

So in particular the assumptions of situation (a) are satisfied with $\Gamma' \triangleleft \Delta'$.

(c) Actually it can be shown [Wol, Lem 8 & end of proof of Th. 6] that if $g(X) > 1$, then X has many automorphisms if and only if X is a curve $X(\Delta)$ of the form described in (b). The automorphisms group of X are then $G = \Gamma'/\Delta'$ for an auxiliary pair $\Delta' \triangleleft \Gamma'$ chosen as in (b).

Counterexample 1.9. Let $p \geq 7$ a prime number and $X(p)$ the quotient of the extended upper half plane $\mathcal{H}^* = \mathcal{H} \cup$ cusps of $\Gamma(p)$ under the action of the principal congruence subgroup $\Gamma(p)$. Then, although the projection map $X(p) \to \mathbf{P}^1_{\mathbf{C}} = X(1)$ is a Galois covering map between compact Riemann surfaces, the triangle groups that define it : $\Gamma(p) \triangleleft \Delta(2, 3, \infty)$ are not cocompact.

Indeed $\Gamma(p)$ has cusps (of common ramification index p, see [DS, §3.9 table 3.3]).

So one is a priori not in the situation of the previous example. And actually the conclusions of (c) $\Leftrightarrow$ (b) do not hold : $X(p)$ does not have many automorphisms. Indeed it can be shown ([Maz, Appendix of part I by J.P. Serre]) that the automorphism group of $X(p)$ is $\mathrm{PSL}_2(\mathbf{F}_p)$, which is $(7 - \frac{42}{7})$ times lower than the Hurwitz bound $84g(X(p) - 1)$.

More systematically, the genus is determined by the orders of the elliptic cycles and the area of a fundamental domain :

Definition 1.10. Endow the upper-half plane with the hyperbolic area normalized as follows : $1/2\pi(dxdy/y^2)$. The *area* of a Fuchsian group Γ, noted $\mu(\Gamma\backslash\mathcal{H})$, is the hyperbolic area $\mu(F)$ of any fundamental domain F of Γ (all these areas being equal by [Kat, Th. 3.1.1]).

Property 1.11 ([JS, 5.10.3] or [Kat, Th 4.3.1]). *Let Γ be a Fuchsian group of the first kind with signature $(g; m_1, \dots, m_r)$. Then*

$$\mu(\Gamma\backslash\mathcal{H}) = (2g-2) + \sum_{i=1}^{r}(1 - \frac{1}{m_i}) \tag{1.4}$$

Where the *area* itself can be determined from:

(A.1) The shape of a Dirichlet domain F, by the formula of Gauss–Bonnet:

Property 1.12 ([JS, Cor 5.5.6] or [Kat, exercice 4.6]). *The area of a n-sided, hyperbolically star-like, polygon F with angles α_i is*

$$\mu(F) = \frac{n-2}{2} - \sum_{i=1}^{n}\frac{\alpha_i}{2\pi} \tag{1.5}$$

Example 1.13. Consider a non empty hyperbolic triangle T with angles $\frac{\pi}{a}, \frac{\pi}{b}, \frac{\pi}{c}$. The genus being 0, the area $\mu(T)$ thus equals

$$\mu(T) = \frac{1}{2}\Big(1 - \Big(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\Big)\Big)$$

[which is the formula of Gauss–Bonnet]. The triples of integers which minimizes this sum while keeping it strictly positive is $(2, 3, 7)$.

Actually, a mere case enumeration using Property 1.11 (see [JS, 5.10.7]) shows that the $(2, 3, 7)$ triangle group is the cocompact Fuchsian group with the smallest hyperbolic area.

(A.2) A subgroup construction :

Property 1.14 ([JS] prop 5.10.9 ii). *Let Γ be a cocompact Fuchsian group of the first kind and Δ a subgroup of index n. Then $\mu(\Delta\backslash\mathcal{H}) = n\mu(\Gamma\backslash\mathcal{H})$.*

(A.3) The arithmeticity of Γ :

Property 1.15 (Shimizu's formula). *Let us narrow the setting of Theorem 1.1: let F be a totally real field of degree n and discriminant d_F, B a division quaternion algebra of discriminant $\mathfrak{D}$ with exactly one split real place, and Γ be the arithmetic group arising from the* units of norm one *of a maximal order. Then*

$$\mu(\Gamma\backslash\mathcal{H}) = \frac{4}{(2\pi)^{2n}} d_F^{3/2}\zeta_F(2)\Phi(\mathfrak{D}) \tag{1.6}$$

Where we recall :

$$\Phi(\mathfrak{D}) = |(\mathbf{Z}_F/\mathfrak{D})^\cdot| = N(\mathfrak{D}) \prod_{\mathfrak{p}|\mathfrak{D}} \left(1 - \frac{1}{N(\mathfrak{p})}\right)$$

For a shorter idelic proof see [Vig, IV.1.Exemples 5) & IV Corollaire 2.7], and [Voi$_5$, Main Theorem 39.1.8] for the higher-dimensional case.

The next section deals with the elliptic invariants m_i in the arithmetic case. Notice that, for every given artihmetic Fuchsian group, this information can also be obtained by [Voi$_3$, Algorithms 3.2 & 4.7]. Namely, given an exact pseudo-basis of a quaternion order, it returns (i) a (numerical) Dirichlet fundamental domain for the groups of units (either of norm one or totally positive) with arbitrary center, and (ii) an exact presentation of Γ by elements which pair the sides of the domain (the sides being possibly cut into two halves).

2 Elliptic points and genera

2.1 Density of general genera

Let $X_0(\mathfrak{N})_{\mathbf{C}}$ and $X_0^+(\mathfrak{N})_{\mathbf{C}}$ be the Riemann surfaces $\overline{\Gamma_0(\mathfrak{N})}\backslash\mathcal{H}$ and $\overline{\Gamma_0^+(\mathfrak{N})}\backslash\mathcal{H}$, and Ψ, Φ the functions defined in equation III.(5.11).

Proposition 2.1 ([Duc, equations (III.5) and (IV.13)])**.** *Fix F and let the disciminant $\mathfrak{D}$ and the level $\mathfrak{N}$ take every possible values. Then the genera $g_{\mathfrak{N},\mathfrak{D}}$ and $g^+_{\mathfrak{N},\mathfrak{D}}$ of $X_0(\mathfrak{N})_{\mathbf{C}}$ and $X_0^+(\mathfrak{N})_{\mathbf{C}}$ take arbitrarily large values. And there exists constants $\lambda_{F,max}$ and $\lambda^+_{F,max}$ such that they satisfy $g^{(+)}_{\mathfrak{N},\mathfrak{D}} \leq \lambda^{(+)}_{F,max}\Psi(\mathfrak{D}_i)\Phi(\mathfrak{N}_i)$.*

Notice that the first statement ($g^{(+)}_{\mathfrak{N},\mathfrak{D}}$ arbitrarily large) is not obvious. Indeed one has to control for the number of elliptic points in [Duc, equation III.5]. It will be shown in this section how to do it on an example.

Corollary 2.2. *Allow the discriminants $(\mathfrak{D}_j)_j$ and the levels $(\mathfrak{N}_k)_k$ to vary and take every possible values. Then the families $(X_0(\mathfrak{N}_k)_{\mathbf{C}})_{j,k}$ and $(X_0^+(\mathfrak{N}_k)_{\mathbf{C}})_{j,k}$ have* dense genera *in the sense of Definition 2.1.*

2.2 General elliptic points counting

Let $\Gamma \subset \mathrm{SL}_2(\mathbf{R})$ be an arithmetic Fuchsian group. Suppose that $\Gamma = \iota_{B,v}(\mathcal{O}(\mathfrak{N})^1)$ is the image of the units of norm one of an Eichler order, so that Γ *contains* -1. Let x be an element of B of minimal polynomial $f = X^2 - \mathrm{trace}(x)X + n(x)$ over F. One says that the conjugacy class of x is a *conjugacy class of minimal polynomial* f.

Let $q > 1$ be an integer, and z a point of the upper half plane whose fixator in $\overline{\Gamma}$ is of order q. One says that the orbit $\Gamma(z)$ is an *elliptic cycle of order* q, and its image $\bar{z} \in X_0(\mathfrak{N})_{\mathbf{C}}$ an *elliptic point* of order q.

Lemma 2.3 ([Vig, IV.2.9]). *The number of elliptic cycles of order q is equal to the* half *of the number of conjugacy classes, in Γ, of elements with minimal polynomial $X^2 - 2\cos(2\pi/(2q))X + 1$.*

Remark 2.4. A precision on the demonstration. The fact that g and g' are in the same cyclic group implies that they stabilize the same unique element $z \in \mathcal{H}$. The equality $g' = g"g"^{-1}$ thus implies that the image $\overline{g"} \in \mathrm{PSL}_2(\mathbf{R})$ is in the same cyclic group as $\overline{g}$ and $\overline{g'}$. And so in particular $\overline{g"}$ commutes with $\overline{g'}$.

Definition 2.5 ([Vig, p26]). Let R be a quadratic order over $\mathbf{Z}_F$, of fraction field L, and $\mathcal{O}$ an order of B. One says that an embedding $\iota : K \to B$ induces an *optimal (or maximal) embedding of R in $\mathcal{O}$* if and only if $\iota^{-1}(\mathcal{O}) \cap L = R$.

Proposition 2.6 ([Vig, Corollaire 5.14]). *Let h be an element of B which is strictly quadratic over F, and $f = X^2 - tX + n$ its minimal polynomial. Then the number of $\mathcal{O}(\mathfrak{N})^1$-conjugacy classes in $\mathcal{O}(\mathfrak{N})$ of elements with minimal polynomial f, is equal to*

$$\sum_R m_1(R),$$

where R runs over the orders of $F(h)$ containing h, and $m_1(R)$ is the number of $\mathcal{O}(\mathfrak{N})^1$-conjugacy classes of maximal embeddings of R in $\mathcal{O}(\mathfrak{N})$.

Proposition 2.7 ([Vig, III.5.11 and III.5.13]). *Suppose that there is only one conjugacy class of Eichler orders in B. Let R be a quadratic order over $\mathbf{Z}_F$, and for all $\mathfrak{p}$ prime, $m_{\mathfrak{p}}(R)$ the number of classes of maximal embeddings of $R_{\mathfrak{p}}$ in $\mathcal{O}(\mathfrak{N})_{\mathfrak{p}}$ modulo $(\mathcal{O}(\mathfrak{N})_{\mathfrak{p}})^\bullet$. Then :*

$$m_1(R) = [\mathrm{nrd}(\mathcal{O}(\mathfrak{N})^\bullet) : \mathrm{nrd}(R^\bullet)].h(R) \prod_{\mathfrak{p}\ prime} m_{\mathfrak{p}}(R), \tag{2.1}$$

where $h(R)$ is the number of classes of ideals of R (and nrd *the reduced norm on B).*

We will be only interested in the cases where the completions $B_{\mathfrak{p}}$ are matrix algebras. So the values of $m_{\mathfrak{p}}$ will be computed only in these cases. They are given by the following proposition.

Proposition 2.8 ([Vig, II.3.5])**.** *Let (F,π) be a local field, $B = \mathrm{M}_2(F)$ the matrix algebra over F and $\mathcal{O}_n$ an Eichler order of level π^n. Let $K = F(g)$ be a quadratic extension, which is supposed generated by an integer g such that the order $R = \mathbf{Z}_F[g]$ be* maximal*. Let $p(X) = X^2 - tX + m$ the minimal polynomial of g, one defines the sets*

$$E(n) = \left\{ x \in \frac{R}{R.\pi^n},\ p(x) = 0. \right\}$$

Then the number of maximal embeddings of R in $\mathcal{O}_n$ modulo the conjugacy by $\mathcal{O}_n^\bullet$, is equal to :

- $|E(n)|$ *if $\mathcal{O}_n$ is maximal ($n = 0$), or if $t^2 - 4m$ is invertible;*
- $|E(n)| + |\mathrm{Im}(E(n+1) \to E(n))|$ *otherwise.*

So in particular whenever the order: $\mathcal{O}(\mathfrak{N})_{\mathfrak{p}}$ of the quaternion algebra completed at $\mathfrak{p}$ is maximal (so for almost all $\mathfrak{p}$), then the factor $m_{\mathfrak{p}}(R)$ in the product of (2.1) is equal to one.

2.3 Case of the group (2,3,7)

Global embedding numbers

Let $F = \mathbf{Q}(\cos(2\pi/7))$ then $[F : \mathbf{Q}] = 3$. Fix one real place ι, then let B be the quaternion algebra over F which is ramified exactly at the two other real places (and no finite place)[3]Let $\mathfrak{N} = \prod_i \mathfrak{p}_i^{e_i}$ be an ideal of $\mathbf{Z}_F$ along with its decomposition in primes.

[3]Actually the geometry of the groups to be built doesn't depend on the choice of ι. Indeed let σ be an automorphism of F and let B^σ be the quaternion algebra ramified exactly at the two other places than ι^σ. Then, the finite discriminant being trivially Galois-invariant, we obtain that B^σ is the *conjugate quaternion algebra* of B in the sense of Remark V.5.7. Which thus trivially leads to the same Shimura curves.

Lemma 2.9. *For each n, let ζ_n be a primitive n-th root of unity. Then the set of numbers q, such that there exists a quadratic extension of F containing ζ_{2q}, is equal to $\{2,3,7\}$. In addition for these values of q, the orders $\mathbf{Z}_F[\zeta_{2q}]$ are maximal in the corresponding fields $F(\zeta_{2q})$.*

Proof The first one is a brutal enumeration.

For the second one I trust Magma. □

The maximality condition of Proposition 2.8 is thus satisfied for all the local orders obtained by completion of these orders.

Furthermore the narrow class number of F, $|\mathrm{Cl}_\infty(F)|$, being equal to one, all the Eichler orders of level $\mathfrak{N}$ are conjugate in B by Corollary III.2.5. Thus the assumption of Proposition 2.7 holds.

Lemma 2.10. *Under the same assumtions:*

- $h(\mathbf{Z}_F[\zeta_{2q}]) = 1$ *for* $q = 2, 3, 7$.
- $[\mathrm{nrd}(\mathcal{O}(\mathfrak{N})^\bullet) : \mathrm{nrd}(R^\bullet)] = 2$ *for* $R = \mathbf{Z}_F[\zeta_{2q}]$ *and for all* $\mathfrak{N}$.

Proof For the first, I trust Magma.

For the second, let use the equality $\mathrm{nrd}(\mathcal{O}(\mathfrak{N})^\bullet) = \mathbf{Z}^\bullet_{F,B}$ from Theorem III.3.1, where $\mathbf{Z}^\bullet_{F,B}$ are the units which are positive at the places that ramify B. So if $\iota_1 = \iota_{B,v}$ is the split real place, let these places be ι_2 and ι_3. To obtain generators of this group, ask Magma for the signs of three generators U_1, U_2, U_3 of $\mathbf{Z}^\bullet_F$: $[-,-,-][-,+,-],[+,+,-]$. From these signs, one deduces generators of $\mathbf{Z}_{F,B}$: $\{U_1^2, U_2^2, U_2U_3, U_3^2\}$. The index in $\mathbf{Z}^\bullet_F$ can now be computed in an elementary way. □

Putting together Lemma 2.3, Proposition 2.7 and Lemma 2.10, the number of elliptic points of order q in $X_0(\mathfrak{N})_{\mathbf{C}}$, $q \in 2, 3, 7$, is equal to

$$e_q = \frac{1}{2} \sum_{R=\mathbf{Z}_F[\zeta_{2q}]} 2.1. \prod_{\mathfrak{p} \text{ prime}} m_{\mathfrak{p}}(R) = \prod_{\mathfrak{p} \text{ prime}} m_{\mathfrak{p}}(\mathbf{Z}_F[\zeta_{2q}]) \ . \tag{2.2}$$

In the rest of the section we will only consider levels $\mathfrak{N}$ of the form $\mathfrak{p}_2^i.\mathfrak{p}_7^j$, where $\mathfrak{p}_2$ and $\mathfrak{p}_7$ are (resp.) the unique prime ideals above (2) and (7).

It is thus sufficient to compute the factors $m_{\mathfrak{p}_2}(\mathbf{Z}_F[\zeta_{2q}])$ and $m_{\mathfrak{p}_7}(\mathbf{Z}_F[\zeta_{2q}])$ in (2.2). Indeed the others are equal to one so play no role in Proposition 2.7.

Notice similarly that the embedding number $m_{\mathfrak{p}}$ at $\mathfrak{p}$ is one as soon as $\mathfrak{p} \nmid \mathfrak{N}$, because the local order $\mathcal{O}_{\mathfrak{p}}$ is then maximal.

Local embeddings of $\mathbf{Z}_F[\zeta_4]$

- at $\mathfrak{p}_7$: The minimal polynomial of ζ_4 has no solution modulo $\mathfrak{p}_7$. Thus $m_{\mathfrak{p}_7} = 0$ as soon as $j \geq 1$ [and one otherwise].
- at $\mathfrak{p}_2$: The minimal polynomial of ζ_4 has a unique solution modulo $\mathfrak{p}_2$ and no solution modulo $\mathfrak{p}_2^2$. Thus $m_{\mathfrak{p}_2} = 1$ if $i \in \{0, 1\}$, and 0 afterwards.

Local embeddings of $\mathbf{Z}_F[\zeta_6]$

The discriminant of the minimal polynomial of ζ_6 is equal to (3), so is inversible modulo $\mathfrak{p}_2$ and $\mathfrak{p}_7$. Thus we are in the first case of Proposition 2.7.

So by Hensel's lemma, the roots modulo $\mathfrak{p}_2$ (respectively $\mathfrak{p}_7$) lift to a unique solution modulo $\mathfrak{p}_2^i$ (respectively $\mathfrak{p}_7^j$) for all $i \geq 1$ (respectively j) ≥ 1.

- at $\mathfrak{p}_7$: $m_{\mathfrak{p}_7} = 2$ distinct roots as soon as $j \geq 1$ [and 1 for $j = 0$].
- at $\mathfrak{p}_2$: $m_{\mathfrak{p}_2} = 0$ root as soon as $i \geq 1$ [and 1 for $i = 0$].

Local embeddings of $\mathbf{Z}_F[\zeta_{14}]$

- at $\mathfrak{p}_7$: The minimal polynomial of ζ_{14} has an unique solution (with multiplicity two) modulo $\mathfrak{p}_7$, then no solution modulo $\mathfrak{p}_7^i$ for $j \geq 2$. Thus $m_{\mathfrak{p}_7} = 1$ if $j \in \{0, 1\}$, and 0 afterwards.
- at $\mathfrak{p}_2$: The minimal polynomial of ζ_{14} has its discriminant invertible modulo $\mathfrak{p}_2$. Thus we are in the first case of Proposition 2.7. Furthermore these roots all come from the two disctinct roots modulo $\mathfrak{p}_2$ by Hensel's lemma. So $m_{\mathfrak{p}_2} = 2$ as soon as $i \geq 1$ [and 1 for $i = 0$].

2.4 Outcome : elliptic points for $\mathfrak{N} = \mathfrak{p}_2^i.\mathfrak{p}_7^j$

Corollary 2.11. *The elliptic points of the Riemann surfaces $X_0(\mathfrak{p}_2^i.\mathfrak{p}_7^j)_{\mathbf{C}}$ are:*

- $\boxed{i{=}j{=}0}$ *:* $[2, 3, 7]$*;*
- $\boxed{j{=}0}$*,* $i{=}1$ *:* $[2, 7, 7]$ *then for* $i \geq 2$ *:* $[7, 7]$*;*
- $\boxed{j{=}1}$*,* $i \geq 1$ *:* $[7, 7]$*;*

- $\boxed{i=0}$, *j=1 :* $[3,3,7]$ *then for* $j \geq 2$ *:* $[3,3]$*;*
- *for the rest* $(\{i \geq 1\} \cap \{j \geq 2\})$ *:* $[\varnothing]$.

2.5 Density of the genera in the family $X_0(\mathfrak{p}_2^i.\mathfrak{p}_7^j)_{\mathbf{C}}$

Corollary 2.12. *The genera of the Riemann surfaces* $X_0(\mathfrak{p}_2^i.\mathfrak{p}_7^j)_{\mathbf{C}}$ *are:*

- $\boxed{i=j=0}$ *:* 0 *;*
- $\boxed{j=0}$, *i=1 : 1 then for* $i \geq 2$ *:* $8^{i-2}.6/7 + 1/7$*;*
- $\boxed{j=1}$, $i \geq 1$ *:* $8^{i-1}.6/7 + 1/7$*;*
- $\boxed{i=0}$, *j=1 : 0 then for* $j \geq 2$ *:* $7^{j-2}.2/3 + 1/3$*;*
- *for the rest* $(\{i \geq 1\} \cap \{j \geq 2\})$ *:* $7^{j-2}\,[8^{i-1}.6/7 + 1/7]$.

Proof $[2,3,7]$ is a triangle group, so of genus 0. The others are deduced by Riemann–Hurwitz and by recurrence. □

The following fact, which was pointed to us by N.D. Elkies, allows to conclude that the ordered genera $(g_{i,j})_{i,j}$ of the family $X_0(\mathfrak{p}_2^i.\mathfrak{p}_7^j)_{\mathbf{C}}$ are *dense* in the sense of Definition I.2.1:

Proposition 2.13. *Let* p *and* q *be to numbers relatively prime to one another. Then for all* $\epsilon > 0$*, there exists* N *such that, as soon as* $p^i.q^j > N$*, there exists* i'*,* j' *such that* $p^{i'}.q^{j'} > p^i.q^j$ *and* $\left|\frac{p^{i'}.q^{j'}}{p^i.q^j} - 1\right| < \epsilon$.

The following proof was greatly contributed to by H. Randriam, and also by J. Pieltant.

Lemma 2.14. *Let* ρ *be an irrational number. Then for all* $\epsilon > 0$*, there exists* N *a positive integer such that the fractionnal part* $\{N.\rho\} < \epsilon$.

Proof Let M be large enough such that $\frac{1}{M} < \epsilon$. Let us partition the interval $[0,1[$ in M intervals $[i/M,(i+1)/M[$ of equal length. One considers the sequence of the fractional parts $(\{n.\rho\})_{n\in\mathbf{N}}$. By the pigeonhole principle, there exists two distinct values of this sequence: $0 \leq \{N_1.\rho\} < \{N_2.\rho\} < 1$ that lie in the *same interval.*

- If $N_2 > N_1$, then the positive integer $N_2 - N_1$ suits.
- Else if $N_1 = N_2 + k$, with k a positive integer, let μ be the difference $\mu = \{N_2.\rho\} - \{(N_2 + k).\rho\} < \frac{1}{M}$. Hence the fractional part $\{k.\rho\}$ is equal to $1 - \mu$. One can iterate and consider the sequence of fractional parts: $\{N_2.\rho\}, \{(N_2 + k).\rho\}, \{(N_2 + 2k).\rho\} \ldots$. Its first values decrease regularly, with steps equal to μ. But by hypothesis $\mu < \frac{1}{M}$. Thus the sequence eventually reaches a value (of the form $\{N_2 + m.k\}$) contained in the first interval $[0, \frac{1}{M} < \epsilon[$. Finally, the positive integer $N_2 + m.k$ suits.

□

Lemma 2.15. *Let p and q be to numbers relatively prime to one another. Then for all $\epsilon' > 0$, there exists integers a and b such that $0 < a \log p + b \log q < \epsilon'$. Furthermore one can choose the sign of a.*

Proof p and q being prime to one another, the quotient $\frac{\log p}{\log q}$ is irrational.
For $a > 0$, it suffices to apply the previous lemma to $\alpha = \frac{\log p}{\log q}$ and $\epsilon = \frac{\epsilon'}{\log q}$. One then chooses $a = N$ and $b = -E(N \frac{\log p}{\log q})$.
For $a < 0$, one applies the previous lemma to $\alpha = \frac{\log q}{\log p}$. □

Let us now prove the proposition.
Consider $\epsilon > 0$. By the previous lemma there exists:

- a, b two positive integers such that $\left|\frac{p^a}{q^b} - 1\right| < \epsilon$,
- and also c, d two positive integers such that $\left|\frac{q^d}{p^c} - 1\right| < \epsilon$.

One chooses N large enough such that:

$$p^i.q^j > N \Rightarrow (i > c \text{ or } j > b).$$

Consider $p^i.q^j > N$. Then by this choice of N, at least one of the two following inequalities is satisfied:

j > b One chooses $i' = a + i > 0$ and $j' = j - b > 0$. Thus, $\frac{p^{i'}.q^{j'}}{p^i.q^j} = \frac{p^a}{q^b}$ is strictly lower than 1 and satisfies $\left|\frac{p^{i'}.q^{j'}}{p^i.q^j} - 1\right| < \epsilon$.

i > c One chooses $i' = i - c > 0$ et $j' = j + d > 0$. Thus, $\frac{p^{i'}.q^{j'}}{p^i.q^j} = \frac{q^d}{p^c}$ is strictly larger than 1 and satisfies $\left|\frac{p^{i'}.q^{j'}}{p^i.q^j} - 1\right| < \epsilon$.

Chapter V

Descent of canonical models

1 Leitfaden

The following three results:

(a) Theorem 4.12 (ii): a ramified cover with no automorphisms and field of moduli $\mathbf{Q}$ descends to a cover over $\mathbf{Q}$. (i): This descended cover is furthermore unique, up to $\mathbf{Q}$-isomorphisms of covers;

(b) Theorem 5.11 Let $X_0(1)$ be uniformized by a triangle group with distinct indices, arizing from a quaternion algebra with Galois-stable discriminant. Let $\mathfrak{N}$ be a Galois-stable ideal. Then the complex cover $X_0(\mathfrak{N}) \longrightarrow X_0(1)$ has field of moduli equal to $\mathbf{Q}$;

(c) Proposition 5.12: the ramified covers $X_0(\mathfrak{N}) \longrightarrow X_0(1)$ have no automorphisms;

...imply the main result :

Theorem 5.14 : Let $X_0(1)$ be uniformized by a triangle group with distinct indices, arizing from a quaternion algebra with Galois-stable discriminant. Let $\mathfrak{N}$ be a Galois-stable ideal. Then the complex cover $X_0(\mathfrak{N}) \longrightarrow X_0(1)$ descends to a cover over $\mathbf{Q}$. This descended cover is furthermore unique, up to $\mathbf{Q}$-isomorphisms of covers.

2 Field of definition and field of moduli of covers

The definitions and statements in this paragraph stick to covers of $\mathbf{P}^1_k$. They correspond to regular extensions $E/k(T)$, with geometric counterpart $Ek^{sep}/k^{sep}(T)$.

One could have stated the results for a more general base B_k instead, with function field K/k. And thus dealt with regular extensions E/K and their geometric counterpart Ek^{sep}/Kk^{sep}. In this generality Prop 2.6 would not always hold: see the counterexamples following [DE, Remark 5.5].

Another advantage is that if k'/k is a Galois extension, then $\tau \in \mathrm{Gal}(k'/k)$ has a straightforward prolongation to $Kk' = k'(T)$: the one that fixes T. We will adopt this one throughout. Changing this prolongation (*i.e.* the k-structure of $\mathbf{P}^1_{k'}$, as illustrated in footnote 1) would change the field of moduli: see [DE, p45].

Definition 2.1 (Ramified cover [DèbDo] §2.1)**.** Let k be a field. A *(branched) algebraic cover* of $\mathbf{P}^1_k$ is the data of (i) X a proper (projective), geometrically integral smooth curve over k, along with (ii) a finite, non constant, generically unramified morphism $\pi : X \to \mathbf{P}^1_k$.

The assumption geometrically irreducible is equivalent to the extension of function fields $k(X)/k$ being *regular*. That is to say : $[\bar{k}(X) : \bar{k}(T)] = [k(X) : k(T)]$, which is itself equivalent to k being algebraically closed in $k(X)$.

The function field functor yields an equivalence of categories between the categories: {birational classes of covers; subcover maps} and: {finite regular field extensions; field inclusion maps} [Dèb$_2$, §3.3.3 & §3.3.4].

Definition 2.2 ([Dèb$_2$, 3.1.15])**.** Let k be a field and k'/k an extension and $E/k'(T)$ a finite extension. One says that :

- E is defined on k *as mere extension of* k' *(or as mere curve)*, if and only if there exists a finite regular extension $E_0/k(T)$ such that E_0k' and E are k'-isomorphic;
- $E/k'(T)$ is defined on k *as mere extension of* $k'(T)$ *(or as mere cover)* if and only if there exists a finite regular extension $E_0/k(T)$ such that E_0k' and E are $k'(T)$-isomorphic;

- [Cultural: suppose furthermore that $E/k'(T)$ is a Galois extension, endowed with an isomorphism $u : G \to \mathrm{Gal}(E/k'(T))$. Such a pair (E, u) is called a G-extension. Then it is *defined on k as G-extension* if and only if there exists a finite regular G-extension $E_0/k(T)$ such that E_0k' and E are (G-equivariantly) $k'(T)$-isomorphic.]

One then says that k is a *field of definition*, and that $E_0/k(T)$ is a *k-model* (resp. as mere curve, mere cover and G-extension) of $E/k'(T)$.

Prop-Def 2.3 (Action of $\mathrm{Gal}(k'/k)$ [DèbDo, §2.3 & §2.6])**.** Let k'/k be a Galois extension with Galois group Γ, and again $E/k'(T)$ a finite (G-) extension. Let $F/k(T)$ be a Galois closure containing E.

Let τ be an element in Γ, the extension ${}^{\tau}E/k'(T)$ is defined as follows. Let $\tilde{\tau}$ be any arbitrary prolongation of τ to $\mathrm{Gal}(F/k(T))$ that fixes T, then:

$$k'(T) \subset_{\mathrm{incl}} \tilde{\tau}(E) \subset_{\mathrm{incl}} F \tag{2.1}$$

where all the $\subset_{\mathrm{incl}}$ stand for the set-theoretic inclusion in the fixed Galois extension[1] F.

[Cultural: for the G-extensions ([Dèb$_2$, Prop 3.1.17]): ${}^{\tau}E$ is the ${}^{\tau}G = \tilde{\tau}G\tilde{\tau}^{-1}$-extension with action ${}^{\tau}u = \tilde{\tau}u\tilde{\tau}^{-1}$.]

Furthermore for any such choice of prolongation $\tilde{\tau}$, ${}^{\tau}E/k'(T)$ is $k'(T)$ isomorphic to the base-change by τ of the extension $E/k'(T)$. Thus ${}^{\tau}E/k'(T)$ is in fact well defined up to a $k'(T)$-isomorphism of extension.

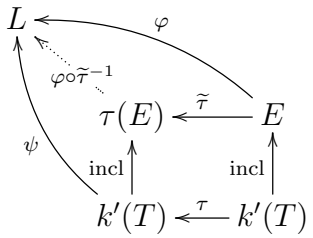
Finally if $E/k'(T)$ is defined over k (as a k', $k'(T)$ or G-extension), then it is (k', $k'(T)$, respectively G)- isomorphic to its conjugates ${}^{\tau}E/k'(T)$.

[1] As discussed in [DE, p45], other choices of k- structures for $Kk' = k'(T)$ may lead to nonisomorphic conjugates, and hence different field of moduli. This issue is analogous to the case of varieties over finite fields, where different k-structures lead to different geometric Frobeniuses over k'. For example here, the choice of a fixed Galois closure F implicitly determined the k-structure :

$$\begin{cases} k(T) \otimes_k k' \longrightarrow k'(T) \\ \qquad x, y \to \mathrm{incl}(x).\mathrm{incl}(y) \end{cases} \tag{2.2}$$

So this choice yields the (functorial in τ) collection of isomorphisms $\tau(k'(T)) \to k'(T)$, which are simply the subset-identity in F. But composing (2.2) with a homography r would lead to conjugate these isomorphisms by $\tau(r)$.

Proof For the base-change claim, consider a commutative diagram:



where $\varphi : E \to L$ and $\varphi : k'(T) \to L$ coincide on the right-hand bottom corner $k'(T)$. Then $\varphi \circ \widetilde{\tau}^{-1}$ factors both φ and ψ [indeed, going from the left-hand bottom corner $k'(T)$ to L by the two exterior paths shows that $\psi{=}\varphi{\circ}\mathrm{incl}{\circ}\tau^{-1}$]. So the universal property for the tensor product is satisfied.

Let us prove the final assertion (in the $k'(T)$-extension setting). Let E_0/K be a regular extension such that $E_0 \otimes_{k(T)} k'(T) \cong E$. Then the previous identification with the tensor-product yields the following $k'(T)$-isomorphisms:

$$^{\tau}E \cong E \otimes_{\tau} k'(T) = (E_0 \otimes_{k(T)} k'(T)) \otimes_{\tau} k'(T) \cong E_0 \otimes_{\tau\circ\mathrm{incl}} k'(T)$$

Where incl is the inclusion $k(T) \subset k'(T)$. Which is unchanged after composing by τ. So the latter is equal to $E_0 \otimes_{\mathrm{incl}} k'(T) \cong E$. □

Example 2.4. $\mathbf{C}(\sqrt{T+i})/\mathbf{C}(T)$ is defined on $\mathbf{R}$ as $\mathbf{C}$-extension, but not as a $\mathbf{C}(T)$-extension. Indeed suppose that it were the case. Let τ be the $\mathbf{R}(T)$-linear morphism $\begin{cases} \mathbf{C}(T) \longrightarrow \mathbf{C}(T) \\ i \to -i \end{cases}$, and $\widetilde{\tau}$ the $\mathbf{R}(T)$-linear prolongation $\begin{cases} \mathbf{C}(\sqrt{T+i}) \longrightarrow \mathbf{C}(\sqrt{T-i}) \\ \sqrt{T+i} \to \sqrt{T-i} \end{cases}$. Then by assumption and by the previous proposition, there exists a $\mathbf{C}(T)$-isomorphism $\varphi : \mathbf{C}(\sqrt{T+i}) \to \mathbf{C}(\sqrt{T-i})$. By $\mathbf{C}(T)$-linearity one has $T+i = \varphi(\sqrt{T+i})^2$. So $\varphi(\sqrt{T+i})$ is either equal to $\sqrt{T+i}$ or to $-\sqrt{T+i}$, both being impossible.

Example 2.5. $E = \mathbf{Q}(\xi_d)(T^{1/d})/\mathbf{Q}(\xi_d)(T)$ is defined over $\mathbf{Q}$ as $\mathbf{Q}(\xi_d)(T)$-extension. Indeed it arises from the extension $\mathbf{Q}(T^{1/d})/\mathbf{Q}(T)$, of same degree.

[Cultural: it is not defined as a $G = (\mathbf{Z}/d\mathbf{Z})^{\bullet}$-extension. The most straightforward proof is probably to check that E is not G-conjugate to its twists[2] . It will be done in counterexample 2.8.]

[2]Another proof for this, suggested by [Dèb$_2$, 3.1.16] : show that the (d) of corollary

Proposition 2.6. *Suppose that k is a field of characteristic zero, k'/k a Galois extension and let $F/k(T)$ be a Galois extension.Prolonging the action of* $\mathrm{Gal}(\overline{k}/k)$ *to* $\overline{k}(T)$ *by fixing T, assume that* $\mathrm{Gal}(\overline{k}/k)$ stabilizes the set D of geometric branch points of $F/k'(T)$.

Then noting $G = \mathrm{Gal}(F/k(T))$, $N = \mathrm{Gal}(F/k'(T))$ *and* $\Gamma = \mathrm{Gal}(k'/k)$, *there exists a section s to the following exact sequence:*

(Seq/Split)
$$1 \longrightarrow N \longrightarrow G \underset{\pi}{\overset{s}{\rightleftarrows}} \Gamma \longrightarrow 1$$

Proof For a quick reference: the first criterion stated in the discussion done below [DE, Th. 5.1] applies here. Indeed k being of characteristic zero, the condition (Sec/Split)' is equal to (Sec/Split). And $k(T)$ has an infinite number of closed points.

For a proof, adapt for example [Dèb$_2$, Th 3.2.1]. □

If $E/k'(T)$ is defined on k (in either one of the three meanings of Definition 2.1), then it is isomorphic to its conjugates. This necessary condition is restated group-theoretically as follows (see also [DèbDo] §2.7) :

Definition 2.7. Same assumptions as in Prop-Def 2.3

$\big[k'/k$ is a Galois extension with Galois group Γ, $E/k'(T)$ a finite (G-) extension and let $F/k(T)$ be a Galois closure containing E. Note as above G and N the Galois groups of $F/k(T)$ and $F/k'(T)$. Let $H \subset N$ be the fixator subgroup of the (G-)extension $E/k'(T)$. For every τ in Γ, choose $\widetilde{\tau}$ any prolongation to G that fixes $T\big]$. One says that :

- [Wol, lemma 5] the *field of moduli of E as mere k'-extension (as mere curve)* is the subfield $k_{m,c}$ of k' fixed by

$$\{\tau \in \Gamma, \text{ such that } \widetilde{\tau}(E) \text{ is } k'\text{-isomorphic to } E\};$$

3.1.18 is not satisfied. First, the *distinguished generator of the inertia* at the ideal $(T^{1/d})$ is by definition (3.1.4.1) the element $\gamma \in \mathrm{Gal}\Big(\mathbf{Q}(\xi_d)(T^{1/d})/\mathbf{Q}(\xi_d)(T)\Big)$, which sends $T^{1/d}$ on $\xi T^{1/d}$. Its conjugacy class C boils down to $\{\gamma\}$ because G is abelian. Compute what does this conjugacy class become when one conjugates the extension by an element $\sigma \in \mathrm{Gal}(\mathbf{Q}(\xi_d)/\mathbf{Q})$. So let $\sigma : \xi \to \xi^j$ (j invertible mod d), and $\tilde{\sigma}$ its prolongation to the automorphism of $\mathbf{Q}(\xi_d)(T^{1/d})/\mathbf{Q}$ that sends $T^{1/d}$ to itself. Then the inertia invariant of the conjugate G-extension ${}^{\tilde{\sigma}}\mathbf{Q}(\xi_d)(T^{1/d})/\mathbf{Q}((\xi_d)(T))$, is equal to $\{\gamma^{j^{-1} \pmod d}\}$. Indeed it suffices to check that $\tilde{\sigma} \circ \gamma^{j^{-1} \pmod d} \circ \tilde{\sigma^{-1}}$ sends indeed $T^{1/d}$ on $\xi T^{1/d}$ [Which could actually be directly deduced from the last point of corollary 3.1.13]. This invariant is different from C so the (d) of the corollary is not satisfied.

- [DèbDo, §2.17 restated] the *field of moduli of E as mere extension of $k'(T)$ (as mere cover)* is the subfield $k_{m,G}$ of k' fixed by

$$\left\{\tau \in \Gamma, \text{ such that there exists } \varphi_\tau \in N,\ \widetilde{\tau} H \widetilde{\tau}^{-1} = \varphi_\tau H \varphi_\tau^{-1}\right\};$$

- [Dèb$_2$, prop 3.1.17 b)] suppose furthermore $E/k'(T)$ Galois, endowed with a fixed isomorphism $u : N/H \to \mathrm{Gal}(E/k'(T))$. Then the *field of moduli of (E,u) as G-extension of $k'(T)$* is the subfield k_m of k' fixed by the automorphisms $\tau \in \Gamma$ such that there exists $\chi_\tau \in N/H = \mathrm{Gal}(E/k'(T))$, such that

$$\forall g \in N/H,\ \widetilde{\tau} u(g) \widetilde{\tau}^{-1} = \chi_\tau u(g) \chi_\tau^{-1}\ .$$

The ramification divisor (and thus the set of branch points on the base) is automatically invariant under the subgroup of $\mathrm{Gal}(k'/k)$ fixing the field of moduli of E as a cover.

Counterexample 2.8. [Cultural: let $d \geq 3$ be an integer and $\xi = \xi_d$ a d-th root of unity. Then the field of moduli of the $G = (\mathbf{Z}/d\mathbf{Z})^\bullet$-extension $E = \mathbf{Q}(\xi_d)(T^{1/d})/\mathbf{Q}(\xi_d)(T)$ is not $\mathbf{Q}$. For this, consider any $\tau \in \mathrm{Gal}\big(\mathbf{Q}(\xi_d)/\mathbf{Q}\big)$: $\xi \to \xi^j$ ($j \in (\mathbf{Z}/d\mathbf{Z})^\bullet$), and extend it to E by fixing $T^{1/d}$. Suppose that threre exists $\chi_\tau : T^{1/d} \to \xi^k T^{1/d}$ in $\mathrm{Gal}\big(E/\mathbf{Q}(\xi_d)(T)\big)$ such that for all g : $T^{1/d} \to \xi^l T^{1/d}$ in $\mathrm{Gal}(E/\mathbf{Q}(\xi_d)(T))$ the relation (2.7) holds. This is actually impossible because applying it to $T^{1/d}$ would imply $jl = l$ for all l.]

3 Subgroups and their monodromy representations

3.1 Facts

Consider the group of permutations $(S_d, .)$ with the reverse composition law: $a.b \widehat{=} b \circ a$. One says that a group morphism $G \to (S_d, .)$ that induces a transitive action on the set of d elements, is a *transitive right representation* of G in S_d.

Prop-Def 3.1. let G be a group and d an integer. Then one has the following bijection of sets of conjugacy classes, induced by the (non canonical) two

arrows:

$$\left\{\begin{array}{c}G\text{-conjugacy classes of}\\ \text{subgps of index } d\text{: } H\subset G\end{array}\right\} \qquad \left\{\begin{array}{c}S_d\text{-conjugacy classes of transitive}\\ \text{right-representations } (S_d,.)\leftarrow G\end{array}\right\}$$

$$H\subset G \longmapsto \phi_H : (S_{H\backslash G},.)\leftarrow G \quad \text{(action on the right classes)}$$

$$\mathrm{Fix}_G(1) \longleftarrow \phi : (S_d,.)\leftarrow G$$

Given a subgroup H, one says that the (S_d conjugacy class of the) group morphism $\phi_H : G\to (S_d,.)$ is the *monodromy representation* of H.

Its kernel is equal to the intersection of the conjugates of H in G: $\cap_{g\in G} g^{-1}Hg$. This is in particular the largest normal subgroup of G contained in H.

The image of G in $(S_d,.)$ is thus isomorphic to the resulting quotient group :

$$G\Big/\bigcap_{g\in G} g^{-1}Hg. \tag{3.1}$$

It is called the *monodromy group* of H.

Proof The second arrow does induce a well defined map when quotienting the source and the target by conjugacy [if two representations are conjugate (by $\sigma\in S_d$), then the fixators $\mathrm{Fix}_G(1)$ are conjugate (by any element of G sending 1 to $\sigma(1)$)].

Let show that the first arrow also does.

(i) Two choices of numberings of the set G/H yields conjugated permutations.

(ii) Two conjugate subgroups H yield conjugate permutations.

Let us show the second point with the left-action convention $\phi : G\to S_{G/H}$, by commodity. Let n be an element of G, $(g_i)_{i=1\ldots d}$ a set of representatives of G/H and (ng_in^{-1}) the corresponding set of representatives of G/nHn^{-1}. Let σ be the permutation of $\{1..d\}$ such that for all i, $ng_i\in g_{\sigma(i)}H$ (so for all i, $g_i\in ng_{\sigma^{-1}(i)}H$). Then for all $\gamma\in G$, $\gamma ng_i\in g_{\phi(\gamma)\circ\sigma(i)}H\in g_{\sigma^{-1}\circ\phi(\gamma)\circ\sigma(i)}nH$.

Next, the arrows are inverse to each other because (i) the kernel of the right action $H\backslash G\to G$ is H and (ii') (idem to (ii)) permutations with conjugate kernels are conjugate in S_d.

Finally for the kernel of $G\to S_{G/H}$: it is equal to the intersection of the fixators of the right classes Hg_i: $\cap_{i=1}^d g_i^{-1}Hg_i$. It is immediate to show that this subgroup is normal in G. □

Example 3.2 (π_1 of $\mathbf{P}^1$ minus r points). Consider the group on r generators with the following presentation:

$$\pi_1 = \langle \delta_1, \dots, \delta_r,\ \delta_1 \dots \delta_r = 1 \rangle \tag{3.2}$$

Then the conjugacy classes of subgroups $\pi_1 \supset H$ of index d correspond to

$$\{\text{r-uples of permutations } (\sigma_1, \dots, \sigma_r) \text{ in } (S_d, .) \text{ such that } \sigma_1 \dots . \sigma_r = 1\} \Big/ \sim$$

where $\sim$ means simultaneous conjugacy in S_d.

Attention : the data of a r-uple of permutations (the images) alone does not determine the group morphism ϕ_H. It determines it modulo a choice of ordered generators δ_i (the preimages).

The following lemma will be used for explicit computations:

Lemma 3.3 ([Dèb$_2$, 7.4.2]). *Let G act on the left on a finite set X, $\phi : G \to S_X$) the corresponding transitive left-representation. Let $x \in X$ be any element and G_x be its stabilizer. Then the representation ϕ is isomorphic to the left representation $G \to S_{G/G_x}$.*

3.2 Case of congruence subgroups

A complete example

Example 3.4. Consider the degree 3 totally real field $F = \mathbf{Q}\big(\cos(2\pi/7)\big)$ and fix a generator α of F with minimal polynomial $P_{min} = X^3 + X^2 - 2X - 1$ over $\mathbf{Q}$. Fix the basis $[R_1, R_2, R_3] = [1, \alpha, \alpha^2]$ of the ring of integers $\mathbf{Z}_F$. Consider the prime ideal $\mathfrak{p}_7 \subset \mathbf{Z}_F$ of norm 7 above the totally ramified prime $(7) \subset \mathbf{Z}$. In the previous basis, it has the following two generators :

$$\mathfrak{p}_7 = \mathbf{Z}_F \big\langle [49, 0, 0], [25, 10, 1]. \big\rangle$$

Consider now the quaternion algebra B over F ramified exactly at two real places (noted ι_2 and ι_3) and no finite place. Fix a presentation of A :

$$A = F\Big\langle 1, i, j, k,\ i^2 = -2\alpha^2 + 2\alpha + 1,\ j^2 = \alpha^2 + \alpha - 2,\ ij = k. \Big\rangle$$

Fix any Eichler order $\mathcal{O}(\mathfrak{p}_7)$ of level $\mathfrak{p}_7$ (F having narrow class number one, they are all conjugate by Corollary III.2.5). For example the one with the

following pseudobasis:

$$\begin{aligned}
&(\mathbf{Z}_F\langle R_1\rangle, 1),\\
&(\mathbf{Z}_F\langle 7R_1, 5R_1+R_2\rangle, i),\\
&(\mathbf{Z}_F\langle \frac{1}{2}R_1\rangle, (\alpha+1)+(\alpha^2+\alpha)i+j),\\
&(\mathbf{Z}_F\langle \frac{1}{2}R_1\rangle, (\alpha^2+\alpha)+(\alpha-1)i+k)
\end{aligned}$$

Now consider the subgroup $G=\overline{\Gamma_0(\mathfrak{p}_7)}$ of $\mathrm{PSL}_2(\mathbf{R})$ defined as in III.(-), i.e. the image of the units of norm one of the order $\mathcal{O}(\mathfrak{p}_7)$. It has the following explicit presentation as a triangle group:

$$G=\left\langle \delta_a,\delta_b,\delta_c,\ \delta_a^7=\delta_b^3=\delta_c^3=1,\ \delta_a\delta_b\delta_c=1\right\rangle$$

where the generators are expressed in the previous pseudobasis:

$$\begin{aligned}
\delta_a =&[-2R_2-R_3, 0, -\frac{1}{2}R_1, R_2+\frac{1}{2}R_3],\\
\delta_b =&[-R_1-2R_2-R_3, R_1-2R_2-R_3, \frac{1}{2}R_2, R_1+\frac{1}{2}R_2],\\
\delta_c =&[2R_2+R_3, 0, 0, -R_1-\frac{1}{2}R_2]
\end{aligned}$$

Let $\iota_{\mathfrak{p}_7}: A\hookrightarrow \mathrm{M}_2(F_{\mathfrak{p}_7})$ be an embedding of A into the matrix ring completed at $\mathfrak{p}_7$ such that $\mathcal{O}(\mathfrak{p}_7)$ maps onto the integral matrices which are upper-triangular modulo $\mathfrak{p}_7$. There are several possible maps (compose at the source with $\mathrm{PSL}_2(\mathbf{Z}_F)$), so we should have also made it explicit.

Let us consider the residue ring $\mathbf{Z}_F/\mathfrak{p}_7^2$, which is finite local with maximal ideal $\mathfrak{p}_7$. The embedding $\iota_{\mathfrak{p}_7}$ composed with the residue map $\pi_{\mathfrak{p}_7^2}$ modulo $\mathfrak{p}_7^2$:

$$A\hookrightarrow \mathrm{M}_2(\mathbf{Z}_{F,\mathfrak{p}_7})\twoheadrightarrow \mathrm{M}_2(\mathbf{Z}_F/\mathfrak{p}_7^2),$$

induces a surjective morphism of G onto the subgroup $\overline{\Gamma_0(\mathfrak{p}_7)}\subset \mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}_7^2)$ of matrices which are upper-triangular modulo $\mathfrak{p}_7$. This morphism is determined by the respective images of the generators of G :

$$M_a=\begin{pmatrix}[-3,3,0] & [1,0,0]\\ [2,-1,0] & [-3,-3,0]\end{pmatrix},\ M_b=\begin{pmatrix}[1,-1,0] & [-3,2,0]\\ [3,2,0] & [1,-1,0]\end{pmatrix}$$

$$M_c=\begin{pmatrix}[1,-3,0] & [0,-1,0]\\ [1,3,0] & [-2,3,0]\end{pmatrix}$$

Define $\mathcal{O}(\mathfrak{p}_7^2) \subset \mathcal{O}(\mathfrak{p}_7)$ as the canonical Eichler suborder of level $\mathfrak{p}_7^2$ relative to the same choice of the embedding $\iota_{\mathfrak{p}_7}$ [namely: elements which map by $\iota_{\mathfrak{p}_7}$ to integral matrices upper triangular modulo $\mathfrak{p}_7$].

The previous data finally allows to compute the monodromy representation relative to the subgroup

$$H \widehat{=} P\mathcal{O}(\mathfrak{p}_7^2)^1 = \overline{\Gamma_0(\mathfrak{p}_7^2)} \subset G = P\mathcal{O}(\mathfrak{p}_7)^1 = \overline{\Gamma_0(\mathfrak{p}_7)}$$

of the units of norm one (modulo -1). Indeed, it is equivalent to quotient everything by the normal subgroup $\overline{\Gamma'(\mathfrak{p}_7^2)} \triangleleft P\mathcal{O}^1$, and compute the monodromy representation of the quotient subgroups $\widetilde{\Gamma_0(\mathfrak{p}_7^2)} \subset \widetilde{\Gamma_0(\mathfrak{p}_7)}$ modulo $\overline{\Gamma'(\mathfrak{p}_7^2)}$.

But, thanks to Proposition III.5.4, reduction modulo $\overline{\Gamma'(\mathfrak{p}_7^2)}$ sends congruence subgroups onto their counterparts in the finite group $\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{N})$ (the groups studied in III.5.3). So it is equivalent to work with these latter subgroups from now on.

We describe the left-representation $\phi_H : G \to (S_7, \circ)$. By Lemmas 3.3 and 5.2, it suffices to compute the left action of the matrices $M_a, M_b, M_c \in \Gamma_0(\mathfrak{p}_7)$ on the subset (ii) of Prop-Def 5.1, equal to $\{(\alpha, 1),\ \alpha \in (\mathbf{Z}_F/\mathfrak{p}_7^2)\backslash(\mathbf{Z}_F/\mathfrak{p}_7^2)^\bullet\}/\sim$. After arbitrarily numbering this subset, we obtain the corresponding triple of permutations :

$$\sigma_{7,2} = [\sigma_a = (1,6,4,2,7,5,3),\ \sigma_b = (1,6,2)(4,5,7),\ \sigma_c = (1,3,4)(2,7,6)]$$

Which satisfy, as expected, $\sigma_a \circ \sigma_b \circ \sigma_c = 1$. Finally these permutations generate the monodromy group of H in S_7, which happens to be of order 3×7.

Caution 3.5. : as warned in example 3.2, the previous triple $\sigma_{7,2}$ alone does not always determine the representation ϕ_H. It determines it *up to the choice of the generators* of G that map to the triples. So, in the case that there would exist two such choices leading to nonconjugate representations, the map ϕ_H would *not* be determined by the sole triple.

Which is what happens here. Indeed, another run of the algorithm with a different presentation for G yields a second triple:

$$\sigma_{7,1} = [\sigma_a = (1,7,4,5,3,6,2),\ \sigma_b = (1,5,7)(3,6,4),\ \sigma_c = (1,2,3)(4,5,6)]$$

which is *non-simultaneously conjugate* to the first one (but generates a conjugate monodromy group, as expected).

These are actually the only two possible triples[3]: an exhaustive search by the algorithm BelyiInit in [Sij$_2$] shows that these are the only ones with this cycle lengths and monodromy group of order 21.

Summing-up: if one fixes arbitrary generators of G, then the monodromy representation ϕ_H of the group H will be necessarily given by one of the two triples $\sigma_{7,1}$ and $\sigma_{7,2}$.

Example 3.6. With the same quaternion algebra as above, consider the prime ideal $(2) = \mathfrak{p}_2 \subset \mathbf{Z}_F$ of norm 8 above the inert prime 2. Then $\overline{\Gamma_0(\mathfrak{p}_2)} \in \mathrm{PSL}_2(\mathbf{R})$ is again a triangle group, of signature $(7,7,2)$.

The computations take place in $\mathrm{PSL}_2(R)$ with R the local ring $\mathbf{Z}_F/\mathfrak{p}_2^2$. The output is the (isomorphism class of) the monodromy group of the subgroup $\overline{\Gamma_0(\mathfrak{p}_2^2)} \subset \overline{\Gamma_0(\mathfrak{p}_2)}$. It is the subgroup of order $2^3.7$ in S_8 generated by anyone of these two triples:

$$\sigma_{2,1} = [(1,5,3,7,8,2,4),\ (1,8,3,2,4,5,6),\ (1,2)(3,4)(5,6)(7,8)]$$
$$\sigma_{2,2} = [(1,3,5,2,6,7,8),\ (1,5,2,8,6,3,4),\ (1,2)(3,4)(5,6)(7,8)]$$

And this time again they represent the two possible simultaneous conjugacy class of triples generating this monodromy group. So, forgetting again the generators of $\Gamma_0(\mathfrak{p}_2)$ that map to these triples, one ends up with two possibilities for the monodromy representation.

Example 3.7. With the same quaternion algebra as above, consider the prime ideal $\mathfrak{p}_3 = (3) \subset \mathbf{Z}_F$ of norm 27 above the inert prime 3. Then $\overline{\Gamma_0(\mathfrak{p}_3)} \in \mathrm{PSL}_2(\mathbf{R})$ is a Fuchsian group of genus one on two generators: U_1, U_2 satisfying $U_1U_2U_1^{-1}U_2^{-1} = 1$ (It is the fundamental group of the pointed elliptic curve $X_0(\mathfrak{p}_3)$). The same computations yield a monodromy group for $\overline{\Gamma_0(\mathfrak{p}_3^2)} \subset \overline{\Gamma_0(\mathfrak{p}_3)}$ of order $3^3.13$.

Comparing the monodromy groups with $\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}^2\mathbf{Z}_F)$

With the same notations and conventions as in sections III.1.2 and III.5, let $\mathfrak{p}$ be a prime of F and $\mathfrak{N}$ an ideal of F. We would like to compare the monodromy groups of the inclusions:

[3] Anticipating on the results of VI5.2, a monodromy computation shows that triples $\sigma_{7,1}$ and $\sigma_{7,2}$ correspond to the inclusions of $\overline{\Gamma_0(\mathfrak{p}_7^2)} \subset \overline{\Gamma_0(\mathfrak{p}_7)}$ and of its Atkin–Lehner conjugate $w_{\mathfrak{p}_7}\overline{\Gamma_0(\mathfrak{p}_7^2)}w_{\mathfrak{p}_7}^{-1} \subset \overline{\Gamma_0(\mathfrak{p}_7)}$ (see also VI.5.4). A direct computation with explicit Atkin–Lehner conjugation of groups would be obviously more satisfactory.

- $\overline{\Gamma_0(\mathfrak{p}^2)} \subset \overline{\Gamma_0(\mathfrak{p})}$, with the group $\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}^2) = \overline{\Gamma_0(1)}/\overline{\Gamma'(\mathfrak{p}^2)}$;
- and of $\overline{\Gamma(1)} \subset \overline{\Gamma_0(\mathfrak{N})}$, with the group $\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{N}) = \overline{\Gamma(1)}/\overline{\Gamma'(\mathfrak{N})}$ (by Proposition III.5.4).

The former is dealt with in this section (and we thank H. Randriam for drawing our attention on this point), on the cases of Examples 3.4 and 3.7. The latter will be dealt in general in Proposition 5.15.

Property 3.8. *With the same quaternion algebra B as in Examples 3.4, 3.6 and 3.7 and for $\mathfrak{p}$ equal to $\mathfrak{p}_7$ or $\mathfrak{p}_3$, the largest normal subgroup N of $G = \overline{\Gamma_0(\mathfrak{p})}$ contained in $H = \overline{\Gamma_0(\mathfrak{p}^2)}$ is* strictly bigger *than $\overline{\Gamma'(\mathfrak{p}^2)}$.*

Thus the Galois closures of the covers (see Theorem 4.7) $X_0(\mathfrak{p}^2) \to X_0(\mathfrak{p})$ are strictly smaller *than $X'(\mathfrak{p}^2) \to X_0(\mathfrak{p})$.*

Proof By the equation (3.1), the quotient G/N has cardinality equal to the monodromy group of the inclusion $H \subset G$. Recall that these monodromy groups for $\mathfrak{p}_7$, $\mathbf{P}_2$ and $\mathfrak{p}_3$ have cardinalities:

$$3.7,\ 2^3.7 \text{ and } 3^3.13\,,$$

as computed in Examples 3.4 and 3.7. On the other hand:

$$[G : \overline{\Gamma'(\mathfrak{p}^2)}] = [\overline{\Gamma_0(\mathfrak{p})}/\overline{\Gamma'(\mathfrak{p}^2)}] = \frac{[\overline{\Gamma(1)} : \overline{\Gamma'(\mathfrak{p}^2)}]}{[\overline{\Gamma(1)} : \overline{\Gamma_0(\mathfrak{p})}]}$$

where the numerator equals $|\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}^2)|$ by Proposition III.5.4 and the denominator is given by the (5.13) of Corollary III.5.6.

Using the formula for $|\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}^2)|$ of Lemma III.5.3, one gets:

$$\big[G : \Gamma(\mathfrak{p}^2)\big] = \boxed{\text{if } 2 \nmid q\text{:}}\ \frac{q^4(q^2-1)(q^2-q)}{2 \times (q^2-q)} \frac{1}{q+1} = \frac{1}{2}q^4(q-1) \tag{3.3}$$

$$\boxed{\text{else:}}\ \frac{q^4}{q \times (1+q)} \frac{(q^2-1)(q^2-q)}{q^2-q} = q^3(q-1) \tag{3.4}$$

Which gives for $\mathfrak{p}_7$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$:

$$3.7^4,\ 2^9.7 \text{ and } 3^{12}.13$$

which are all strictly bigger than the orders of the monodromy groups recalled above. □

4 Arithmetic covers with no topological automorphisms

4.1 A field-theoretic criterion of descent over the field of moduli

Lemma 4.1. *(Partial functoriality of the monodromy representation (1)). Let G be a group, and $N, H \subset G$ two subgroups. Let ϕ_H be the transitive (left) monodromy representation of the subgroup $H \subset G$. Assume that the restriction $\phi_H|_N : N \to S_d$ is* transitive. *Then*

(i) $\phi_H|_N$ is equal to the representation corresponding to $N \cap H \subset N$;

(ii) $\left|\frac{G}{H}\right| = \left|\frac{N}{N \cap H}\right|$

Proof Note N/H the left-classes in G/H that have a representative in N. It is stable under the left-action of N. Consider the injection of sets: $N/H \subset G/H$. Then the assumption that the left-action of N is transitive implies that it is a bijection. In particular there exists a set of representatives n_i of the left classes G/H that all belong to N, thus the first statement.

Next, the set morphism $N \to G/H$ induced by the inclusion being surjective, factorizing on the left by the equivalence modulo H yields the bijection:

$$\frac{N}{N \cap H} \to \frac{G}{H}.$$

hence the second statement. □

Lemma 4.2. *(Partial functoriality of the monodromy representation (2)) Let ψ be an automorphism of G and $G \supset H$ be a subgroup of G of index d. Then if $\phi : G \to S_{G/H}$ is in the conjugacy class of the (left) monodromy representation of $H \subset G$, then the conjugacy class of the representation $\phi' : G \to S_{G/\psi(H)}$, is equal to that of $\phi \circ \psi^{-1}$.*

Proof Let $\{g_i\}_{i=1\ldots d}$ be an ordered set of representatives of the right classes G/H, and choose accordingly the set $\{\psi(g_i)\}_{i=1\ldots d}$ of representatives of $G/\psi(H)$. Let γ be an element of G. Then by definition of ϕ':

$$\gamma.\psi(g_i)\psi(H) \in \psi(g_{\phi'(\gamma)(i)})\psi(H)$$

Composing by ψ^{-1} gives:

$$\psi^{-1}(\gamma).g_iH \in g_{\phi'(\gamma)(i)}H$$

So by definition of ϕ : $\phi(\psi^{-1}(\gamma))(i) = \phi'(\gamma)(i)$. □

This enables to restate the field of definition condition using representations:

Proposition 4.3 ([Dèb$_2$, Prop 4.1.2]). *Let k be a field, k' a Galois extension with group $\Gamma = \mathrm{Gal}(k'/k)$ and $F/k(T)$ a finite Galois extension containing $k'(T)$, with groups $G = \mathrm{Gal}(F/k(T))$ and $N = \mathrm{Gal}(F/k'(T))$. Suppose that the sequence* (Seq/Split) *has a splitting s (for example under the assumptions of Proposition 2.6):*

$$1 \longrightarrow N \longrightarrow G \underset{\pi}{\overset{s}{\rightleftarrows}} \Gamma \longrightarrow 1$$

Consider $E/k'(T)$ a mere extension with fixed field $H \subset N$ of index d and $\phi : G \to S_{N/H}$ the corresponding transitive (left) monodromy representation. Then the data of $E_0/k(T)$ a regular $k(T)$-model of $E/k'(T)$, is equivalent to the data of a group morphism $\varphi : \Gamma \to S_d$ such that for all $x \in N$, and all $\tau \in \Gamma$,

$$\phi\big(s(\tau)xs(\tau)^{-1}\big) = \varphi(\tau)\phi(x)\varphi(\tau)^{-1}.$$

Proof By the splitting, G is isomorphic to the semi-direct product $N \triangleleft \Gamma$. Thus, morphisms $G \to S_d$ correspond to pairs of group morphisms $\{(\phi : N \to S_d, \varphi : \Gamma \to S_d)\}$ that are compatible to the semi-direct product.

Finally, ϕ being transitive, any prolongation $(\phi, \varphi) : G \to S_d$ is transitive. So by the correspondence of Proposition 3.1, arises from a subgroup $H_0 \in G$ of index d. Finally, the restriction ϕ of (ϕ, φ) to N being transitive, (i) of the Lemma 4.1 implies that $H_0 \cap N = H$. □

And likewise to restate the field of moduli condition:

Lemma 4.4 ([Dèb$_2$] Prop 4.4.3). *Same assumptions as in Definition 2.7*

⌈let k be a field of characteristic zero, k'/k a finite Galois extension of group Γ, $E/k'(T)$ a finite (G-) extension of degree d. Let $F/k(T)$ be a Galois closure containing E. Let again G and N be the Galois group of $F/k(T)$ and $F/k'(T)$, and for each $\tau \in \Gamma$, note $s(\tau) = \widetilde{\tau}$ any prolongation of τ to G fixing $k(T)$.⌋

Let now $H \subset N$ be the subgroup fixing E and ϕ the corresponding representation. Then an element $\tau \in \Gamma$ fixes the field of moduli of E if and only if there exists $\varphi_\tau \in S_d$ such that for all $x \in G$,

$$\phi\big(s(\tau)^{-1} x s(\tau)\big) = \varphi_\tau \phi(x) \varphi_\tau^{-1}.$$

Proof N being normal in G, the conjugation by $s(\tau)$ is an (outer) automorphism of N. So by Lemma 4.2, the monodromy representation associated to $s(\tau) H s(\tau)^{-1}$ is equal to $x \to \phi\big(s(\tau)^{-1} x s(\tau)\big)$.

Next, noting $\chi_\tau \in N$ the conjugating element as in 2.7, the point (ii) in Prop-Def 3.1 shows that the representation associated to the conjugate subgroup $\chi_\tau H \chi_\tau^{-1}$ is equal to a conjugate permutation, say $x \to \varphi_\tau^{-1} x \varphi_\tau\big)$. □

Let $\phi(N)$ be the monodromy group of $H \subset N$. Notice that for all τ_1, $\tau_2 \in \Gamma$, the quantity

$$\varphi_{\tau_1 \tau_2}^{-1} \varphi_{\tau_1} \varphi_{\tau_2}$$

Belongs to the centralizer $C = \mathrm{Cen}_{S_d}(\phi(N))$. Thus if it is trivial, the φ_τ define a group morphism $\Gamma \to S_d$ and the proposition 4.3 applies:

Corollary 4.5 ([Dèb$_2$, Prop 4.4.4])**.** *Under the same assumptions as in 4.4, suppose that the field of moduli of E is k. Then if $\mathrm{Cen}_{S_d}(\phi(N)) = \{1\}$, E comes from a regular extension $E_0/k(T)$.*

Remarks 4.6. This can be seen as an analog of Weil's descent theorem for quasi-projective varieties with no automorphisms [MilAG, Th. 16.32]. Indeed by Theorem 4.7 (iii)&(v) and Theorem 4.9, the centralizer $\mathrm{Cen}_{S_d}(\phi(N))$ is antiisomorphic to the automorphism group of the corresponding topological cover. But a direct proof showing that it is the automorphism group of the field extension would be way more satisfactory!

Other descent criteria are derived in [Dèb$_2$, Prop 4.4.4] with the same approach of obtaining such a group morphism $\Gamma \to G$. With more work, [DèbDo] express the obstruction to its existence, as a cohomology class with coefficients in the center of the monodromy group $Z(\phi(N))$. Thus they obtain the striking corollary 3.2, that descent is possible as soon as this center is trivial.

4.2 Characterization and descent from topological monodromy

The Galois theory of connected covers of topological spaces basically states:

- a dictionary between subgroups of the π_1 of the base, and connected covers
- such that the action of the π_1 on the fiber –by prolongation of paths– corresponds to the monodromy representation of the subgroup
- and such that the automorphisms of the cover are the permutations of the fiber that commute with the action of the π_1.

It can be summarized as follows:

Theorem 4.7. *Let $\boldsymbol{t} = \{t_1, \dots, t_r\}$ a set of points in $\mathbf{P}^1_{\mathbf{C}}$ and $f : X \to \mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}$ a topological (non ramified) connected covering of degree d. Fix a point $t_0 \in \mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}$. Then the lifting property of paths defines a* right*-action of $\pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0)$ on the preimage $f^{-1}(z_0)$. The representation ρ of $\pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0)$ in S_d induced is defined up to conjugation in S_d. It is called the* topological monodromy representation.

(i) [Don, §4 prop. 7 and §4.2.2] Let x_0 be a point of X. Then the conjugacy class of ρ coincides *with the class of the right-monodromy representation ϕ of the subgroup $f_*(\pi_1(X, x_0)) \subset \pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0)$.*

(ii) [Don, idem] Note $\widetilde{X}$ the universal covering space of X. Then modulo isomorphisms of covers and conjugacy in S_d, one has the following bijection of isomorphism classes:

$$\left\{\begin{matrix}\textit{Isom. classes of top. connected} \\ \textit{covers of degree } d \quad f : X \to \mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}\end{matrix}\right\} \quad \left\{\begin{matrix}\textit{Conjug. classes of transit. right-} \\ \textit{repres. } (S_d, .) \leftarrow \pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0)\end{matrix}\right\}$$

$$X = \widetilde{X}/H \longleftarrow\!\!\!\longleftarrow\!\!\!\dashv H \subset \pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0).$$

(iii) [Dèb$_2$, th 7.6.1] The group of automorphisms $\mathrm{Aut}(f)$ *acts on the* left *on the preimage $f^{-1}(z_0)$. This defines an* injection *in $(S_d, \circ)/\sim$, whose image is equal to the centralizer in S_d of the monodromy group $\phi(\pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0))$ (acting on the* right *on the preimage). These two actions thus define the antiisomorphism:*

$$(S_d, \circ) \supset \mathrm{Aut}(f) \xrightarrow{anti \sim} \mathrm{Cen}_{S_d}\Big(\phi\big(\pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0)\big)\Big) \subset (S_d, .)$$

(iv) [Dèb$_2$, th 7.7.1] Suppose now that the covering f is Galois. Then the left *action of* $\mathrm{Aut}(f)$ *is* transitive. *Moreover by a group-theoretic lemma,*

the previous anti-isomorphism induces an anti-isomorphism with the monodromy group itself :

$$\mathrm{Aut}(f) \xrightarrow{\sim} \phi\big(\pi_1(\mathbf{P}^1_{\mathbf{C}}\backslash \boldsymbol{t}, t_0)\big) \cong \frac{\pi_1(\mathbf{P}^1_{\mathbf{C}}\backslash \boldsymbol{t}, t_0)}{f_*(\pi_1(X, x_0))}$$

(v) *In particular, (iii), (iv) and equation* (3.1) *of 3.1 show that the monodromy group of a cover is* equal *to the automorphism group of the Galois closure.*

Thanks to the dictionnary above, it is possible to prove that in the case of Riemann surfaces, then –up to isomorphism– the topological cover f comes from a *compact analytic ramified* cover defined above the missing points $\boldsymbol{t}$. This is Riemann's (analytic) existence theorem:

Theorem 4.8 ([Don, §4.2.2] or [Dèb$_2$, §8.2.1])**.** *Let $\mathcal{X}$ be a* compact *connected Riemann surface, $F : \mathcal{X} \to \mathbf{P}^1_{\mathbf{C}}$ a proper analytic map of degree d which is ramified above $\boldsymbol{t} \subset \mathbf{P}^1_{\mathbf{C}}$ and let $X = \mathcal{X} - f^{-1}(\boldsymbol{t})$ be the (punctured) Riemann surface. Then, the restriction of F to the topological (unramified) covering $f : X \to \mathbf{P}^1_{\mathbf{C}}\backslash \boldsymbol{t}$, ([Don, §4.1] or [Dèb$_2$, th. 8.3.3]) defines the first arrow of the following bijection of isomorphism classes:*

$$\left\{\begin{array}{c}\textit{Isom. classes of proper analytic}\\ \textit{maps } F : \mathcal{X} \to \mathbf{P}^1_{\mathbf{C}}\\ \textit{of degree } d \textit{ with } \mathcal{X} \textit{ compact.}\end{array}\right\} \qquad \left\{\begin{array}{c}\textit{Isom. classes of top. connected}\\ \textit{covers of degree } d \;\; f : X \to \mathbf{P}^1_{\mathbf{C}}\backslash \boldsymbol{t}\end{array}\right\}$$

$$F \longmapsto f \quad (\textit{restriction})$$

$$[\textit{fill above the branch points}] \longleftarrow\!\shortmid\; f$$

Finally, the following theorem states (i) that a compact analytic cover is birational to the analytification –call this functor $(.)^{\mathrm{an}}$– of an *algebraic* cover $f : \mathcal{X} \to \mathbf{P}^1_{\mathbf{C}}$ (def. 2.1). (ii) and that, up to fixing a finite Galois closure, the two monodromy representations correspond (the one from Galois theory of fields, and the one from topological coverings (ρ, as in th. 4.4)).

Theorem 4.9. *Let $P(T, Y)$ an irreducible polynomial in $\mathbf{C}[T, Y]$ such that $\deg_Y(P) > 0$. Consider the function field $E = \mathbf{C}[T, Y]/P(T, Y)$. Then the projection to T induces an algebraic cover of degree d (up to birational map):*

$F : \mathcal{X} \to \mathbf{P}^1_{\mathbf{C}}$, where $\mathcal{X}$ is an integral smooth projective curve with function field E [Dèb$_2$, §8.3.5 & th. 8.3.12]. Note this $F = Cover(E)$.

For the reciprocal correspondence, let $\mathcal{X}$ be a compact Riemann surface and $f : \mathcal{X} \to \mathbf{P}^1_{\mathbf{C}}$ be an analytic cover. Then the image of the induced morphism between function fields:

$$f^*M(\mathbf{P}^1_{\mathbf{C}}) \hookrightarrow M(\mathcal{X})$$

is equal to the subfield $\mathbf{C}(f)$ [Dèb$_2$, th. 8.3.6]. Furthermore the field extension $[M(\mathcal{X}) : \mathbf{C}(f)]$ is of degree d [Dèb$_2$, th. 8.3.11].

This induces the bijection of classes:

$$\left\{\begin{array}{c}\textit{Isom. classes of separable}\\ \textit{field extensions of}\\ \textit{degree } d\ \ [E : \mathbf{C}(T)]\end{array}\right\} \qquad \left\{\begin{array}{c}\textit{Birat. classes of proper analytic}\\ \textit{maps } F : \mathcal{X} \to \mathbf{P}^1_{\mathbf{C}}\\ \textit{of degree } d \textit{ with } \overline{X} \textit{ compact.}\end{array}\right\}$$

$$E \longmapsto F^{an} : \mathcal{X}^{an} \to \mathbf{P}^1_{\mathbf{C}} \qquad \text{via } (.)^{an} \circ \mathrm{Cover}$$

$$[M(\mathcal{X}) : \mathbf{C}(f)] \longmapsfrom f : \mathcal{X} \to \mathbf{P}^1_{\mathbf{C}}$$

Moreover [Dèb$_2$, 8.3.12 c)] the extension $[E : \mathbf{C}(T)] = [M(\mathcal{X}) : \mathbf{C}(f)]$ is Galois if and only if the corresponding topological cover $f : X \to \mathbf{P}^1_{\mathbf{C}}$ (restriction of F to the smooth locus) is Galois. In this case the pullback of maps: $\left\{\begin{array}{c}\mathrm{Aut}(f) \longrightarrow \mathrm{Gal}([M(\mathcal{X}) : \mathbf{C}(f)])\\ \chi \to \chi^*\end{array}\right.$ *defines an anti-isomorphism.*

The next theorem shows that descent of covers from $\mathbf{C}$ to $\overline{\mathbf{Q}}$ is unique:

Theorem 4.10 ([Dèb$_1$, §12])**.** *Let $\boldsymbol{t} \subset \mathbf{P}^1_{\mathbf{C}}$ be a $\overline{\mathbf{Q}}$-rational set of points. Then any algebraic unramified (étale) cover $W \to \mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}$ descends to cover of $\mathbf{P}^1_{\overline{\mathbf{Q}}} \backslash \boldsymbol{t}$, which is furthermore* unique *up to $\overline{\mathbf{Q}}$-isomorphisms.*

Remark 4.11. In the demonstration proposed in [Se$_2$, th 6.3.3], the statement:

$$\pi_1(X \times Y) = \pi_1(X) \times \pi_1(Y) \tag{4.1}$$

holds in the case where at least one of the two factors X or Y is *compact* ([Sza, cor 5.6.6]).

But the situation here is as follows: $\overline{\mathbf{Q}} \subset K \subset \mathbf{C}$ is an algebraically closed field, $K' = K(t)$ a transcendental extension of degree 1, and one of the two factors above : $X = \mathbf{P}^1_K \backslash \boldsymbol{t}$ is *not compact*. So it is needed that Y be compact.

Although the author claims that it is exactly the case: $Y = C = \mathbf{P}^1_K$, the problem is that to prove this, the author needs that any unramified cover $W \to X \times_K K(t)$ does extend to $W \to X \times_K \mathbf{P}^1_K$ (although it is a priori only defined on the generic fiber). Which is not obvious, at least in higher dimension : for example the argument of [Sza, cor 5.6.6] would only show that the morphism extends to an *affine subset* Y of $\mathbf{P}^1_K$.

But there exists a way around, using Bertini's connectedness theorem, which is specially devised to avoid the formula (4.1): see [Sza, Remark 5.7.8] and the proof of 5.7.6 above. This approach generalizes [Dèb$_1$, §12] for the case of covers with arbitrary smooth connected projective base.

This finally allows to state a criterion that guarantees the unicity –and sometimes the existence– of the descent an algebraic cover, only from its topological monodromy representation:

Theorem 4.12. *Let $\overline{\mathbf{Q}} \supset k' \supset k \supset \mathbf{Q}$ be a Galois extension of number fields with group $\Gamma = \mathrm{Gal}(k'/k)$. Consider an algebraic cover $f : X \to \mathbf{P}^1_{k'}$ of degree d ramified at most over a finite set $\boldsymbol{t} \subset \mathbf{P}^1_{\bar{k}}$, and let $\rho : \pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0) \to (S_d, .)$ be its topological monodromy representation.*

(i) Suppose that the monodromy group $\rho\big(\pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0)\big)$ has trivial centralizer *in S_d, then f has* at most *one model*[4] *over k: $f_0 : X_0 \to \mathbf{P}^1_k$.*

(ii) Suppose furthermore that the field of moduli of f is k. Then f does have a model over k.

Proof Let $F/k(X)$ be a Galois extention that contains the extension $E/k'(X)$ corresponding to f. Let again $G = \mathrm{Gal}(F/k(T))$ and $N = \mathrm{Gal}(F/k'(T))$ be the corresponding Galois groups, $H \subset N$ the subgroup corresponding to E and $\phi : N \to S_d$ its monodromy representation. By the last statement of Theorem 4.9, and by (i), (iii) and (v) of Theorem 4.7, the centralizer $\mathrm{Cen}_{S_d}\phi(N)$ is equal to $\mathrm{Cen}_{S_d}\big(\rho(\pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0))\big)$. Which is trivial by assumption. The second statement now follows from Corollary 4.5.

[4] It can be seen as a GAGA instance of the general principle stated in [Se$_1$, III.1)]. Indeed by Theorem 4.7, $\mathrm{Cen}_{S_d}(\phi(\pi_1(\mathbf{P}^1_{\mathbf{C}} \backslash \boldsymbol{t}, t_0))) \subset (S_d, .))$ is anti-isomorphic to the automorphism group of the cover. Once again, a purely field-theoretic proof of this, that wouldn't involve the topological monodromy, would be very welcome!

For the unicity, suppose now that there exists two models $E_0/k(X)$ and $E_0'/k(X)$ of E over k. Then by the correspondence of Proposition 4.3, they would respectively be determined by group morphisms $\varphi, \varphi' : \Gamma \to S_d$ such that for s a fixed section of the exact sequence and for all τ in Γ,

$$\phi\big(s(\tau)xs(\tau)^{-1}\big) = \varphi(\tau)\phi(x)\varphi(\tau)^{-1},$$

(and similarly for φ'). But these two relations then imply that $\varphi(\tau)\varphi'(\tau)^{-1}$ is in $\mathrm{Cen}_{S_d}\phi(N) = \{1\}$. So φ and φ' coincide, and so do E_0 and E_0'. □

5 Descent of the canonical covers $X_0(\mathcal{N}) \to X(1)$

The conventions are those laid in §III.1.2, and in §III.5.1 for the congruence subgroups. In particular $\mathcal{O}$ is a maximal order. The additional assumption made at the beginning of Chapter IV also holds (unicity of the split real place).

This last assumption implies that the field F is totally real (otherwise the complex place would be split).

Let $\mathfrak{N}$ be a ideal of F and ∞ the infinite places of F. Then let $F(\mathfrak{N}.\infty)$ be the abelian extension associated to the ray class group of modulus $\mathfrak{N}.\infty$. In particular when $\mathfrak{N} = 1$, one recovers the narrow class field $F_\infty = F(\infty)$ of Definition III.1.1.

Set $X_0(\mathfrak{N})$, $X_0(\mathfrak{N})^+$, $X(\mathfrak{N})$, $X(\mathfrak{N})^+$ and $X'(\mathfrak{N})$ for the quotients of the upper half plane $\mathcal{H}$ by $\Gamma_0(\mathfrak{N})$, $\Gamma_0^+(\mathfrak{N})$ etc.

5.1 Canonical models and their reduction

Shimura provides canonical models for the analytic quotients of the upper-half plane by principal congruence subgroups :

Theorem 5.1. *Consider the compact Riemann surface $\Gamma^+(\mathfrak{N})\backslash\mathcal{H}$. Then there exists:*

- *a smooth projective curve $X(\mathfrak{N})^+$ over the class field $F(\mathfrak{N}\infty) \subset \mathbf{C}$;*
- *and a holomorphic function $\varphi : \mathcal{H} \to X(\mathfrak{N})^+ \times_{F(\mathfrak{N}\infty)} \mathbf{C}$;*

which is the unique morphism, up to a compatible $F(\mathfrak{N}\infty)$-isomorphism of curves, that satisfies the following:

(i) [Sh_1, Th. 3.2 & 3.3] φ induces a biholomorphism

$$\Gamma(\mathfrak{N})\backslash\mathcal{H} \to X^+(\mathfrak{N}) \times_{F(\mathfrak{N}\infty)} \mathbf{C}\,,$$

(ii) [Sh_1, 3.2.3 (canonical model condition)] Let $\mathcal{O}$ a maximal order that contains the Eichler order of level $\mathfrak{N}$ involved. Then for all purely quadratic imaginary extension L of F such that $\mathbf{Z}_L \subset \mathcal{O}$, let $z \in \mathcal{H}$ be the fixed point of L. Then z comes from an algebraic point of $X(\mathfrak{N})^+$, *whose field of coordinates $\kappa(z)$ generates the class field of L: $L.F(\mathfrak{N}\infty)\kappa(z) = L(N\infty)$. z is called a* CM-point *for L.*

Similarly, canonical models $X_0^+(\mathfrak{N})$ for the Riemann surfaces $\Gamma_0^+(\mathfrak{N})\backslash\mathcal{H}$ exist and are all defined over the narrow class field[5] *$F_\infty = F(\infty)$.*

They are furthermore functorial with respect to the inclusion of congruence subgroups[6]*.*

Theorem 5.2 ([Sh_1, Th. 3.17 simplified])**.** *In addition to the assumptions of the section, suppose that $\mathfrak{N} = 1$ and that F is of* narrow class number one. *Let z be a CM point for L as above , then the action of* $\mathrm{Gal}(\mathbf{C}/F)$ *on $X^+(1)$ sends CM-points for L to CM points*[7] *for L.*

Example 5.3 (Triangle groups from maximal orders [Sh_1, 3.18.3]). Suppose again that F is of *narrow class number one.* Suppose that the Fuchsian group $\overline{\Gamma^+(1)} \subset \mathrm{PSL}_2(\mathbf{R})$ is a triangle group with *distinct* indices a, b, c. Then Shimura's canonical model over F for the Riemann surface $\Gamma^+(1)\backslash\mathcal{H} = \mathbf{P}^1_{\mathbf{C}}$ has three rational points. And in particular is equal[8] to $\mathbf{P}^1_F$.

Proof: consider the elliptic point z_a of order a. Then it comes from an algebraic CM-point for the (strictly) quadratic cyclotomic extension $F(\zeta_a)$. So by Theorem 5.2, this CM-point is mapped under $\mathrm{Gal}(\mathbf{C}/F)$ to a CM-point for $F(\zeta_a)$. But the orders of the three elliptic points being distinct, it is mapped to itself.

---

[5] See for example [Duc, formula IV.2] for a treatment in the modern approach.

[6] I.e.: quotienting the upper-half plane by a larger congruence subgroup yields a functorial map $X_0^+(\mathfrak{N}) \to X_0^+(\mathfrak{N}')$ between the two models: see [Del, Corollary 5.4], defined over F_∞ (by [MilSV, Theorem 13.6], the field of definition of the connected components $X_0^+(\mathfrak{N})$ being F_∞ by [Sij_1, (3.6)]). So we are surprised not to be able to descend the map f_2 in VI.5.1.

[7] Indeed, the condition on τ in loc. cit. is empty because $F(\infty.\mathfrak{N}) = F$. The automorphisms being taken over F (and not only L), this statement is in a sense stronger than the prediction of the [Sh_1, Th. 3.5] in this particular case (see the formula (4) in the introduction of loc. cit.). But we don't know if there also exists a reciprocity formula over F (and not only L).

[8] A similar argument, using the automorphisms of $\mathbf{P}^1_{\mathbf{C}}$ and Theorem 5.6, enables [Hal, Proposition 1] to prove that $\mathbf{P}^1_F$ is also a canonical model in the cases where $\Gamma_0^+(1)$ has (i) exactly three elliptic points of the same order, along with (ii) a fourth elliptic point of distinct order.

Theorem 5.4 (Reduction with many points [Duc, Th IV.4.5]). *Let $\mathfrak{p}$ be a prime of $\mathbf{Z}_F$ of norm $q = |\mathfrak{p}|$ which: (i) does not divides the finite discriminant $\mathfrak{D}$ of B nor the level $\mathfrak{N}$ (ii) and has trivial class in $\mathrm{Cl}_\infty(F)$. Consider $\mathfrak{P}$ a prime above $\mathfrak{p}$ in the narrow class field F_∞.*

Then the canonical model $X_0^+(\mathfrak{N})$ (over F_∞) has good reduction modulo $\mathfrak{P}$ over $\mathbf{F}_q$.

Under these conditions, allow the discriminant $\mathfrak{D}$ and level $\mathfrak{N}$ to vary such that the genera sorted in increasing order: $g_i = g_{\mathfrak{N},\mathcal{D}} = g(X_0^+(\mathfrak{N}))$ tend to infinity.Then the number of $\mathbf{F}_{q^2}$-points is asymptotically optimal:

$$\frac{|X_0^+(\mathfrak{N}_i)(\mathbf{F}_{q^2})|}{g_i} \xrightarrow[i\to\infty]{} q-1$$

Let $T = T(\mathfrak{p})$ be the Hecke operator [Duc, p63] acting on the Jacobian of the Riemann surface $\mathrm{Jac}(X_0^+(\mathfrak{N}))$. The dual of this action on the classes of divisors, is an action on the space of holomorphic differentials , which identify themselves to the quaternionic modular cuspforms for the group $\Gamma_0^+(\mathfrak{N})$.

Theorem 5.5 (Point counting). *Under the conditions of Theorem 5.4, let $T = T(\mathfrak{p})$ be the Hecke operator acting on the Jacobian of the Riemann surface $\mathrm{Jac}(X_0^+(\mathfrak{N}))$. Then the number of points of the curve reduced at $\mathfrak{p}$ is:*

$$\left|\overline{X_0^+(\mathfrak{N})}(\mathbf{F}_q)\right| = q + 1 - \mathrm{Tr}(T) \tag{5.1}$$

$$\left|\overline{X_0^+(\mathfrak{N})}(\mathbf{F}_{q^2})\right| = q^2 + 1 - \mathrm{Tr}(T^2) + 2qg \tag{5.2}$$

Proof Apply [Duc, Corollary 2.7] and, to obtain the second equation in this form, replace $T(\mathfrak{p}^2)$ using [Duc, Corollary 2.3] with $r = 1$. □

5.2 Field of moduli: the Theorem of Doi–Naganuma

Doi and Naganuma show that the quaternion algebra with conjugate discriminant leads to the conjugate canonical model. Which implies a field of moduli property under Galois-invariant conditions.

One considers once and for all a subfield $F \subset \mathbf{C}$. Let us call $\iota = \iota_v$ this set-theoretic inclusion, corresponding to the place v. By the asumption laid in the first paragraph of Chapter IV, v is the unique real place of F that splits the quaternion algebra B.

Then, let σ be an automorphism of $\mathbf{C}$. The set-theoretic image $\sigma F = \sigma(F)$ is the field. Denote $\iota_{\sigma F}$ the set-theoretic inclusion $\sigma F \subset \mathbf{C}$, which is also a field inclusion. It thus corresponds to a place $v_{\sigma F}$ of σF. [9]

Theorem 5.6 ([DN, Theorem])**.** *Let B' be the quaternion algebra over σF which is ramified exactly at:*

- the infinite place $\iota_{\sigma F}$;

- and the conjugate $\sigma(\mathfrak{D})$ of the finite places $\mathfrak{D}$ where B is ramified.

Consider $\mathcal{O}(\mathfrak{N})$ an Eichler order of level $\mathfrak{N}$ in B, and $X^+(\mathfrak{N})_{F_{\mathfrak{N}\infty}}$ the canonical model for the corresponding group of totally positive units $\Gamma^+(\mathfrak{N})$ (cf. III.5.1 and Theorem V.5.1)

Then the conjugate curve ${}^{\sigma}X^+(\mathfrak{N})$ is a canonical model, over the class field $\sigma F_{\sigma(\mathfrak{N})\infty}$, for the subgroup of totally positive units of a certain Eichler order $\mathcal{O}'(\sigma(\mathfrak{N}))$ of level $\sigma(\mathfrak{N})$ in B'.

The same result holds when considering the canonical models $X_0(\mathfrak{N})^+$ over F_∞, and their conjugates ${}^{\sigma}X_0(\mathfrak{N})^+$ over σF_∞.

Similarly, there exists isomorphisms between the curves $X_0^+(\mathfrak{N})$ and their conjugates: see e.g. [Moo, 2.14 Theorem] (or [MilClo, Theorem 5.5]) for the modern approach.

Remark 5.7. It seems to us that an important point must be clarified in the litterature.

Suppose that $\sigma F = F$, so that $\iota = \iota_{\sigma F}$.

Suppose in addition that $\sigma(\mathfrak{D}) = \mathfrak{D}$.

Then in Theorem 5.6 one has $B' = B$.

But attention : *B' is not the conjugate algebra ${}^{\sigma}B = B \otimes_{F,\sigma} F$.* Because ${}^{\sigma}B$ is ramified at the infinite place $\iota \circ \sigma^{-1}$, which is different from $\iota = \iota_{\sigma F}$.

Assume e.g. that there is only one conjugacy class of Eichler orders of a fixed level. Then the canonical model for the congruence group $\Gamma(\sigma(\mathfrak{N}))^+$ of the conjugate algebra ${}^{\sigma}B$ is *trivially equal* to $X(\mathfrak{N})^+$, *and not* to ${}^{\sigma}X(\mathfrak{N})^+$ ("sens évident" in [Vig$_2$, Theorem 3])

Example 5.8. Let us describe the curves referenced as e5d5D5i/ii in [Sij$_3$, Tables A.1/2/3] (they will also serve as Counterexamples 5.18). Let F be the quadratic field with polynomial $t^2 - t - 1$ and non-trivial automorphism σ. Let $\mathfrak{p}_5$ the prime ideal above the ramified prime 5, and $\mathfrak{p}_{11}$ and $\sigma(\mathfrak{p}_{11})$ the two primes above the split (11). Fix a real place ι of F.

[9] so that if $\sigma F = F$, then $v_{\sigma F} = v$

Let B be the quaternion algebra with finite discriminant $\mathfrak{p}_5$ and split exactly at ι.

Consider the two congruence groups $\Gamma_0(\mathfrak{p}_{11})$ and $\Gamma_0(\sigma(\mathfrak{p}_{11}))$. This has a meaning since B has a unique conjugacy class of Eichler orders of given level, because the narrow class number of F equals one.

Then the canonical models of these congruence groups: $X_0(\mathfrak{p}_{11})$ =e5d5D5i and $X_0(\sigma(\mathfrak{p}_{11}))$ =e5d5D5ii, have conjugate Jacobians over F: see Table A.3 of loc. cit.)

How can one explain this ? We are in the same situation than in the previous remark: the discriminant being Galois-invariant, the algebra B' of Theorem IV.4.5 restated above is equal to B. Thus by Theorem 5.6, the conjugate curve ${}^{\sigma}X_0(\mathfrak{p}_{11})$ is equal to $X_0(\sigma(\mathfrak{p}_{11}))$.

Example 5.9. Let us recompute Example 3 page 21 of Voight–Willis 2013. There is a slight typo in the reference: with minimal polynomial $a^2 + a - 1$, then the value of a should be the opposite of what is stated in the first paragraph of Example 3 in the reference. Let us detail our input and results below:

The totally real field is $F\langle a\rangle$, of degree 2 over $\mathbf{Q}$ and with minimal polynomial $a^2 + a - 1$.

We generate an algebra B ramified at: the prime $\mathfrak{p} = (5a + 2)$ with $N(\mathfrak{p}) = 31$, and the place which sends $a \to A = -1.61...$ (and not $-0.61...$)

We generate a CM point fixed by an embedding of the CM extension of polynomial $y^2 + y + 2$, as the origin of the power series expansions

$\to$ We obtain the same j-invariant as in the paper, equal to $-18733.423...$ Which is recognized as the embedding of

$$-(11889611722383394a + 8629385062119691)/31^8$$

by the split real place.

Then: we generate the conjugate quaternion algebra B^σ as in Remark 5.7, i.e. where the ramified places are the conjugates of both the finite and infinite ramified places of B.

$\to$ We get the same j-invariant "j^σ" $= j = -18733.423..$, as predicted by the trivial statement of Remark 5.7.

Now: we generate the "Doi-Naganuma" quaternion algebra B' as in Theorem 5.6. I.e. B' is ramified at the conjugate of $\mathfrak{p}$, but at the same infinite place as B.

$\rightarrow$ We find the conjugate j-invariant : $j' = 12438.17832...$, equal to the embedding of $-(11889611722383394a + 8629385062119691)/31^8$ by the ramified real place. So it is indeed the conjugate of j, as predicted by Theorem 5.6.

To be sure, we also check that the conjugate algebra $B^{\sigma'}$ also leads to the same j-invariant: $j^{\sigma'} = j'$.

Corollary 5.10 ([DN, Corollary, slightly relaxed]). *Suppose furthermore that:*

(i) F *is* Galois *over* $\mathbf{Q}$*;*
(ii) B *has a* unique conjugacy class of maximal orders*;*
(iii) the discriminant $\mathfrak{D}$ *is* $\mathrm{Gal}(F/\mathbf{Q})$-invariant*;*
(iv) the level $\mathfrak{N}$ *is* $\mathrm{Gal}(F/\mathbf{Q})$-invariant.

Then $\mathbf{Q}$ *is the field of moduli (as a mere curve) of the canonical model* $X^+(\mathfrak{N})$ *of* $\Gamma^+(\mathfrak{N})\backslash\mathcal{H}$.

5.3 Field of moduli of canonical covers

We would like to show more in the case of triangle groups:

Theorem 5.11. *In addition to the assumptions of Corollary 5.10, suppose furthermore that*

(ii') *(⇒ ii) F is of narrow class number one. [Thus: $F(\infty) = F$, and* $\boxed{\Gamma^+(\mathfrak{N}) = \Gamma(\mathfrak{N})\ \textit{and}\ \Gamma_0^+(\mathfrak{N}) = \Gamma_0(\mathfrak{N})}$ *by III.3.2];*
(v) the group $\overline{\Gamma(1)} \widehat{=} \bar{\iota}(\mathcal{O}^1) \subset \mathrm{PSL}_2(\mathbf{R})$ *is a* triangle group with elliptic points of distinct orders.

Then $\mathbf{Q}$ *is the field of moduli of the canonical* cover $X(\mathfrak{N}) \rightarrow X(1)$. *The same result holds for the canonical cover* $X_0(\mathfrak{N}) \rightarrow X(1)$.

Proof As in Theorem 5.1, let φ, $\varphi_{\mathfrak{N}}$, φ_σ and $\varphi_{\sigma,\mathfrak{N}}$ the biholomorphisms defining the canonical models of $X(1) = \mathbf{P}^1_F$, ${}^\sigma X(1) = \mathbf{P}^1_F$, $X(\mathfrak{N})$ and ${}^\sigma X(\mathfrak{N})$. By the assumption (ii') and the example 5.3, the three elliptic-CM points on both the models $\mathbf{P}^1_F$ are F-rational. So composing by a F-isomorphism, one can choose them to be at $0, 1, \infty$ with the same orders on both $\mathbf{P}^1_F$.

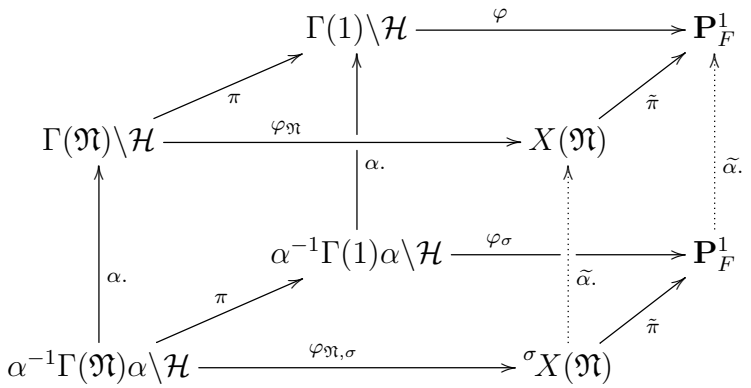
As in 5.6, let $\mathcal{O}'$ be the maximal order of $B' = B$ that gives rize to ${}^\sigma X(\mathfrak{N})$. By assumption it is conjugate in B to $\mathcal{O}$: let α be the conjugating element. Then the left multiplication by α acting on $\mathcal{H}$, induces an isomorphism $\alpha.$ from the complex quotient $\Gamma'(\mathfrak{N})\backslash\mathcal{H} = \alpha^{-1}\Gamma(\mathfrak{N})\alpha\backslash\mathcal{H}$ to $\Gamma(\mathfrak{N})\backslash\mathcal{H}$ (and similarly for $\Gamma(1)$).

We follow the argument of [Sh$_1$, 3.14.3]: consider the biholomorphism $\phi_{\mathfrak{N}} \circ \alpha$. It realises $X(\mathfrak{N})$ as a canonical model for the conjugate Eichler order $\alpha^{-1}\mathcal{O}(\mathfrak{N})\alpha$. Thus by unicity of the canonical model (Theorem 5.1), there exists a compatible $F(\mathfrak{N})$-isomorphism $\widetilde{\alpha}.$ between ${}^{\sigma}X(\mathfrak{N})$ and $X(\mathfrak{N})$ (and similarly a compatible F-isomorphism $\widetilde{\alpha}.$ for $\Gamma(1)$).

But the image by $\alpha.$ of the elliptic points on $\alpha^{-1}\overline{\Gamma(1)}\alpha\backslash\mathcal{H}$ are the elliptic points in the same order for $\overline{\Gamma(1)}\backslash\mathcal{H}$. So the induced morphism $\widetilde{\alpha}.$ sends the points $0, 1, \infty$ of $\mathbf{P}^1_F$ to the points $0, 1, \infty$ of $\mathbf{P}^1_F$, thus is the *identity*.

So that the right-face of the commutative cube ($\square$):

($\square$)



is in fact a $F(\mathfrak{N})$-isomorphism of *covers* of $\mathbf{P}^1_F$. $\square$

5.4 Field of definition

Descent and topological characterisation

Under the assumptions of Theorem 5.11, the cover $X(\mathfrak{N}) \to X(1)$ being also *Galois*, the Proposition A.1.6 implies that *the cover is defined over* $\mathbf{Q}$. We would like to draw the same conclusion for the *nonGalois* covers $X_0(\mathfrak{N}) \to X(1)$:

Proposition 5.12. *Let B be a quaternion algebra over a number field F which has at least one split infinite place. Let $\mathfrak{N}$ be an ideal of $\mathbf{Z}_F$ the ring of integers of F. Fix a maximal order $\mathcal{O}$ along with nested congruence subgroups of units of* norm one*: $G = \overline{\Gamma(1)}$, $H = \overline{\Gamma_0(\mathfrak{N})}$.*

Then, [excepted in the case $\{F = \mathbf{Q}$ and $2|\mathfrak{N}\}$] the monodromy group of the subgroup $H \subset G$ has a trivial centraliser in $S_{G/H}$.

Thus the topological cover $X_0(\mathfrak{N}) \to X(1)$ has a trivial automorphisms group.

Proof By [Dèb$_2$, Lemme 7.6.5], it suffices to show that $\mathrm{Nor}_G H/H = \{1\}$.

Recall that the kernel $\Gamma'(\mathfrak{N})$ of the natural map from G to $\mathrm{PSL}_2(\mathfrak{N})$, is also included (normal) in H. So it is sufficient to prove the proposition after quotienting everything by $\Gamma'(\mathfrak{N})$ (exercice). Note $\widetilde{G}$ and $\widetilde{H}$ the quotients (i.e. the images in $\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{N})$).

From the Chinese remainder (Sun Tsu) decomposition of Lemma III.5.3 (iv), it is also sufficient to prove the proposition it in each component. Namely for each prime factor $\mathfrak{p}^e||\mathfrak{N}$, one can consider from now on the group $G = \mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}^e)$ and its subgroup $H = \widetilde{\Gamma_0(\mathfrak{p}^e)}$. And what is to be shown, is that the normalizer of the subgroup of upper-triangular matrices: $\widetilde{\Gamma_0(\mathfrak{p}^e)}$, in $\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}^e)$, is reduced to $\widetilde{\Gamma_0(\mathfrak{p}^e)}$ itself. Consider an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}^e)$ in the normalizer. Then for every $\begin{pmatrix} u & v \\ 0 & u^{-1} \end{pmatrix}$ in $\widetilde{\Gamma_0(\mathfrak{p}^e)}$, the conjugate:

$$\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} u & v \\ 0 & u^{-1} \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is upper-triangular.

But the bottom-left entry is proportional to $ac(-u+1/u) - vc^2$, which is thus equal to zero.

Choose first $u = v = 1$. Then $c^2 = 0$, so $c \in \mathfrak{p}$. Thus a is not in $\mathfrak{p}$, otherwise the determinant $ad - bc$ would not be invertible. Hence a is invertible.

Choose next $v = 0$. Then simplifying by a, it remains $c(-u + 1/u) = 0$. The following claim shows that there exists a u such that one can simplify by $-u + 1/u$, and thus conclude that $c = 0$.

Claim: there exists an invertible u such that $-u + 1/u \notin \mathfrak{p}$ (so is again invertible). Indeed fix p an element of $\mathfrak{p}$. Then the polynomial $X(-X+1)-p$ in the residue field $\mathbf{Z}_F/\mathfrak{p}$ has at most two roots and a nonzero derivative. So by Hensel liftings it has still at most two roots in $\mathbf{Z}_F/\mathfrak{p}^e$. So, provided that the cardinality $|\mathbf{Z}_F/\mathfrak{p}^e|$ is greater than $2|\mathfrak{p}/\mathfrak{p}^e|$, then such a u exists. But by the formulas of Lemma 5.3 (i), the difference between the two cardinalities is equal to $q^e - 2.q^{e-1}$, where $q = |\mathbf{Z}_F/\mathfrak{p}|$. By assumption $q > 2$, so this difference is strictly positive, which proves the claim. □

Remark 5.13. As a sanity check, one can verify this fact numerically for the cases that are of interest for this work. Namely for B the quaternion algebra of Examples 3.4, 3.6 and 3.7, let $\mathfrak{p}$ be one of the primes $\mathfrak{p}_2, \mathfrak{p}_7$ and $\mathfrak{p}_3$ of $\mathbf{Z}_F$, compute the monodromy group of the inclusions $\Gamma_0(\mathfrak{p}^2) \subset \Gamma(1)$ with the same algorithm as in Example 3.4. Then trust Magma for the fact that it has trivial centralizer in $S_{G/H}$.

Theorem 5.14. *Under the additional assumptions made in theorem 5.11:*

(i) *F is* Galois *over* $\mathbf{Q}$*;*
(ii') *F is of strict class number one (so $F(\infty) = F$);*
(ii) *the discriminant $\mathfrak{D}^f$ is* $\mathrm{Gal}(F/\mathbf{Q})$-invariant
(iii) *the level $\mathfrak{N}$ is* $\mathrm{Gal}(F/\mathbf{Q})$-invariant.
(iv) *the group $\Gamma(1) \widehat{=} \bar{\iota}(\mathcal{O}^+) \subset \mathrm{PSL}_2(\mathbf{R})$ is a* triangle group with elliptic points of distincts orders.

Then the canonical cover $f : X_0(\mathfrak{N}) \to X(1)$ descends *to* $\mathbf{Q}$.

This descent is furthermore characterised as being the unique *cover over* $\mathbf{Q}$ *(and actually over any algebraic extension of* $\mathbf{Q}$*) that has the monodromy representation of the topological cover $X_0(\mathfrak{N}) \to X(1)$.*

Proof From Proposition 5.12 and the fact that the field of moduli of the canonical cover f is equal to $\mathbf{Q}$ (by Theorem 5.11), the theorem 4.12 (ii) applied to $k' = F$ and $k = \mathbf{Q}$ implies that the canonical cover f descends to $\mathbf{Q}$.

Theorem 4.12 (i) applied with $k' = \overline{\mathbf{Q}}$ and $k = \mathbf{Q}$ then implies the unicity statement. □

An alternative proof for descent only

Proposition 5.15. *Let $\mathfrak{N}$ be an ideal of $\mathbf{Z}_F$. Fix a maximal order $\mathcal{O}$ and nested congruence groups of units of norm one: $G = \overline{\Gamma(1)}$, $H = \overline{\Gamma_0(\mathfrak{N})}$ and $\overline{\Gamma'(\mathfrak{N})} \triangleleft H$.*

Then the greatest normal subgroup of G contained in H

$$N = \bigcap_{g \in G} gHg^{-1}, \tag{5.3}$$

is equal to $\overline{\Gamma'(\mathfrak{N})}$.

Thus the Galois closure of the corresponding topological cover $X_0(\mathfrak{N}) \to X(1)$ is equal to $X'(\mathfrak{N}) \to X(1)$, with automorphism group equal to $\mathrm{PSL}_2(\mathfrak{N})$.

Proof One can again quotient everything by the normal subgroup $\overline{\Gamma'(\mathfrak{N})}$.

Again from the Chinese remainder (Sun Tsu) decomposition of Lemma III.5.3 (iv), it is also sufficient to suppose from now on that $G = \mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}^e)$ and $H = \Gamma_0(\mathfrak{p}^e)/\Gamma'(\mathfrak{p}^e)$ (for $\mathfrak{p}^e||\mathfrak{N}$). And thus to show that the largest normal subgroup N of G included in H is $\{1\}$.

Firstly, conjugating H by $g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ shows that

$$N \subset \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\}.$$

Finally let $n \in N$ be such a diagonal matrix. Then the equation (5.3) shows that it remains diagonal after any base change of the free module $\left(\mathbf{Z}_F/\mathfrak{p}^e\right)^2$ [This fact was pointed to us by B. Meyer]. So if (e_1, e_2) is the canonical basis, considering the base change by $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, there exists a scalar $\lambda \in \mathbf{Z}_F/\mathfrak{p}^e$ such that the basis vector $e_1 + e_2$ is taken to $\lambda(e_1 + e_2) = ae_1 + a^{-1}e_2$. Thus $a^{-1} = \lambda = a$.

For the last statement, the (hard) Proposition III.5.4 implies that the inclusion $\overline{\Gamma(1)}/\overline{\Gamma'(\mathfrak{N})} \subset \mathrm{PSL}_2(\mathfrak{N})$ is an equality. □

Let us derive an alternative proof of the *existence* statement of Theorem 5.14. By Proposition 5.15, the monodromy group of the cover $f : X_0(\mathfrak{N}) \to X(1)$ is equal to $\mathrm{PSL}_2(\mathfrak{N})$, which is center-free by construction. So by the (hard) [DèbDo, corollary 3.2] (see remarks 4.6), $\mathbf{Q}$ being the field of moduli of the canonical cover f, it descends to $\mathbf{Q}$.

Remark 5.16. One can check Proposition 5.15 numerically one some cases. Let B be the quaternion algebra of Examples 3.4, 3.6 and 3.7. Let $\mathfrak{p}$ be one of the primes $\mathfrak{p}_7$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$ of $\mathbf{Z}_F$, compute the monodromy group of the inclusions $\Gamma_0(\mathfrak{p}^2) \subset \Gamma(1)$ with the same algorithm as in Example 3.4. The cardinalities of these monodromy groups are equal to $2^3.3.7^4$, $2^9.3^2.7$ and $2^2.3^{12}.7.13$.

These cardinalities are expected be equal to $|\mathrm{PSL}_2(\mathbf{Z}_F/\mathfrak{p}^2)|$. Which is indeed the case, as verified from the formulas given by Lemma III.5.3.

5.5 Why the assumptions in Doi–Naganuma are necessary

Counterexample 5.17. The assumption (iii) in Corollary 5.10 is necessary. Indeed consider F the Galois totally real field of polynomial $t^3 - t^2 - 2t + 1$, ι a fixed real place of F, $\mathfrak{p}_7$ the ideal over 7, and $\mathfrak{p}_{13}$ one of the three ideals over 13. Consider the quaternion algebra B ramified exactly at: the finite places $\mathfrak{p}_7\mathfrak{p}_{13}$ and at that the two real places other than ι. Then the canonical model of the curve $X(1)$ is of genus one, and its Jacobian is one of the three elliptic curves e7d49D91i/ii/iii described in [Sij$_3$, Tables A.1/2/3][10] [11].

By the Theorem 5.6 they form an orbit under the Galois group of F. Notice also that the assumptions (i), (ii) (the narrow class number of the field F being one) and (iv) (the order is maximal) of the corollary are satisfied. But none of the j-invariants is rational, so the field of moduli is not $\mathbf{Q}$.

Counterexample 5.18. The assumption (iv) in Corollary 5.10 is necessary. Indeed the counterexamples $X_0(\mathfrak{p}_{11})$ and $X_0(\mathfrak{p}'_{11})$ e5d5D5i/ii in loc. cit. satisfy all the other assumptions. But since their levels are not Galois-stable ($\mathfrak{p}_{11}$ and $\mathfrak{p}'_{11}$), it is thus not surprising to see that their Jacobians have non-rational j-invariants.

Counterexample 5.19. The assumption (ii) in Corollary 5.10 is necessary. Indeed the genus one curve e2d1125D16: $X(1)$ in loc. cit. satisfies all the other assumptions (it arises from a maximal order and the algebra has a Galois-stable discriminant). But the conclusion of the corollary does not hold because the Jacobian of $X(1)$ has a nonrational j invariant.

5.6 Canonical models not defined over their field of moduli

Overview of the counterexamples

Three canonical models appear in the work [Sij$_3$], that have their field of moduli (as mere curves) equal to $\mathbf{Q}$ –because they satisfy the conditions of

[10] Notice that in the reference, it is instead the finite discriminant $\mathfrak{p}_7\mathfrak{p}_{13}$ that is *fixed*, and the infinite discriminant ι that *varies*. But the two constructions are actually the same. Indeed one passes from one to the other by conjugating the whole quaternion algebra (both finite and infinite places). Which leads to the same curve, as stressed in Remark 5.7.

[11] The curves e9d81D51i/ii/iii would also provide a similar counterexample.

Corollary 5.10–, but are not defined over $\mathbf{Q}$. These curves are all of genus one and arize from maximal orders ($X = X(1)$).

The left-hand column of table of Table 5.1 is a reference for the data for each of the three curves, as given in the tables of [Sij$_3$]. The second and last columns give the number field F and the finite discriminant $\mathfrak{D}$ of the quaternion algebra B (where, for example, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ stand for the two primes over the split prime 3). The two columns in the middle describe whether the primes 2 and 3 are inert in F

Table 5.1: Counterexamples

curve	F	2 inert	3 inert	$\mathfrak{D}^f$
e2d13D4	$\mathbf{Q}(\sqrt{13})$	yes	no	$\mathfrak{p}_2$
e2d13D36				$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$
e3d8D9	$\mathbf{Q}(\sqrt{2})$	no	yes	$\mathfrak{p}_3$

Proof for one counterexample

Let us show that the curve X with label e2d13D36 is not defined over $\mathbf{Q}$.

X is a curve of genus one defined over F, but doesn't necessarily have a rational point. However one can derive properties of its Jacobian J, which is an elliptic curve over F:

- Its conductor equals 6, by [Sij$_3$, Proposition 2.1.6].

- The valuation of its j-invariant at $\mathfrak{p}_2$ is equal to -10 (resp. -2 at $\mathfrak{p}_3$ and $\mathfrak{p}_3'$). Let us detail this result for the valuation at $\mathfrak{p}_2$. First, define the quaternion algebra H ramified exactly at both infinite places of F and at $\mathfrak{p}_3\mathfrak{p}_3'$. Call $\mathcal{O}_H$ the maximal order of H. As in [Sij$_3$, Proposition 3.1.9 (ii)] , consider $\mathcal{O}_H(\mathfrak{p}_2)$, a level $\mathfrak{p}_2$ suborder of $\mathcal{O}_H$. Consider the set of classes of right ideals of $\mathcal{O}_H(\mathfrak{p}_2)$, noted $\mathrm{Pic}_r(\mathcal{O}_H(\mathfrak{p}_2))$. To each ideal class $[\mathrm{I}(\mathfrak{p}_2)]$ in this set, associate the weight[12] $|\mathcal{O}_l(\mathrm{I}(\mathfrak{p}_2))^\bullet/\mathbf{Z}_F^\bullet|$. These weights can be computed by running the Magma ([Ma]) file PadInit in [Sij$_2$]. The sum of these weights is then equal to the opposite of the valuation of j at $\mathfrak{p}_2$, by [Sij$_3$, Proposition 3.1.14 (iii)].

[12]Equal to the cardinality of the projectivized group of units of the left-order of $\mathrm{I}(\mathfrak{p}_2)$.

Now if the curve X were defined over $\mathbf{Q}$, then the Jacobian J would descend to an *elliptic curve* $J_{\mathbf{Q}}$ over $\mathbf{Q}$, by the argument of [MilJV, Proposition 1.9]. So, let us suppose that such a rational model $J_{\mathbf{Q}}$ does exist, then

- the conductor of $J_{\mathbf{Q}}$ is either equal to 6, or to $6 \cdot 13^2$. This is proven by the following discussion, whose arguments were brought to us by Randriam:
  - at every place p but 13, the extension $F_{\mathfrak{P}}\mathbf{Q}_p$ does not ramify, so the conductor of $J_{\mathbf{Q}}$ has the same valuation than J, by Proposition 5.4 (a) of [Sil]. (As regards the particular cases of 2 and 3, note that J has multiplicative reduction at these places, so the valuation of the conductor of $J_{\mathbf{Q}}$ is necessarily equal to 1 at these places.)
  - at the place 13 where the extension $F_{\mathfrak{P}}/\mathbf{Q}_{13}$ ramifies, $J_{\mathbf{Q}}$ cannot have multiplicative reduction. For that if it were the case, then J would also have multiplicative reduction at 13 (by [Sil, Proposition 5.4 (b)]). This contradicts the result above on the conductor of J.
- the j-invariant of $J_{\mathbf{Q}}$ should be equal to the one of J. So, in particular, it should have the valuations at 2 and 3 predicted above.

Then, by a lookup in the tables of Cremona (proved to be exhaustive, see the introduction of [Cr]), only two elliptic curves E_1 and E_2 over $\mathbf{Q}$ fulfill the conditions above:

$$y^2 + xy + y = x^3 - 70997x + 7275296$$
$$y^2 + xy = x^3 - 11998412x + 15995824272$$

But considered over F, neither of their conductors is equal to 6 (one obtains isomorphic curves over F of conductor 6.13). So neither of them can be $J_{\mathbf{Q}}$, which therefore does not exist.

Alternative verifications (and nailing down the crucial point of the thesis)

In [Sij$_1$, Chapter 7], 5.6 it is shown that the canonical model of J over F is given by

(5.4)

$$J_F : y^2+(r+1)xy+(r+1)y = x^3+(16383r-38230)x+(1551027r-3576436)$$

where r is a root of $t^2 - t - 3$. Notice that the j-invariant is equal to $18013780041269221/9216$ so J_F is *rational*. Thus J_F has field of moduli $\mathbf{Q}$ (in particular is a $\mathbf{Q}$-curve). And actually $J_{\overline{\mathbf{Q}}}$ is *isomorphic over* $\overline{\mathbf{Q}}$ *to an elliptic curve over* $\mathbf{Q}$. But our point here is that the curve J_F over F itself, i.e. the canonical model, doesn't descend over $\mathbf{Q}$: this is one of the main subtleties that motivate this thesis.

Explicit methods to prove rigoroulsy equation (5.4) were also performed in [Sij$_1$].

Nevertheless, we would like to make a digression and recall the additional sanity checks for the validity of equation (5.4) that were performed in our joint work [BPRS, §3.8]:

- First, we checked that every quadratic twist of this model involving $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$, leads to a strict increase of the actual conductor 6, so cannot be a candidate for J.

- In addition, we compared the traces of Frobenius on J at several primes, to those predicted by the isomorphism of [Sij$_3$, (5.16)] (or stated in [DV, Th. 5.9]). This isomorphism asserts that the representation of the Hecke algebra on the (one-dimensional) space of differentials on E, is isomorphic to the representation of the Hecke algebra on the subspace of the Hilbert cusp forms on F that are *new* at $\mathfrak{D}$. The comparison was made possible, since the traces for this last representation are also computable in Magma (by the work of Dembélé and Donnelly [DemDo]).

Now: take equation (5.4) of the jacobian J for granted, and let us show (Nodesc): J does not descend to an *elliptic* curve over $\mathbf{Q}$. Hence, as remarked above, this will give one more proof that the curve e2d13D36 is not defined over $\mathbf{Q}$. For example, here are two ways to see (Nodesc):

- The trace of the Frobenius of J at the prime (11) of F, is equal to 22, which is not of the form $n^2 - 2 \cdot 11$.

- Alternatively, one can check that the Weil cocycle criterion is not satisfied for the curve J. Namely, letting σ be the conjugation of the quadratic field F, this boils down to verifying that, for any F-isomorphism $f_\sigma : J \to J^\sigma$ from J to the conjugate curve, then f_σ does not satisfy $f_\sigma \circ \sigma(f_\sigma) = \mathrm{id}$. The automorphism group of the elliptic curve J being of order two, this is quickly done.

Finally, there exists a last – and more straightforward – way to prove that e2d13D36 is a counterexample. It does not use the actual equation for the canonical model J, nor appeals to the various sophisticated theories used above (that predict the traces, conductor and j-invariant). This approach consists in computing the traces of the Hecke operators on J in the direct manner. Namely, [Sij$_1$, Algorithm 4.2.1] (available in [Sij$_2$], TakData) enables one to compute the action of the Hecke operators on the homology of the complex curve Y_0^1. Then, the computation of the trace at the inert prime (11) leads to the same result, and thus conclusion, as above.

Chapter VI

Explicit recursive families

The notations and assumptions of Chapter IV hold, and as in Chapter V the field F is supposed to be totally real.

1 Leitfaden

Let us trace back the logics of this chapter and its role in the proof of Theorem B. The statements about canonical covers are summed-up in Theorem C in §6.1 at the end of this addendum.

(a) the moduli interpretation of the involution of Atkin–Lehner (§2.3 paragraph "Atkin–Lehner");
implies that:

(b) the dotted map φ in diagram (3.2) in §3.2 is surjective;

One has:

(c) φ is injective;

Proof: follows from §2.1, which describes the Atkin-Lehner involution in our narrow class number one setting. Or, as suggested at the beginning of §3.2: shown in [Duc, Proposition IV.5.1].

Then (b) + (c) implies that φ is bijective. Which implies that:

(d) towers of Shimura curves are recursive;

Also, one has :

(e) the first steps of the towers considered in VI.5 descend over $\mathbf{F}_3$;

Proof: the unicity statement of Theorem V.5.14 shows that the candidates for the canonical covers found in §5.2 are the correct ones. This is stated neatly in the wrap-up Theorem C of §6.

Thus (d) + (e) implies:

(f) the whole towers descend over $\mathbf{F}_3$;

The possibility to intertwin modular towers of coprime levels (§3.1) + the density of the genera in the intertwinned family (§IV.2.5) finally implies that:

(g) Theorem B holds.

2 Sketch of the moduli interpretation

We would like to detail the moduli interpretation over the complex numbers, that underlies the recursive modular towers introduced in [El_1, 3rd variation].

The field F is assumed to be of narrow class number one (Definition III.1.1). The assumption that B is a division algebra is dispensable here (it is only necessary for the quotients $\Gamma_0(\mathfrak{N})\backslash\mathcal{H}$ to be compact).

2.1 The involution of Atkin-Lehner

Thanks to the classification of III.4.1 and to Proposition III.4.1, the following description from [Ogg, §2] also applies in the class number one setting.

Let $\mathfrak{l}$ be a prime of $\mathbf{Z}_F$, $i \geq 0$ an integer and $\mathcal{O}(\mathfrak{l}^i)$ an Eichler order of level $\mathfrak{l}^i$. The group of invertible two-sided fractional ideals that are maximal at the ramified places, can be described as follows: (i) the obvious ones $x\mathcal{O}(\mathfrak{l}^i)$ for $x \in \mathbf{Z}_F\backslash\{0\}$ (ii) a nonobvious one $J = J(\mathfrak{l}^i)$, that satisfies $J^2 = \mathfrak{l}^i\mathcal{O}(\mathfrak{l}^i)$. It is defined as follows by its completions at each finite place:

- at every $\mathfrak{p} \neq \mathfrak{l}$, $J_\mathfrak{p} = \mathcal{O}(\mathfrak{l}^i)_\mathfrak{p}$
- and (a) either $\mathfrak{l}|\mathfrak{D}$ then $J_\mathfrak{l}$ is the maximal ideal of $\mathcal{O}(\mathfrak{l}^i)_\mathfrak{l}$ (b) or else:

$$\omega_i \widehat{=} \begin{pmatrix} 0 & 1 \\ \pi_\mathfrak{l}^i & 0 \end{pmatrix}, \; J_\mathfrak{l} = \omega_i \,.\, \mathcal{O}(\mathfrak{l}^i)_\mathfrak{l} = \mathcal{O}(\mathfrak{l}^i)_\mathfrak{l} \,.\, \omega_i.$$

J is principal, generated by a *totally positive element*

$$w_i \in \mathcal{O}(\mathfrak{l}^i)$$

in the normalizer of $\Gamma_0(\mathfrak{l}^i)$. Thus the holomorphic transformation of the upper-half plane $\mathcal{H}$ defined by w_i, induces an involution of the Riemann surface $X_0(\mathfrak{l}^i)_{\mathbf{C}}$.

Furthermore two such generators w_i and w_i' differ by an element of $F^\bullet\mathcal{O}^1$. that is independant of the choice of w_i. By unicity of the canonical model condition, as in Theorem V.5.11, it induces an involution w_i of the canonical model $X_0(\mathfrak{l}^i)$: *the involution of Atkin–Lehner*.

2.2 Classical modular curves

Without level: the classical complex modular curve $X_0(1)$, without the cusps, parametrizes the isomorphism classes of complex elliptic curves E. Namely:

$$\tau \in \mathcal{H} \to E_\tau\mathbf{C}/\big(\mathbf{Z}\tau \oplus \mathbf{Z}\big)$$

With level: $X_0(N)$ (without the cusps) parametrizes the isomorphism classes of elliptic curves endowed with a cyclic subgroup of order N (see [DS, Theorem 1.5.1]). Equivalently, $X_0(N)$ parametrizes the isomorphism classes of isogenies $E \to E/H$ defined by a cyclic subgroup of order N.

Atkin-Lehner: For l prime and i a positive integer, the matrix $w_i = \begin{pmatrix} 0 & 1 \\ -l^i & 0 \end{pmatrix}$ defines an involution $w_i : z \to -1/l^i z$ of the upper-half plane $\mathcal{H}$, and normalizes the congruence group $\Gamma_0(l^i)$. Thus yields a well-defined involution w_i of $X_0(l^i)$.

In the previous moduli interpretation, this involution sends the isogeny $\big\{E = \mathbf{C}/\big(\tau\mathbf{Z} \oplus \mathbf{Z}\big) \longrightarrow E' = E/\big(H = \langle 1/l^i\rangle\big)\big\}$ to the *dual isogeny* $\big\{E' = \mathbf{C}/\big(\tau\mathbf{Z} \oplus 1/l^i\mathbf{Z}\big) \longrightarrow E'/\langle\tau/l^i\rangle \overset{[l^i]}{=} E\big\}$.

2.3 Rational quaternion algebras

Let B be a rational quaternion algebra with discriminant D, let us fix

$$\iota : B \hookrightarrow B \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathrm{M}_2(\mathbf{R})$$

a real splitting and $\mathcal{O}$ a maximal order. For each $\tau \in \mathcal{H}$, let Y_τ be the vector $\begin{pmatrix} \tau \\ 1 \end{pmatrix}$ of $\mathbf{C}^2$.

Without level

(See [Lan, IX], the notes of J. Stankewicz or [Voi$_5$, §42.6]). The space $(B \otimes \mathbf{R}).Y_\tau$ is the full $\mathbf{C}^2$, thus:

$$\eta_\tau : b \in B \longrightarrow b.Y_\tau \subset \mathbf{C}^2 \text{ is an embedding, and} \tag{2.1}$$

$$\Lambda_\tau = \mathcal{O}.Y_\tau \subset \mathbf{C}^2 \text{ is a lattice.} \tag{2.2}$$

Every complex torus of dimension two, with multiplication by $\iota(B)$ and uniformized by a lattice isomorphic to $\iota(\mathcal{O})$, arizes in this way –up to B-equivariant isomorphism ([Lan, Theorem 4.2]).

Fix in addition $T \in \mathcal{O}$, such that $T^2 + D = 0$. It defines a positive involution ρ on B:

$$x^\rho = T^{-1}\,\overline{x}\,T.$$

Then the skew-symmetric form:

$$E_\tau : \big(\iota(a).Y_\tau\,,\,\iota(b).Y_\tau\big) \longrightarrow \frac{1}{D}\,\mathrm{tr}(Tb^\rho a) = \mathrm{tr}(Ta\bar{b})$$

is (up to a sign) a Riemann form with respect to the lattice Λ_τ, of determinant one. Notice that the Rosati involution is induced by the involution ρ.

Two such principally polarized $(B, \iota, \mathcal{O}, T)$-lattices (or "QM-lattices") Λ_τ and $\Lambda_{\tau'}$ are (B-equivariantly) isomorphic if and only if $\tau' \in \iota(\mathcal{O}^1)\tau$ ([Lan, Theorem 5.1])

Thus the complex Shimura curve $X_0(1)$ parametrizes the isomorphism classes of $(B, \iota, \mathcal{O}, T)$-principally polarized abelian surfaces.

Example 2.1. Assume that the discriminant D is one. Thus B is the matrix algebra $\mathrm{M}_2(\mathbf{Q})$, with the (non-positive) involution $M \to \overline{M} = \mathrm{tr}(M)\mathrm{Id} - M$. Let $\mathcal{O}$ be $\mathrm{M}_2(\mathbf{Z})$. Thus $\Lambda_\tau = \begin{pmatrix} \mathbf{Z} \oplus \mathbf{Z}\tau \\ \mathbf{Z} \oplus \mathbf{Z}\tau \end{pmatrix}$ and A_τ is the square of an elliptic curve: $Ell_\tau \times Ell_\tau$.

If furthermore $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, the (positive) involution ρ is thus $M \to {}^{\mathrm{t}}M$ the transposition. Therefore the restriction of the Riemann form:

$$E_\tau : \big(M_1.Y_\tau\,,\,M_2.Y_\tau\big) \longrightarrow \mathrm{tr}(M_1.T.{}^{\mathrm{t}}M_2)$$

to each factor ($\mathbf{C}\times\{0\}$ and $\{0\}\times\mathbf{C}$) coincides with the canonical Riemann form on Ell_τ.

With level: case of the matrix algebra

Let us keep on the previous example with $B=\mathrm{M}_2(\mathbf{Q})$ and $\mathcal{O}=\mathrm{M}_2(\mathbf{Z})$. The N-torsion on $A_\tau=Ell_\tau\times Ell_\tau$ has a straightforward basis as a $\mathbf{Z}/N\mathbf{Z}$-module:

$$A_\tau[N]=\left\langle \begin{pmatrix}1/N\\0\end{pmatrix},\begin{pmatrix}0\\1/N\end{pmatrix},\begin{pmatrix}\tau/N\\0\end{pmatrix},\begin{pmatrix}0\\\tau/N\end{pmatrix}\right\rangle\equiv(\mathbf{Z}/N\mathbf{Z})^4.$$

Rigidify the previous isomorphism classes of squares of elliptic curves, with a subgroup Q of $A[N]\cong(\mathbf{Z}/N\mathbf{Z})^4$. Q is asked to be a sub-$\mathbf{Z}/N\mathbf{Z}$-module isomorphic to $\mathbf{Z}/N\mathbf{Z}\oplus\mathbf{Z}/N\mathbf{Z}$ and cyclically generated under multiplication by the quaternion order $\mathcal{O}=\mathrm{M}_2(\mathbf{Z})$. Thus Q is easily seen to be of the form:

$$Q=\begin{pmatrix}(\mathbf{Z}/N\mathbf{Z}).C/N\\(\mathbf{Z}/N\mathbf{Z}).C/N\end{pmatrix}+\Lambda_\tau=\mathrm{M}_2(\mathbf{Z}/N\mathbf{Z}).\begin{pmatrix}(\mathbf{Z}/N\mathbf{Z}).C/N\\0\end{pmatrix}+\Lambda_\tau,$$

with C a complex number of order N modulo $N\Lambda_\tau$. Thus of the form $c+d\tau$, $c,d\in\mathbf{Z}$ and $\gcd(c,d,N)=1$.

Let us now characterize standard representatives of rigidified squares of elliptic curves, mimicking [DS, Theorem 1.5.1]. Consider any square of elliptic curve $Ell_{\tau'}\times Ell_{\tau'}$ endowed with a subgroup Q of the N-torsion as above. From the condition $\gcd(c,d,N)=1$, there exists a matrix

$$\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathcal{O}^1=\mathrm{SL}_2(\mathbf{Z})$$

Define $\tau=\gamma.\tau'$ and $C=c\tau'+d$ as above. Then multiplication by C defines an isomorphism from the rigidified square of elliptic curves:

$$\left[Ell_\tau\times Ell_\tau,\begin{pmatrix}(\mathbf{Z}/N\mathbf{Z}).1/N\\(\mathbf{Z}/N\mathbf{Z}).1/N\end{pmatrix}+\Lambda_\tau\right]\tag{2.3}$$

to $[E_{\tau'}\times E_{\tau'},Q]$.

Let us finally study when two standard representatives for τ and τ' as in (2.3) are isomorphic. An isomorphism commuting with the quaternionic

multiplication is necessarily an homothety. Therefore there exists a complex number m and $\gamma \in \mathcal{O}^1 = \mathrm{SL}_2(\mathbf{Z})$ such that

$$m\begin{pmatrix} \tau \\ 1 \end{pmatrix} = \gamma.\begin{pmatrix} \tau' \\ 1 \end{pmatrix}. \tag{2.4}$$

And thus $\tau = \gamma.\tau'$ and $m = c\tau' + d$, where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. It is furthermore required that the torsion subgroups are sent to one another:

$$m.\left\{\begin{pmatrix} \mathbf{Z}/N\mathbf{Z}.1/N \\ \mathbf{Z}/N\mathbf{Z}.1/N \end{pmatrix} + \Lambda_\tau\right\} = \left\{\begin{pmatrix} \mathbf{Z}/N\mathbf{Z}.1/N \\ \mathbf{Z}/N\mathbf{Z}.1/N \end{pmatrix} + \Lambda_{\tau'}\right\}$$

Thus considering the first coordinate, $(c\tau'+d)/N$ must belong to $1/N\mathbf{Z}+\tau'\mathbf{Z}$, so $d \equiv 0 \mod N$ and γ belongs to the standard Eichler suborder

$$\mathcal{O}(N) = \begin{pmatrix} \mathbf{Z} & \mathbf{Z} \\ N\mathbf{Z} & \mathbf{Z} \end{pmatrix} \subset \mathcal{O} = \mathrm{M}_2(\mathbf{Z}).$$

In conclusion, $\Gamma_0(N)\backslash\mathcal{H}$ parametrizes isogenies between principally polarized products of elliptic curves, defined by a subgroup Q of the N-torsion, isomorphic to $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ and cyclically generated under multiplication by the maximal order $\mathcal{O} = \mathrm{M}_2(\mathbf{Z})$.

With level: general case

In the previous case, the order $\mathcal{O} = \mathrm{M}_2(\mathbf{Z})$ had a canonical explicit matrix action on the N-torsion points: the one induced from the complex action of $B = \mathrm{M}_2(\mathbf{Q})$ on $\mathbf{C}^2$.

Here one needs to make a choice. Consider the surjective morphism of $\mathcal{O}$-modules:

$$\eta_{\tau/N} : \lambda \in \mathcal{O} \longrightarrow \iota(\lambda).\begin{pmatrix} \tau/N \\ 1/N \end{pmatrix} \in \frac{1}{N}\Lambda\Big/\Lambda = A[N].$$

Choosing an isomorphism as in the proof of Proposition III.5.4:

$$\overline{\iota_N} : \mathcal{O}/N\mathcal{O} \cong \mathrm{M}_2(\mathbf{Z}/N\mathbf{Z})\,,$$

$\eta_{\tau/N}$ factorizes through a –non-canonical– isomorphism of $M_2(\mathbf{Z}/N\mathbf{Z})$-modules:

$$\overline{\eta_{\tau/N}} : M_2(\mathbf{Z}/N\mathbf{Z}) \xrightarrow{\sim} A[N].$$

Letting e_{ij} be the standard elementary matrices in $\mathrm{M}_2(\mathbf{Z}/N\mathbf{Z})$, define the N-torsion point:

$$C_\tau = \overline{\eta_{\tau/N}}(e_{12}) \in \overline{\eta_{\tau/N}}\Big(e_{11}.\mathrm{M}_2(\mathbf{Z}/N\mathbf{Z})\Big) \tag{2.5}$$

(the analogous of $\begin{pmatrix} 1/N \\ 0 \end{pmatrix}$). It generates likewise a QM-cyclic subgroup:

$$Q_\tau = \overline{\eta_{\tau/N}}\big(\mathrm{M}_2(\mathbf{Z}/N\mathbf{Z})\big).C_\tau + \Lambda_\tau.$$

of $A[N]$, isomorphic to $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$.

Let us study when two standard rigidified QM abelian surfaces:

$$[A_\tau, Q_\tau] \text{ and } [A_{\tau'}, Q_{\tau'}]$$

are isomorphic. Once again (i) an isomorphism is necessarily induced by multiplication by a complex number m (ii) and there exists $\gamma \in \mathcal{O}^1$, such that $\tau = \gamma.\tau'$ and the equation (2.4) holds.

Here the additional condition is that Q_τ is sent to $Q_{\tau'}$. The group $Q_{\tau'}$ being cyclic under $\mathcal{O}$, one has:

$$m.C_\tau \in \iota(\mathcal{O}).C_{\tau'},$$

So that, letting $e \in \mathcal{O}$ be any element that reduces modulo N to e_{12}, by equation (2.5) there exists $u \in \mathcal{O}$ such that:

$$m.\iota(e).\begin{pmatrix} \tau/N \\ 1/N \end{pmatrix} = \iota(u.e).\begin{pmatrix} \tau'/N \\ 1/N \end{pmatrix}.$$

Replacing the LHS with (2.4) yields:

$$\iota(e.\gamma)\begin{pmatrix} \tau'/N \\ 1/N \end{pmatrix} = \iota(u.e).\begin{pmatrix} \tau'/N \\ 1/N \end{pmatrix}.$$

Finally the vector $\begin{pmatrix} \tau/N \\ 1/N \end{pmatrix}$ having no torsion under $\mathcal{O}$, this implies the equality in $\mathcal{O}$:

$$e.\gamma = u.e$$

Reducing modulo N, identifying $\mathcal{O}/N\mathcal{O}$ with a matrix algebra by the isomorphism $\overline{\iota_N}$ and multiplying the matrices, this implies that γ is upper-triangular modulo N. Thus belongs to the standard Eichler suborder. The unit γ being furthermore of norm one, this results in:

Two standard rigidified QM-abelian surfaces for τ and τ' are isomorphic if and only if $\tau \in \Gamma_0(N)\tau'$.

Remark 2.2. The Morita equivalence for matrix algebras ([Lam, proof of Theorem 17.20] or [Brou, Proposition 1.25]) implies that every nonzero $M_2(\mathbf{Z}/N\mathbf{Z})$-submodule Q of $A[N]$ is isomorphic to $Q' = e_{11}Q \oplus e_{11}Q$. Where $M_2(\mathbf{Z}/N\mathbf{Z})$ acts on the left on Q' by matrix–column vector multiplication.

So in particular Q is fully determined, as a $M_2(\mathbf{Z}/N\mathbf{Z})$-module, by the $\mathbf{Z}/N\mathbf{Z}$ module generated by $C = e_{11}Q$. Which is, in our case, free of rank one.

However the isomorphisms of $M_2(\mathbf{Z}/N\mathbf{Z})$-modules allowed in our situation are only those arizing from complex homotheties.

This is why we did not use this argument as in [Cl$_1$], and stuck with non-canonical choices and explicit computations.

Atkin-Lehner

The case of the matrix algebra mimicks the case of classical modular curves. The involution of Atkin–Lehner:

$$w_N = \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$$

sends the standard rigidified QM lattice:

$$\widetilde{\Lambda_\tau} = \left[\mathrm{M}_2(\mathbf{Z}).\begin{pmatrix} \tau \\ 1 \end{pmatrix}, \begin{pmatrix} \mathbf{Z}/N\mathbf{Z}.1/N \\ \mathbf{Z}/N\mathbf{Z}.1/N \end{pmatrix} + \Lambda_\tau\right]$$

to the standard rigidified QM lattice:

$$\widetilde{\Lambda_{w_N\tau}} = \left[\mathrm{M}_2(\mathbf{Z}).\begin{pmatrix} w_N.\tau \\ 1 \end{pmatrix}, \begin{pmatrix} \mathbf{Z}/N\mathbf{Z}.1/N \\ \mathbf{Z}/N\mathbf{Z}.1/N \end{pmatrix} + \Lambda_{w_N.\tau}\right]$$

Where $w_N.\tau = -1/(N\tau)$. Thus the complex homothety of multiplication by τ sends $\widetilde{\Lambda_{w_N\tau}}$ to the –non standard– rigidified QM lattice:

$$\Big[\Lambda_{w_N.\tau}\mathrm{M}_2(\mathbf{Z})\begin{pmatrix} w_N.\tau \\ 1 \end{pmatrix}, \begin{pmatrix} \mathbf{Z}/N\mathbf{Z}.1/N \\ \mathbf{Z}/N\mathbf{Z}.1/N \end{pmatrix} + \Lambda_{w_N.\tau}\Big].$$

One recognizes the pair that parametrizes the dual isogeny of $\widetilde{\Lambda_\tau}$. *But beware that the QM-structure and the polarization have been twisted by* w_N.

In the general case, let us borrow the more intrinsic description of the QM-cyclic isogenies proposed in [Cl$_1$]. Assume for simplicity that the level N is a prime power p^e. The Eichler order $\mathcal{O}(p^e)$ is the intersection of the two maximal orders $\mathcal{O}$ and $\mathcal{O}'$, who differ exactly at their completions at p:

$$\mathcal{O}_p = \begin{pmatrix} \mathbf{Z}_p & \mathbf{Z}_p \\ \mathbf{Z}_p & \mathbf{Z}_p \end{pmatrix} \text{ and } \mathcal{O}'_{\mathfrak{p}} = \begin{pmatrix} \mathbf{Z}_p & p^{-e} \\ p^e & \mathbf{Z}_p \end{pmatrix}$$

This gives rize to two isogenies, of kernel isomorphic to $\mathcal{O}/\mathcal{O}(p^e) \cong \mathbf{Z}/p^e\mathbf{Z}$:

$$q_{1,\tau} : A_\tau = \mathbf{C}^2\Big/\iota(\mathcal{O}(p^e)).\begin{pmatrix} \tau \\ 1 \end{pmatrix} \longrightarrow A_{\tau,1}\mathbf{C}^2\Big/\iota(\mathcal{O}).\begin{pmatrix} \tau \\ 1 \end{pmatrix} \text{ and} \tag{2.6}$$

$$q_{2,\tau} : A_\tau = \mathbf{C}^2\Big/\iota(\mathcal{O}(p^e)).\begin{pmatrix} \tau \\ 1 \end{pmatrix} \longrightarrow A_{\tau,2}\mathbf{C}^2\Big/\iota(\mathcal{O}').\begin{pmatrix} \tau \\ 1 \end{pmatrix} \tag{2.7}$$

The maximal orders $\mathcal{O}$ and $\mathcal{O}'$ are conjugate by the Atkin-Lehner element: $\mathcal{O}' = w_e\mathcal{O}w_e^{-1}$. Let us see how the involution w_e of the upper half plane, sends q_1 to q_2. Let $M_e = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \iota(w_e)$ be the real matrix corresponding to w_e, and let m_e be the complex number $c\tau + d$. Then the following commutative diagram links $q_{1,w_e\tau}$ to q_2:

$$\begin{array}{ccc} \mathbf{C}^2\Big/\frac{1}{m_e}\iota(\mathcal{O}(p^e))M_e^{-1}.\begin{pmatrix} \tau \\ 1 \end{pmatrix} & \xrightarrow{q_{1,w_e\tau}} & \mathbf{C}^2\Big/\frac{1}{m_e}\iota(\mathcal{O})M_e^{-1}.\begin{pmatrix} \tau \\ 1 \end{pmatrix} \\ \Big\uparrow{\scriptstyle \frac{1}{m_e}M_e.} & & \Big\uparrow{\scriptstyle \frac{1}{m_e}M_e.} \\ \mathbf{C}^2\Big/\iota(\mathcal{O}(p^e)).\begin{pmatrix} \tau \\ 1 \end{pmatrix} & \xrightarrow{q_2} & \mathbf{C}^2\Big/\iota(\mathcal{O}').\begin{pmatrix} \tau \\ 1 \end{pmatrix} \end{array} \tag{2.8}$$

Once again, although the vertical arrows are isomorphisms, they twist the polarization and the QM-structure by w_e. The same diagram obviously applies to $q_{2,w_e\tau}$ and q_1.

Finally, the polarization being principal, it enables to define dual isogenies:

$$q_1^\vee : A_{\tau,1} \to A_\tau \text{ and} \tag{2.9}$$

$$q_2^\vee : A_{\tau,2} \to A_\tau. \tag{2.10}$$

In conclusion, the involution w_e sends the QM-cyclic isogeny:

$$q_2 \circ q_1^\vee : A_{\tau,1} \to A_{\tau,2}$$

to the dual isogeny:

$$q_1 \circ q_2^\vee : A_{\tau,2} \to A_{\tau,1}$$

(up to twisting the polarization and the QM-structure by w_e).

Wrap-up

See [El$_1$] for the analogous case of classical modular curves. Let p be a prime number and $i \geq 0$ an integer. The complex curve $X_0(p^{i+1})_{\mathbf{C}}$ parametrizes "cyclic p^i isogenies" between QM polarized abelian surfaces $A_1 \to A_2$. I.e. isogenies that arize from a subgroup Q of $A_1[p^e]$, which is isomorphic to $\mathbf{Z}/p^e \oplus \mathbf{Z}/p^e$ and generated by a point C under multiplication by the maximal order $\mathcal{O}$. This data is equivalent to the chain of cyclic p-isogenies:

$$A_1 \xrightarrow{./\mathcal{O}.p^{i-1}C} A_1\Big/\mathcal{O}.p^{i-1}C \xrightarrow{./\mathcal{O}.p^{i-2}C} \dots \xrightarrow{./\mathcal{O}.C} A_2 \tag{2.11}$$

The projection $f_{i+1} : X_0(p^{i+1}) \to X_0(p^i)$ sends such an isogeny to the one defined by the p^{i-1}-torsion point pC. That is to say, sends a chain (2.11) of cyclic p-isogenies to the chain truncated at the end :

$$A_1 \xrightarrow{./\mathcal{O}.p^{i-1}C} A_1\Big/\mathcal{O}.p^{i-1}C \xrightarrow{./\mathcal{O}.p^{i-2}C} \dots \xrightarrow{./\mathcal{O}.pC} A_1\Big/\mathcal{O}.pC$$

The involution of Atkin–Lehner w_i sends a cyclic $\mathfrak{p}^i$-isogeny $A_1 \to A_2$ to its dual $A_2 \to A_1$. Thus the composition $w_i \circ f_{i+1} \circ w_{i+1}$ sends a chain (2.11) to the chain truncated at the beginning:

$$A_1\Big/\mathcal{O}.p^{i-1}C \xrightarrow{./\mathcal{O}.p^{i-2}C} A_1\Big/\mathcal{O}.p^{i-2}C \xrightarrow{./\mathcal{O}.p^{i-3}C} \dots \xrightarrow{./\mathcal{O}.C} A_2$$

2.4 Over totally real fields

Without level

For general totally real fields $F \not\supseteq \mathbf{Q}$, the following classification makes it necessary to enlarge the quaternion algebra B by a CM field K.

Proposition 2.3 ([Sh$_0$, Prop. 1]). *Every division algebra over* $\mathbf{Q}$ *with a positive involution belongs to the following four types of algebras.*

(Type I) *Totally real algebraic number field F;*

(Type II) *Central simple algebra L over F such that $L_{\mathbf{R}} = L \otimes_{\mathbf{Q}} \mathbf{R} = \prod_{i=1}^{\deg F} \mathrm{M}_2(\mathbf{R})$;*

(Type III) *Central simple algebra L over F such that $L_{\mathbf{R}} = L \otimes_{\mathbf{Q}} \mathbf{R} = \prod_{i=1}^{\deg F} \mathbf{H}$;*

(Type IV) *Central simple algebra L over a totally imaginary quadratic extension K of F.*

So consider the larger quaternion algebra $L = B \otimes_F K$ ([Sh$_1$, §7.3]) and fix, as in the rational case ([Sh$_1$, 7.13]):

(i) positive involution ρ of L (as in [Sh$_0$, Prop. 2]);

(ii) a complex representation $\Phi = \Phi_1 \oplus \ldots \Phi_{[F:\mathbf{Q}]}$ of L equal to $[F : \mathbf{Q}]$ copies of $\mathrm{M}_2(\mathbf{C})$, such that ρ induces the transconjugation of matrices ([Sh$_0$, (6.1.1)]), and such that, in particular, the subfield F acts through its real place in Φ_1 and its complex places in $\Phi_{i>1}$ (see [Sh$_0$, (6.1.3)] and [Sh$_0$, (8)]);

(iii) an ideal $\mathfrak{M}$ of L with left-order a maximal order $\mathcal{O}$ ([Sh$_1$, 7.13]: for example choose $\mathfrak{M} = \mathcal{O}$ a maximal order).

Then consider the isomorphism classes of simple complex polarized abelian varieties A such that ([Sh$_0$, 1.4]):

(i) A is of complex dimension $n = 4[F : \mathbf{Q}]$ and the endomorphism field $\mathrm{End}_{\mathbf{Q}}(A)$ is *isomorphic to L via the complex representation* Φ ([Sh$_0$, 1.4] or [Sh$_1$, 4.1]);

(ii) thus if D is the complex lattice that uniformizes A: $A = \mathbf{C}^n/D$, then Φ induces an isomorphism of L-modules: $\eta : L \to \mathbf{Q}D$. *It is asked that* $\eta^{-1}(D) = \mathfrak{M}$ ([Sh$_0$, (9)-(10)] and [Sh$_1$, §4.1]). Thus the endormorphism ring $\mathrm{End}(A)$ is *equal* to the maximal order $\mathcal{O}$;

(iii) the involution ρ of L induces the Rosati involution.

By the discussion summed up in [Sh$_0$, Theorem 1], all isomorphism classes of such $(L, \Phi, \rho, T, \mathfrak{M})$-abelian varieties arize (with redundancy) from the following construction. Let T be an element of L such that: (i) $T^\rho = -T$ and (ii) $-i\Phi_1(T)$ is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $-i\Phi_{i>1}(T)$ to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ([Sh$_0$, (11),(12),(25)] or [Sh$_1$, (6.1.4)]).

Let $\mathcal{D}$ be the unit disc and for all $z \in \mathcal{D}$, let Y_z be the vector of $(\mathbf{C}^2)^{[F:\mathbf{Q}]} = (\mathbf{R}^4)^{[F:\mathbf{Q}]}$ with its first $\mathbf{R}^4$-component equal to $Y_{z,1} = (1, z, z, 1)$, and the others equal to $Y_{z,i>1} = (1, 1, 1, 1)$. Consider the lattice $\Lambda_z = \Phi(\mathfrak{M}).Y_z \subset \mathbf{C}^{2[F:\mathbf{Q}]}$. Then the skew-symmetric form:

$$E_z(\Phi(a).Y_z, \Phi(b).Y_z) = \mathrm{tr}(aTb^\rho)$$

is a Riemann form.

Two points z and z' in $\mathcal{D}$ give isomorphic polarized lattices if and only if they are in the same orbit of $\mathcal{D}$ under the action of a certain subgroup of units of L: $z' \in \Phi_1(\Gamma(T, \mathfrak{M})).z$ [Sh$_0$, Theorem 2].

With level

Rigidify the previous $(L, \Phi, \rho, T, \mathfrak{M})$ abelian varieties, by endowing them with a full level $\mathfrak{N}$ structure: that is to say, a basis v of the $\mathfrak{N}$-torsion ([Sh$_1$, 7.13]). E.g. the full level $\mathfrak{N} = (1)$ is an empty set. By the statement [Sh$_1$, (4.2.5)]), the unit disc $\mathcal{D}$ parametrizes (with redundance) all such rigidified polarized lattices.

Two points z and z' $\mathcal{D}$ give isomorphic rigidified $(L, \Phi, \rho, T, \mathfrak{M}, v)$-lattices if and only they are in the same orbit of a certain subgroup of units $\Gamma(T, \mathfrak{N}, \mathfrak{M})$ of L [Sh$_0$, Theorem 2].

The miracle is then that, under a suitable choice of CM field K ([Sh$_1$, Proposition (7.6)]), the congruence subgroup $\Gamma(\mathfrak{N}) \subset B \subset L$ in B coincides with the fixator $\Gamma(T, \mathfrak{N}, \mathfrak{M}) \subset L$ of a full level $\mathfrak{N}$ structure ([Sh$_1$, Propositions 4.11 & 6.3]).

Thus every intermediate congruence subgroup Γ: $\Gamma(1) \subset \Gamma \subset \Gamma(\mathfrak{N})$ also fixes intermediate level structures. E.g. $\Gamma_0(\mathfrak{N})$ parametrizes cyclic subgroups and thus cyclic isogenies.

In conclusion, switching to the upper-half plane by [Sh$_1$, (7.3.1)], the complex curve $X_0(\mathfrak{N})$ parametrizes exactly the isomorphism classes of: iso-

genies, between such $(L, \Phi, \rho, T, \mathfrak{M})$ abelian varieties, defined by a group of rank $2[F : \mathbf{Q}]$ which is $\mathcal{O}$-cyclically generated by an $\mathfrak{N}$-torsion element.

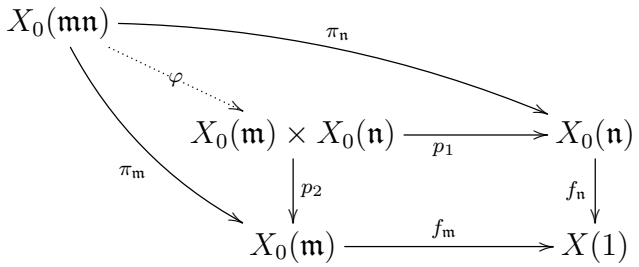
3 Recursive families

The goal of this section is to prove the recursivity of the modular towers introduced in [El_1, 3rd variation], the moduli interpretation underlying them, and to recall how two curves of coprime levels can be intertwinned. This last fact, although already considered in [El_1, 2nd variation] is the key point of this work and was pointed to us by Elkies.

3.1 Intertwinning coprime levels

Consider $\mathfrak{m}$ and $\mathfrak{n}$ two coprime ideals of F. The following diagram commutes:

(3.1)

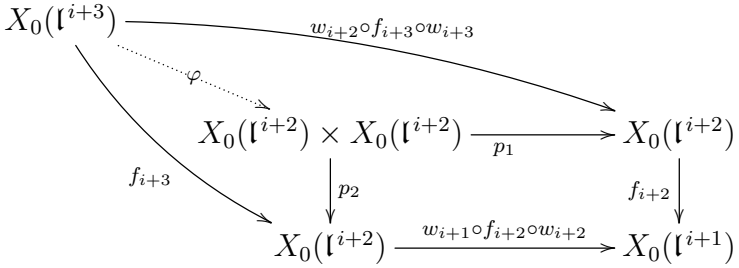


The ideals $\mathfrak{m}$ and $\mathfrak{n}$ being coprime, Corollary III.5.6 implies that the degrees of the projections from $\pi_\mathfrak{m}$ and $\pi_\mathfrak{n}$ are equal to $\Psi(\mathfrak{n})$ and $\Psi(\mathfrak{m})$, themselves equal to the degrees of the projections $X_0(\mathfrak{n}) \to X(1)$ and $X_0(\mathfrak{m}) \to X(1)$. So the induced map $\varphi : X_0(\mathfrak{mn}) \to X_0(\mathfrak{m}) \times X_0(\mathfrak{n})$ to the fibred product is of degree one onto *its image*. This image is a connected component of the fibred product.

The main point is that the complexified map $\varphi_\mathbf{C}$ is surjective. Thanks to the moduli interpretation in paragraph "Atkin–Lehner" of §2.3 above, then the proof is formally the same as in [El_1, top of page 2] (use the wrap up of). Thus the fibred product is geometrically (irreducible), thus φ is an isomorphism.

3.2 Equal levels

Let $i \geq 0$ be an integer and $\mathfrak{l}$ a prime ideal of F. Firstly, one easily checks that the outer-arrows of the following diagram commute (see also the proof of [Duc, Proposition IV.5.1]):

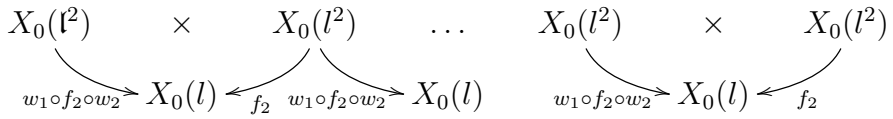
(3.2)


Indeed with the notations of §2.1, consider the ratio $r = w_{i+2}w_{i+3}/w_{i+1}w_{i+2}$. One the one hand r generates the integral two-sided ideal $\mathfrak{p}\mathcal{O}(\mathfrak{p}^{i+1})$. Thus by the narrow class number one assumption, r belongs to $F^+\mathcal{O}(\mathfrak{p}^{i+1})^\bullet$. On the other hand it is a quaternion of totally positive norm. In conclusion $r \in F^+\mathcal{O}(\mathfrak{p}^{i+1})^+$. Which is included in $F^\bullet\mathcal{O}(\mathfrak{p}^{i+1})^1$, by Proposition III.3.2. Thus r induces the identity on $X_0(\mathfrak{p}^{i+1})$.

The induced map φ is again of degree one onto its image for degree reasons.

It is also left as an exercice that the complexified map $\varphi_{\mathbf{C}}$ is surjective (see the wrap up of the moduli interpretation §2.3 above). Thus the fibered product is geometrically (irreducible), thus φ is an isomorphism.

By successive pullbacks of morphisms, a recurrence implies the closed formula for $X_0(\mathfrak{l}^i)$:

(3.3)


4 A new curve with many points –in need of a moduli interpretation

We thank J.–P. Flori for bringing our attention to [Has].

4.1 Predictions from the theory

Let F be the totally real field $F = \mathbf{Q}(\sqrt{3})$. Let $\mathfrak{p}_2$ and $\mathfrak{p}_3$ the primes of norm two and three over the ramified primes (2) and (3), and B the quaternion algebra ramified exactly at: $\mathfrak{p}_2$ and one infinite place. *The narrow class number* $h^+ = |\mathrm{Cl}_\infty(F)|$ *is two* –with corresponding abelian extension $F_\infty = \mathbf{Q}(\sqrt{3}, i)$. So we don't know if a modular tower can be built from Atkin–Lehner involutions –there exists possibly more than one involution at each step ! Nevertheless, our attempt to build recursive curves succeeds:

Consider a maximal order $\mathcal{O}$ in B and the Fuchsian group $\Gamma_0^+(\mathfrak{p}_3^4)$ in $\mathrm{PGL}_2^+(\mathbf{R})$ arising from the *units with totally positive norm* $\mathcal{O}(\mathfrak{p}_3^4)^+$ of the Eichler order[1] of level $\mathfrak{p}_3^4$ in $\mathcal{O}$. By Theorems V.5.1 and V.5.4, $X_0^+(\mathfrak{p}_3^4)$ is defined over the narrow class field F_∞ and has good reduction modulo the prime $\mathfrak{p}_5 = (5)$ over the residue field $\mathbf{F}_{5^2}$.

The number of $\mathbf{F}_{5^4}$-points of the reduction $\overline{X_0^+(\mathfrak{p}_3^4)}_{\mathbf{F}_{5^2}}$ is given by Theorem V.5.5. One can compute the matrix of the Hecke operator $T(\mathfrak{p}_5)$ using two independant algorithms available in Magma:

- the generalization of modular symbols [GV] (which further generalizes [Sij$_1$, Algorithm 4.2.1] for genus one curves);
- the action of Hecke operators on spaces of Hilbert modular forms [DemDo]. As mentionned earlier, the correspondence of Jacquet–Langlands states that the action of $T(\mathfrak{p}_5)$ on the space of holomorphic differentials on $X_0^+(\mathfrak{p}_3^4)$, is isomorphic to its action on the subspace of $\mathfrak{p}_2$-new Hilbert cusp forms on F of level $\mathfrak{p}_3^4$.

But beware, the output of both algorithms is the matrix of the full Hecke operator [Duc, equation (IV.10)] acting on the Jacobian of the full Shimura curve [Duc, equations (IV.1) and (IV.2)] defined over F. Which has $h^+ = 2$ connected components, of which $X_0^+(\mathfrak{p}_{3^4})$. The matrix being diagonalizable with rational values, we simply divide the trace by two, and obtain $\boxed{871 \text{ points over } \mathbf{F}_{5^4}}$.

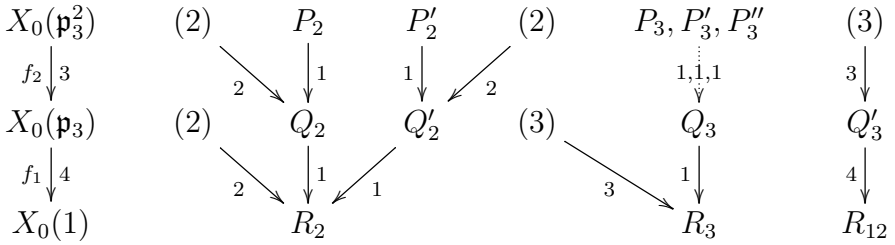
Magma tells us that the Fuchsian group $\Gamma_0^+(\mathfrak{p}_3^4)$ has $\boxed{\text{genus five}}$. So this number of $\mathbf{F}_{5^4}$-points is bigger than the previously best-known value for this genus, equal to 868.

[1] [Has] studies the subgroup $\Gamma_0(\mathfrak{p}_3^4)$ of units of *norm one*, of index two in $\Gamma_0^+(\mathfrak{p}_3^4)$ by Proposition III.3.2

4.2 Verification with explicit equations

Magma tells us that the Fuchsian groups $\Gamma(1)$, $\Gamma_0^+(\mathfrak{p}_3)$ and $\Gamma_0^+(\mathfrak{p}_3^2)$ have signatures $< 0; 2, 3, 12 >$, $< 0; 2, 2, 3, 3 >$ and $< 0; 2, 2, 3, 3, 3 >$. By Corollary III.5.6, the indices are $[\Gamma(1) : \Gamma_0^+(\mathfrak{p}_3)] = N(\mathfrak{p}_3) + 1 = 4$ and $[\Gamma_0^+(\mathfrak{p}_3) : \Gamma_0^+(\mathfrak{p}_3^2)] = N(\mathfrak{p}_3) = 3$.

One deduces from this a possible ramification behaviour for the morphisms $f_1 : X_0^+(\mathfrak{p}_3) \to X(1)$ and $f_2 : X_0^+(\mathfrak{p}_3^2) \to X(\mathfrak{p}_3)$ of degrees 4 and 3. Let R_i, Q_i and P_i be the elliptic points of orders i in the curves $X_0(1)$, $X_0^+(\mathfrak{p}_3)$ and $X_0(\mathfrak{p}_3^2)$, —possibly with a prime (e.g. P_3') when two points have the same order. Non-elliptic ramification points are just numbered with their ramification indices. e.g.: (3) is ramified of order 3 above R_3. The numbers beside the arrows are the ramification indices of the points (hence the redundant 3, etc.).



Remarks 4.1. Considering the covers f_1 and f_2 individually, there is only one possible ramification behaviour for them.

But for the composition $f_1 \circ f_2$, there are two possibilities: one could swap the ramification above the branch points Q_3 and Q_3' (one ramified point instead of three non-ramified, and conversely). However this would have lead to a different monodromy triple for $f_1 \circ f_2$. And, thanks to computations similar to Example V.3.4, we could discard this possibility

Fix the coordinates of R_2, R_3 and R_{12} at $\lambda = -27/625$, 0 and ∞. Set $\omega = \sqrt{-2}$. Then the function:

$$f_1(t) = (t-1)(t-1/5)^3$$

has the desired ramification behavior with Q_2, Q_2' of coordinates $\pm\omega/5$, and with Q_3, Q_3' of coordinates 1 and ∞.

Let us multiply from now on the coordinates on $X_0^+(\mathfrak{p}_3)$ by five, for the sake of reduction modulo (5): $Q_2 = \omega$, $Q_2' = -\omega$, $Q_3 = 5$ and $Q_3' = \infty$.

Exercice: a nonidentity involution of $\mathbf{P}^1$ (in characteristic not two) has trace zero. We look for an involution w_1 that both swaps Q_2, Q_2' and Q_3, Q_3'. The first condition implies that w_1 is of the form$(x+2c)/(cx-1)$ or $2/x$. Then the second implies:

$$w_1 = \frac{5x+2}{x-5}.$$

We find similarly:

$$f_2(z) = -3z - 2z^3$$

which has the desired ramification data with $P_2 = \omega$, $P_2' = -\omega$ and P_3, P_3', P_3'' the roots of $P(X) = (X+1)(X^2 - X + 5/2)$.

We finally look for an involution w_2 that swaps $\pm\omega$, so of the form $(x+2c)/(cx-1)$ or $2/x$, and which furthermore stabilizes the polynomial $P(X)$ up to scalar multiplication. A numerical solving for c provides

$$w_2 = \frac{x+4}{2x-1}.$$

Applying the closed formula (3.3), it follows that the function field of $X_0(\mathfrak{p}_3^4)$ is defined over $\mathbf{F}_3$ by:

$$3x^3y^3 + 2x^3y + 4x^3 + 4x^2 + 2xy^3 + 3xy + 3x + 2 = 0 \text{ and} \tag{4.1}$$

$$3y^3z^3 + 2y^3z + 4y^3 + 4y^2 + 2yz^3 + 3yz + 3y + 2 = 0 \tag{4.2}$$

From this equation, one can run general function field theoretic algorithms in Magma to confirm that this curve is indeed of genus five and has 871 $\mathbf{F}_{5^4}$-points.

4.3 A still unknown moduli interpretation

The complex curve $X_0(1)$ parametrizes classes of polarized abelian varieties with quaternionic multiplication by B as in 2.4. Whereas $X_0^+(1)$ parametrizes only *weak classes*: that is to say, such polarized abelian varieties *modulo* multiplication of the polarization by the action of a totally positive element of F ([Sh$_1$, 4.7, 4.10, 4.11]).

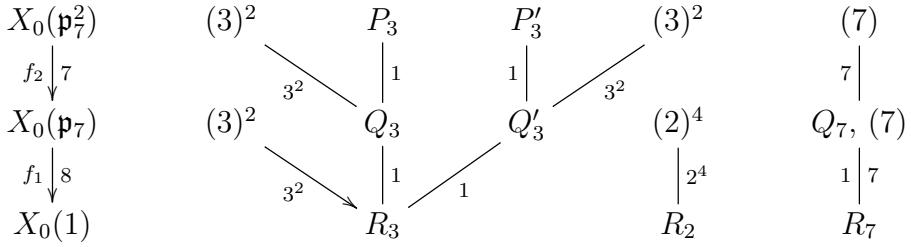
BUT –contrary to the situation $X_0(\mathfrak{p}_3^2) \to X_0(1)$– the curve $X_0^+(\mathfrak{p}_3^2)$ DOES NOT seem to parametrize the quaternionic $\mathfrak{p}_3^2$-isogenies between classes of abelian varieties parametrized by $X_0^+(1)$. Indeed suppose that it were the case, then $X_0^+(\mathfrak{p}_3^2)$ would parametrize three $\mathfrak{p}_3$-isogenies of type $R_3 \to R \to$

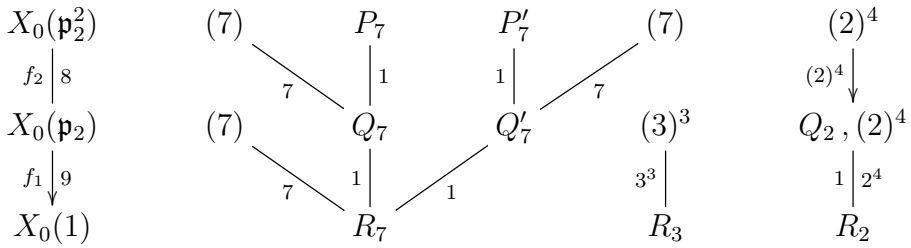
R_3 or R_{12} (R being any point, elliptic or not). But I see only two possible such isogenies when looking at $X_0^+(\mathfrak{p}_3)$, which are $R_3 \to R_{12} \to R_3$ and $R_3 \to R \to R_3$.

5 The intertwinned tower $X_0(\mathfrak{p}_2^i.\mathfrak{p}_7^j)$ over $\mathbf{F}_3$

5.1 The towers $X_0(\mathfrak{p}_7^i)$ and $X_0(\mathfrak{p}_2^i)$

Let us describe the ramification data determined at the end of chapter IV. P_i, Q_i and R_i stand for the elliptic points of orders i in the curves $X_0(1)$, $X_0(\mathfrak{p}_k)$ and $X_0(\mathfrak{p}_k^2)$, $k = 2, 7$ —possibly with a prime (e.g. P_7') when two have the same order. Non-elliptic ramification points are just numbered with their ramification indices. e.g.: $(2)^4$ stands for four ramification points of order two above Q_2. The numbers beside the arrows are the ramification indices of the points (hence the redundant 2^4, etc.). $X_0(\mathfrak{p}_7^i)$ starts from the left and $X_0(\mathfrak{p}_2^j)$ from the middle.





We saw that $X(1)$, $X_0(\mathfrak{p}_2)$ and $X_0(\mathfrak{p}_7)$ are of *genus zero*, whereas $X_0(\mathfrak{p}_7^2)$ and $X_0(\mathfrak{p}_2^2)$ are of *genus one*.

Recall from Example V.3.2 that covers of degree d of the projective line minus three points, are in bijection with conjugacy classes of triples of per-

mutations satisfying:

$$\Big\{\delta_a, \delta_b, \delta_c \in S_d,\ \delta_a \circ \delta_b \circ \delta_c = 1\Big\}$$

Recall the triples for the cover $f_2 : X_0(\mathfrak{p}_2^2) \to X_0(\mathfrak{p}_2)$ obtained in Example V.3.6. Depending on the conjugacy class of the subgroup $\Gamma_0(\mathfrak{p}_2^2)$ inside $\Gamma_0(\mathfrak{p}_2)$, one obtains two possible conjugacy classes of triples:

$$\sigma_2 = [(1,5,3,7,8,2,4),\ (1,8,3,2,4,5,6),\ (1,2)(3,4)(5,6)(7,8)]$$
$$\sigma_2' = [(1,3,5,2,6,7,8),\ (1,5,2,8,6,3,4),\ (1,2)(3,4)(5,6)(7,8)]$$

Remark 5.1. These two possible choices are equivalent for our purpose. Indeed, one of them determines the cover f_2, whereas the other one determines[2] $w_1 \circ f_2$. Anyway, computing the fibre-product (3.2) after substituting $w_1 \circ f_2$ to f_2 gives the same result (exercice).

Likewise for $X_0(\mathfrak{p}_7^2) \to X_0(\mathfrak{p}_7)$ one got in Example V.3.4:

$$\sigma_7 = [(1,6,4,2,7,5,3),\ (1,6,2)(4,5,7),\ (1,3,4)(2,7,6)]$$
$$\sigma_7' = [(1,7,4,5,3,6,2),\ (1,5,7)(3,6,4),\ (1,2,3)(4,5,6)]$$

Each of the four previous permutation triples generate groups in S_7, or S_8, which have a *trivial centralizer*. Thus by the (i) of Theorem V.4.12, if one fixes generators for e.g. the $\pi_1(\mathbf{P}^1_{\mathbf{C}} - \{Q_7, Q_7', Q_2\})$, and one fixes one of those triples, e.g. σ_2, then two covers over *a number field* that both have the triple σ_2, will be isomorphic *over the number field and not only* $\mathbf{C}$.

5.2 Computing the covers

The goal is now clear: for each pair of triples ($\sigma_{7/7'}$ and $\sigma_{2/2'}$), find one of the two uniquely possible covers $f_2 : E \to \mathbf{P}^1$ having this monodromy action. Then check for good reduction over $\mathbf{F}_3$.

j-invariants and rationality of quaternionic modular forms

Thanks to an algorithm for covers of the projective line arizing from subgroups of triangle groups, kindly shared by John Voight, we could determine

[2] Which is the subcover from the image subgroup of $\Gamma_0(\mathfrak{p}_2^2)$ by the Atkin-Lehner involution w_1. This image is non-conjugate in $\Gamma_0(\mathfrak{p}_2)$ (nor in $\Gamma_0(1)$: see Remark 5.4)

the j-invariants of the complex curves of genus one $X_0(\mathfrak{p}_7^2)_{\mathbf{C}}$ and $X_0(\mathfrak{p}_2^2)_{\mathbf{C}}$ whose monodromy over $\mathbf{P}^1$ equals the triples above. Namely:

$$j_7 = -3375 \text{ and } j_2 = 1792 \tag{5.1}$$

The method consists in, e.g. for $X_0(\mathfrak{p}_7^2)_{\mathbf{C}}$:

(i) embedding in $\mathrm{PSL}_2(\mathbf{R})$ the Fuchsian group $\overline{\Gamma_0(\mathfrak{p}_7)}$, seen as the $(7,3,3)$ triangle group Δ, as described in [KVMSV, Prop 2.5] (*not* the quaternionic embedding). And then in the group of direct transformations of the unit disc centered at the elliptic point Q_7 of order 7 of Δ (as in [KVMSV, p 11]) ;

(ii) determining a set of coset representatives for the subgroup $\Gamma = \overline{\Gamma_0(\mathfrak{p}_7^2)}$ defined by the triple σ_7 [KVMSV, Algorithm 3.5]. And thus a fundamental domain for Γ in the unit disc;

(iii) determining a basis $\{g(z)\}$ for the (one dimensional) space of weight two modular forms for this subgroup ([KVMSV, p30-33]);

(iv) by integration of this differential form on the fundamental domain , determining the periods lattice of the elliptic curve $X_0(\mathfrak{p}_7^2)_{\mathbf{C}}$ ([KVMSV, p44-45]);

(v) and possibly compute the Belyi map to $X_0(\mathfrak{p}_7)_{\mathbf{C}}$ ([KVMSV, p33-35], though we didn't use it).

Let us share a surprising pattern in the development of g. After computing a power series expansion with precision 140 in the unit disc centered at Q_7, and normalizing the variable $w \to w/\lambda$ (we chose λ equal to the ratio of the two consecutive non zero coefficients of g of degrees 7 and 8), we found:

$$\begin{aligned} g(w) = 1 &- 2/3.w + 2^3/3^3.w^3 + 2^7/(3^7.7)w^7 + 2^7/(3^7.7)w^8 + 2^9/(3^{10}.7^1)w^{10} \\ &- 2^{13}.5/(3^{13}.7^2.13)w^{14} - 2^{15}.5/(3^{15}.7^2.13).w^{15} + 2^{15}/(3^{16}.7^2.13)w^{17} \\ &- 2^{19}.31/(3^{16}.7^2.13)w^{21} + \dots \end{aligned}$$

This is surprising, firstly because although Q_7 is not an elliptic point for Γ, the development follows a periodic pattern : 1101000 1101000 . . . , where 0 means a zero coefficient and 1 a nonzero one. Finally because the coefficients could be clearly recognized as rational numbers, although the general theory only predicts them to be algebraic.

It also raizes the question of, when one has determined numerically a larger basis of $g > 1$ modular forms, does there exist numerical methods to find a linear transformation to apply to this basis in order to retrieve a rational one (after a further simultaneous normalization).

Theoretical predictions for the canonical models

Several hints help. First, the canonical models of the Shimura curves $X_0(\mathfrak{p}_7^2)_F$ and $X_0(\mathfrak{p}_2^2)_F$ –a priori defined over F– are actually *defined over* $\mathbf{Q}$ by Theorem V.5.14 applied to the corresponding covers $f_1 \circ f_2 : X_0(\mathfrak{p}^2)_F \to X(1)$.

In addition: [Sij$_1$, Th 3.1.6] gives information about the *conductors of the Jacobians over* $F = \mathbf{Q}(\cos(2\pi/7))$. The one of $X_0(\mathfrak{p}_7^2)_F$ is equal to a strict power of $\mathfrak{p}_7$. So by the same argument as on page 102, after descent over $\mathbf{Q}$, the conductor is of the form 7^i, $i \in [1, 2]$. Similarly the one of $X_0(\mathfrak{p}_2^2)_F$ is equal to a strict power of $\mathfrak{p}_2$. So after descent over $\mathbf{Q}$, is of the form $7^i.2^j$, $i \in \{0, 2\}$ and $j \in [1 \dots 8]$ (remind that the exponent of a prime $p > 3$ in the conductor of a rational elliptic curve can't be greater than two).

Finally: a lookup in [LMFDB] selects eight possible elliptic curves for the Jacobian of $X_0(\mathfrak{p}_2^2)_F$. Among which, only one has the traces of Frobenius equal to traces of Hecke operators of level $\mathfrak{p}_2^2$ at the primes $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_{11}$ and[3] $\mathfrak{p}_{17}$:

$$\mathrm{Jac}\big(X_0(\mathfrak{p}_2^2)_F\big) : y^2 = x^3 + x^2 - 114x - 127 \tag{5.2}$$

The case of $\mathrm{Jac}\big(X_0(\mathfrak{p}_7^2)_F\big)$ is similar but an ambiguity remains at this stage, so the determination will be described in what follows.

To start with, in order to compute f_2, one would like to know the field of the coordinates of the (CM-elliptic of order seven) branch points Q_7 and Q_7'. For example, by identifying them as the points that are unramified above R_7 by f_1. So let us compute this last map.

Determining the cover $f_1 : X_0(\mathfrak{p}_2) \to X(1)$

The triple of the genus zero Belyi map f_1 happens to have a trivial centralizer. So the equation of f_1 can be determined without ambiguity from its ramification data.

To start with, the branch points R_2, R_3 and R_7 are rational over F by Example V.5.3, so can be set at ∞, 42 and 0. The following representative for the isomorphism class of f_1 was then computed with the "ASD trick"

[3] The respective traces being -8, -18, 72, -126. Surprisingly, the traces of the other candidates differ only from their signs. I must miss an elementary fact about elliptic curves here.

described in [Bir]:

$$f_1 = \frac{(x+13/7)^7(x^2+7)}{\left(x^4-172/63x^3+2914/147x^2-130204/7203x+39913/441\right)^2} \tag{5.3}$$

In particular Q_7 and Q_7' are at $\pm\sqrt{-7}$.

Equation of the cover $f_{2,F(\sqrt{-7})} : X_0(\mathfrak{p}_2^2)_{\mathbf{Q}(\sqrt{-7})} \to X_0(\mathfrak{p}_2)_{\mathbf{Q}(\sqrt{-7})}$ over a quadratic extension (because of a pointless canonical model)

To start with, both the canonical covers f_1 and $f_1 \circ f_2$ descend to $\mathbf{Q}$ by Theorem 5.14. So the pointed cover $(f_2, (P_7, P_7'))$ descends to $\mathbf{Q}$ (here (P_7, P_7') is seen as a point of degree two). But, as we will see in Remark 5.2, the canonical model $X_0(\mathfrak{p}_2^2)_F$ has no rational point. So it is hopeless to find equations for f_2 over $\mathbf{Q}$ from the rational Weierstrass model (5.2).

We still want to use this Weierstrass model, thus we are going to compute $f_{2,F(\sqrt{-7})}$ over the quadratic extension $\mathbf{Q}(\sqrt{-7}$. So let us chose the smallest finite field of good reduction containing $z=\sqrt{-7}$: namely $\mathbf{F}_{29}$, to compute the cover $f_{2,\mathbf{F}_{29}}$ modulo 29. In particular, the trick detailed in [SV$_1$, page 39] saved days of computations[4].

Next: a (two-variables) Hensel-lifting, followed by lattice methods to recognize rational coefficients (we thank B. Meyer for discussions about this), lead to two possible isomorphism classes of covers defined over $\mathbf{Q}(\sqrt{-7}) \subset F(\sqrt{-7}))$ and ramified over $\{Q_7=\infty,\ Q_7'=1,\ Q_2=0\}$. They are given by the following f_2 and its complex conjugate $\overline{f_2}$, where $z=\sqrt{-7}$:

$$\begin{aligned} f_{2,F(\sqrt{-7})} = \frac{1}{x-1/32(91z+169)}\Big[&1/12544(-z+11)x^4 \\ &+1/12544(-27z-151)x^3+1/3136(71z-109)x^2+1/3136(491z+4231)x \\ &+1/3136(-8411z-14971)+y\Big(1/614656(-13z-49)x^3+1/153664(205z+49)x^2 \\ &+1/76832(-317z+1519)x+1/153664(-2613z+5831)\Big)\Big]. \end{aligned} \tag{5.4}$$

[4]Precompute all the possibilities for the polynomials expressing the resultant between $f_{2,\mathbf{F}_{29}}$ and its derivative.

And the (CM-elliptic of order seven) unramified points above Q_7 and Q'_7 are in affine coordinates:

$$P_7 = [1/32(91z + 169)\,,\, 1/128(-1911z + 931)] \text{ and:} \tag{5.5}$$

$$P'_7 = [-14z + 16\,,\, -98z - 49] \tag{5.6}$$

The "ASD-trick" described in [SV$_1$, Lemma 2.7] provides a sanity check that the equation for $f_{2,F(\sqrt{-7})}$ given here has the correct ramification data. Let $(7) = [2, -7z]$ be the ramified point of degree seven above $Q'_7 = 1$. Then the sum of points $2.P_7 + Q_7 - 5.(7)$ on the elliptic curve $X_0(\mathfrak{p}_2^2)_{F(\sqrt{-7})}$ is expected to be the neutral element, which is indeed the case.

Remark 5.2. We can check that $(f_2, (P_7, P'_7))$ indeeds descends to $\mathbf{Q}$: the map ϕ, equals to the addition of the point $Q = (2 : 7z : 1)$, maps the pointed cover to its conjugate and satisfies the Weil cocycle condition $\phi.\overline{\phi} = 1$.

However there doesn't exist any $F(\sqrt{-7})$-endomorphism of the elliptic curve $X_0(\mathfrak{p}_2^2)_{F(\sqrt{-7})}$ that maps the pair (P_7, P'_7) to a pair of conjugate points.

So the pointed map *doesn't* descent to a pointed map from the elliptic curve $\mathrm{Jac}\big(X_0(\mathfrak{p}_2^2)_F\big)$ to $\mathbf{P}^1_F$. So the canonical model *is not* an elliptic curve.

Reduction and descent over $\mathbf{F}_3$

Reducing the cover modulo[5] $\mathbf{F}_{3^2} = \mathbf{F}_3\langle z^2 = -1\rangle$, the descent begins. First, apply a translation to the elliptic curve $X_0(\mathfrak{p}_7^2)_{\mathbf{F}_{3^2}}$, in order to move the elliptic points P_7 and P'_7 into conjugate points. Then, as suggested in [SV$_2$, A.1], apply a homography to $\mathbf{P}^1_{\mathbf{F}_{3^2}}$ so that (i) the branch points $0, 1$ below P_7 and P'_7 are mapped to the conjugate points z and $-z$ (ii) and ∞ is unchanged (indeed, we notice a $\mathbf{F}_3$-rational point over ∞, so we want to preserve this).

This provides a model over $\mathbf{F}_3$. But being computed by composition by an elliptic-curve translation morphism, the size of the fraction defining the cover explodes. So we recompute a simpler equation over $\mathbf{F}_3$ for the whole cover again, taking advantage of the knowledge of conjugate coordinates for P_7 and P'_7 (and also of the rational point above ∞) determined just above.

[5] Which could also be directly computed in this finite field. But Hensel lifting was problematic from here.

This results in:

$$f_2(x,y) = \frac{1+x^2+x^3+x^4+(x+2x^2)y}{2+x^2+x^3+x^4+x^2y} \tag{5.7}$$

$$X_0(\mathfrak{p}_2^2)_{\mathbf{F}_3} : y^2 = x^3+x^2+2 \tag{5.8}$$

$$w_2 : X_0(\mathfrak{p}_2^2)_{\mathbf{F}_3} \ni P \longrightarrow (1:2:1) - P \tag{5.9}$$

$$w_1 : t \in \mathbf{P}^1_{\mathbf{F}_3} \ni t \longrightarrow -t \tag{5.10}$$

Where w_2 is the involution on $X_0(\mathfrak{p}_2^2)_{\mathbf{F}_3}$ that swaps the elliptic points P_7 and P_7'.

Computation of the cover $f_2 : X_0(\mathfrak{p}_7^2) \to X_0(\mathfrak{p}_7)$

The same hints leave us this time with two candidates for $\mathrm{Jac}\big(X_0(\mathfrak{p}_7^2)_F\big)$: the rational curves 49.a2 and 49.a4 of the LMFDB (which are both isogenous and twists). But attempts to compute the cover with one and the other candidate, singles out 49.a4 as the right one. It has the following model over the rationals:

$$X_0(\mathfrak{p}_7^2)_F : y^2+xy = x^3-x^2-2x-1 \tag{5.11}$$

We could furthermore perform pointed descent of the cover f_2 over $\mathbf{Q}$, thanks to the method of [SV$_2$, A.2] using the ramified point $(7) = \{\infty\}$ of order seven above the rational point $Q_7 = \{\infty\}$. This descended global cover f_2 has also good reduction modulo 2 as a bonus. Here are the equations:

$$f_2(x,y) = 2x+5x^2-3x^3+(-3+3x+x^2)y \text{ branched over} \tag{5.12}$$

$$Q_3, Q_3' = \pm\sqrt{-3}; \tag{5.13}$$

$$w_2 : X_0(\mathfrak{p}_7^2)_{\mathbf{Q}} \ni P \longrightarrow (2,-1,1) - P \tag{5.14}$$

$$w_1 : t \in \mathbf{P}^1_{\mathbf{Q}} \ni t \longrightarrow -1-t \tag{5.15}$$

Remark 5.3. Notice that we removed the Jac in equation (5.11). Indeed we obtain here an equation of the cover f_2 defined over the field F of definition of the curve $X_0(\mathfrak{p}_7^2)_F$ (over the rationals, actually). Thus the ramified point $(7) = \{\infty\}$ of order seven above the rational point $Q_7 = \{\infty\}$ is *rational*. So the canonical model $X_0(\mathfrak{p}_7^2)_F$ is an *elliptic curve*.

Additional monodromy computations for $X_0(\mathfrak{p}_7^i)$

The cover $f_{2,\mathbf{Q}} : X_0(\mathfrak{p}_7^2) \to X_0(\mathfrak{p}_7)$ given in (5.12) being defined over $\mathbf{Q}$, it is possible to use Maple's algorithm to compute the monodromy. We check that it is indeed given by one of the triples $\sigma_{7/7'}$ (depending on the base laces chosen).

But recall that the cover f_2 has no automorphisms, as one checks directly by verifying that the triples σ_7 and σ_7' have trivial centralizers. Thus by Theorem V.4.12 (ii), the $f_{2,\mathbf{Q}}$ given in (5.12) coincides with the *unique* descent of the canonical cover $f_{2,F}$ over $\mathbf{Q}$ (up to $\mathbf{Q}$-isomorphism).

The next remark explains the ambiguity about the choice of base laces (and thus of triple $\sigma_{7/7'}$). The two choices are deduced from one other by the involution of Atkin–Lehner. Thus, as our goal is to compute the fiber product of the cover with its twist by Atkin–Lehner, the choice is harmless.

Remark 5.4. Firstly, we computed the monodromy of the map (5.12) twisted by Atkin–Lehner (basically: compose it with a switch of the conjugate branch points Q_3 and Q_3'). We obtained the two triples σ_7 and σ_7', that correspond to the monodromies of the canonical cover and of its Atkin–Lehner twist.

Remark 5.5. This remark is not mandatory. Fix a representative of the isomorphism class of the cover f_1. Then one could further ask which one as the two candidates f_2 and f_2', gives the correct composed cover $f_1 \circ f_2 : X_0(\mathfrak{p}_7^2) \to X_0(1)$.

Firstly, the triple of the genus zero Belyi map f_1 happens to have a trivial centralizer. So it can be determined straight from its ramification data, with the help of [Bir]. We get e.g.:

$$f_1 = \frac{1}{2^6.3^2} \frac{(x^2 + 232/3x + 3403/36)^3 (x^2 + 3/4)}{(x - 13/6)^7}$$

Then, a computation of the monodromy of the compound cover $f_1 \circ f_2$ (of degree 56 !), shows that, with this choice of f_1, then the f_2 given in (5.12) provides the correct canonical composed cover $f_1 \circ f_2$.

On the contrary, we could unfortunately not perform monodromy computations with the cover $f_{2,F(\sqrt{-7})} : X_0(\mathfrak{p}_2^2) \to X_0(\mathfrak{p}_2)$, because our equations are only defined over $\mathbf{Q}(\sqrt{-7})$. So this leaves open the possibility that the equation in characteristic zero for the covers $f_{2,F(\sqrt{-7})}$ and $\overline{f_{2,F(\sqrt{-7})}}$ that we

obtained in equation (5.4), might actually describe covers with *wrong ramification triples*. Indeed, J. Sijsling's algorithm BelyiInit in [Sij$_2$] provides *another pair* of conjugacy classes of triples that have the *same ramification data* (i.e. cycle lengths) as the pair σ_2 and σ_2':

$$\sigma_{2,wrong} = [(1,2)(3,4)(5,6)(7,8),(1,3,4,5,7,6,8),(1,7,6,8,5,3,2)] \tag{5.16}$$

$$\sigma'_{2,wrong} = [(1,2)(3,4)(5,6)(7,8),(1,5,6,8,3,2,4),(1,3,7,8,5,2,4)] \tag{5.17}$$

Their monodromy group is of cardinality 1344 (instead of 56). There exists a fifth triple with this ramification data but it is discarded (since it cannot account for the pair of nonisomorphic covers $f_{2,F(\sqrt{-7})}$ and $\overline{f_{2,F(\sqrt{-7})}}$ that we obtained).

Thus, this ambiguity motivates the tedious proof done in section 6 (based on exhaustive Hensel liftings). We hope to resort soon to numerical methods to check the monodromy representation anyway. Beforehand, we describe sanity checks.

5.3 Computing the next steps of the towers

As an additional check for both towers, we computed the fibred products defining $X_0(\mathfrak{p}_7^3)_{\mathbf{F}_3}$ and $X_0(\mathfrak{p}_2^3)_{\mathbf{F}_3}$ as in (3.2). More precisely, we could determine their function fields as follows:

Let $\mathbf{A}_4$ be the affine plane with variables x, Y, z, T. Call $E_{x,Y}(\mathfrak{p})$ and $E_{z,T}(\mathfrak{p})$ the polynomials defining the plane models of the elliptic curves $X_0(\mathfrak{p}^2)$ determined above ($\mathfrak{p}$ equals $\mathfrak{p}_2$ or $\mathfrak{p}_7$). Using addition and inversion formulas on an elliptic curve, one determines a rational formula for the involution $w_2(z,T)$, which is correct except at one point.

The locus of the fiber products $X_0(\mathfrak{p}^3)$ in the square of the plane model $X_0(\mathfrak{p}^2) \times X_0(\mathfrak{p}^2)$, is defined by the vanishing of the numerator $N_\mathfrak{p}$ of $w_1 \circ f_2(x,Y) - f_2 \circ w_2(z,T)$. We get (up to points where it is badly defined):

$$\begin{aligned} N_{\mathfrak{p}_7} = {} & 2x^2Yz^4 + 2x^2Yz^3 + 2x^2Yz + 2x^2Y + x^2z^4 + x^2z^3 + x^2z + x^2 + \\ & + xz^4 + xz^3 + xz + x + 2z^2T + z^2 + z + 2 \end{aligned}$$

and

$$\begin{aligned}N_{\mathfrak{p}_2} &= x^4z^8 + 2x^4z^7 + 2x^4z^6T + x^4z^6 + 2x^4z^5T + 2x^4z^5 + 2x^4z^4T + x^4z^4\\ &+ 2x^4z^3T + 2x^4z^3 + 2x^4z^2T + x^4z^2 + x^4zT + x^4z + 2x^4T + 2x^4\\ &+ x^3z^8 + 2x^3z^7 + 2x^3z^6T + x^3z^6 + 2x^3z^5T + 2x^3z^5 + 2x^3z^4T\\ &+ x^3z^4 + 2x^3z^3T + 2x^3z^3 + 2x^3z^2T + x^3z^2 + x^3zT + x^3z + 2x^3T\\ &+ 2x^3 + 2x^2Yz^7 + 2x^2Yz^6T + 2x^2Yz^6 + 2x^2Yz^5T + x^2Yz^5\\ &+ 2x^2Yz^4T + 2x^2Yz^4 + 2x^2Yz^3T + x^2Yz^3 + 2x^2Yz^2T\\ &+ 2x^2Yz^2 + x^2YzT + 2x^2Yz + 2x^2YT + x^2Y + x^2z^8 + 2x^2z^7\\ &+ 2x^2z^6T + x^2z^6 + 2x^2z^5T + 2x^2z^5 + 2x^2z^4T + x^2z^4 + 2x^2z^3T\\ &+ 2x^2z^3 + 2x^2z^2T + x^2z^2 + x^2zT + x^2z + 2x^2T + 2x^2\\ &+ 2xYz^8 + xYz^6 + 2xYz^5 + xYz^4 + 2xYz^3 + xYz^2 + xYz\\ &+ 2xY + z^7 + z^6T + z^6 + z^5T + 2z^5 + z^4T + z^4 + z^3T\\ &+ 2z^3 + z^2T + z^2 + 2zT + z + T + 2\end{aligned}$$

Summing up, one considers the scheme:

$$\mathcal{E} = \{(x, Y, z, T) \in \mathbf{A}_4\,,\ E_{x,Y}(\mathfrak{p}) = E_{z,T}(\mathfrak{p}) = N(x, Y, z, T) = 0\},$$

Which has one irreducible component X of genus five (respectively seven). These are happily the genera predicted by Corollary IV.2.12 for the curves $X_0(\mathfrak{p}_7^3)$ and $X_0(\mathfrak{p}_2^3)$.

Remark 5.6. In addition, $\mathcal{E}$ has one (respectively two) other irreducible components of degree one. They probably occur as $X_0(\mathfrak{p}^2) \times \{0\}$, because of the points where $f_2 \circ w_2(z, T)$ are badly defined.

Our two-variable equations for the function fields of the component X –which is expected to be the one of $X_0(\mathfrak{p}_7^3)$ (respectively $X_0(\mathfrak{p}_2^3)$)– are one page-long. This is mainly due to our computations of $f_2 \circ w_2$ as compositions with the translation by a point on an elliptic curve: this raises the size of the fraction expressing f_2.

Computing it directly as a cover solves this problem (and also suppress the parasitic components): this is done in the final section 6.3.

Next, one enlarges the constant field of X to $\mathbf{F}_{3^3}$ and computes the places of degree one and two of $X_{\mathbf{F}_{3^3}}$. This enables to recover the number of points over $\mathbf{F}_{3^3}$ and $\mathbf{F}_{3^6}$ of the smooth model of $X_{\mathbf{F}_{3^3}}$. Which gives: 28 and 1000 points for $X_0(\mathfrak{p}_7^3)$, and 24 and 1760 points for $X_0(\mathfrak{p}_2^3)$. These numbers happily coincide with those predicted by Theorem V.5.5 (the traces being evaluated with Hilbert modular forms).

6 Wrap-up of VI.5.2 and complements on canonical covers

6.1 Wrap-up statement of VI.5.2

Let us first recall the definition of the towers considered in VI.5. Let $F = \mathbf{Q}(\cos(2\pi/7))$ be the totally real number field of degree three and narrow class number one. Fix once and for all a real embedding $\iota : F \hookrightarrow \mathbf{R}$. Let B be the quaternion algebra over F which is ramified exactly at: the two other infinite places than ι, and no finite place.

One remark about the choice of ι: actually all the levels $\mathfrak{N}$ considered in the thesis for this algebra B are Galois-invariant. Also, the finite discriminant of B is Galois invariant because it is trivial. Thus Remark 5.7 above, about conjugate quaternion algebras, implies that one would get the same Shimura curves if having fixed another infinite split place $\iota \circ \sigma$ for B.

B acts on the upper-half plane through through the split real place $\iota : B \hookrightarrow \mathrm{M}_2(\mathbf{R})$. Consider the prime ideals $\mathfrak{p}_2$ and $\mathfrak{p}_7$ of F above the inert prime (2) and the ramified (7). Define the corresponding nested families of congruence subgroups of $\mathrm{PSL}_2(\mathbf{R})$: $\overline{\Gamma_0(\mathfrak{p}_2^i)}$ and $\overline{\Gamma_0(\mathfrak{p}_2^j)}$ (see III.5.1). Forming the quotients of the upper-half plane, inclusions of nested subgroups give rize to the two towers of canonical covers (see Theorem V.5.1) over F:

$$\ldots \xrightarrow{f_4} X_0(\mathfrak{p}_7^3) \xrightarrow{f_3} X_0(\mathfrak{p}_7^2) \xrightarrow{f_2} X_0(\mathfrak{p}_7) \xrightarrow{f_1} X_0(1)$$
$$\ldots \xrightarrow{f_4} X_0(\mathfrak{p}_2^3) \xrightarrow{f_3} X_0(\mathfrak{p}_2^2) \xrightarrow{f_2} X_0(\mathfrak{p}_2) \xrightarrow{f_1} X_0(1)$$

Theorem C. *(i) The* canonical cover $f_{2,F} : X_0(\mathfrak{p}_7^2)_F \longrightarrow X_0(\mathfrak{p}_7)_F$ *descends over* $\mathbf{Q}$*. Its equation, and that of the Atkin–Lehner involutions, are given by Equations VI.*(5.11) *and VI.*(5.12)–(5.15)*:*

$$X_0(\mathfrak{p}_7^2)_F : y^2 + xy = x^3 - x^2 - 2x - 1 \tag{6.1}$$
$$f_{2,\mathbf{Q}}(x,y) = 2x + 5x^2 - 3x^3 + (-3 + 3x + x^2)y\ ,\ \textit{branched over} \tag{6.2}$$
$$Q_3, Q_3' = \pm\sqrt{-3}; \tag{6.3}$$
$$w_2 : X_0(\mathfrak{p}_7^2)_{\mathbf{Q}} \ni P \longrightarrow (2,-1,1) - P \tag{6.4}$$
$$w_1 : t \in \mathbf{P}^1_{\mathbf{Q}} \ni t \longrightarrow -1 - t \tag{6.5}$$

(ii) The quadratic base field extension to $F(\sqrt{-7})$ of the canonical model $X_0(\mathfrak{p}_2^2)_F$ *is given by VI.*(5.2)*:*

$$X_0(\mathfrak{p}_2^2)_{F(\sqrt{-7})} : y^2 = x^3 + x^2 - 114x - 127\,.$$

(ii')The quadratic base field extension to $F(\sqrt{-7})$ of the canonical cover $X_0(\mathfrak{p}_2^2)_F \longrightarrow X_0(\mathfrak{p}_2)_F = \mathbf{P}^1_F$*, is given by VI.*(5.4)*:*

$$\begin{aligned} f_{2,F(\sqrt{-7})} =& \frac{1}{x - \frac{1}{32}(91z+169)}\Big[\frac{1}{12544}(-z+11)x^4 + \frac{1}{12544}(-27z-151)x^3 \\ &+\frac{1}{3136}(71z-109)x^2 + \frac{1}{3136}(491z+4231)x + \frac{1}{3136}(-8411z-14971) \\ &+y\Big(\frac{1}{614656}(-13z-49)x^3 + \frac{1}{153664}(205z+49)x^2 \\ &+\frac{1}{76832}(-317z+1519)x + \frac{1}{153664}(-2613z+5831)\Big)\Big]. \end{aligned}$$

(iii) The equations for the reduction over $\mathbf{F}_{3^6}$ *of the* canonical cover after the quadratic extension to $F(\sqrt{-7})$*:* $f_2 : X_0(\mathfrak{p}_2^2)_{F(\sqrt{-7})} \longrightarrow X_0(\mathfrak{p}_2)_{F(\sqrt{-7})} = \mathbf{P}^1_{F(\sqrt{-7})}$*, and likewise for the Atkin–Lehner involutions, are given by Equations VI.*(5.7) *to* (5.10)*. Luckily for us, they descend over* $\mathbf{F}_3$*:*

$$\begin{aligned} f_2(x,y) &= \frac{1+x^2+x^3+x^4+(x+2x^2)y}{2+x^2+x^3+x^4+x^2y} \\ X_0(\mathfrak{p}_2^2)_{\mathbf{F}_3} &: y^2 = x^3 + x^2 + 2 \\ w_2 &: X_0(\mathfrak{p}_2^2)_{\mathbf{F}_3} \ni P \longrightarrow (1,2,1) - P \\ w_1 &: t \in \mathbf{P}^1_{\mathbf{F}_3} \ni t \longrightarrow -t \end{aligned}$$

Proof (i) Recall that the verifications done in the paragraph "Additional monodromy computations "$f_{2,\mathbf{Q}}$" prove that the equation of $f_{2,\mathbf{Q}}$ given in (6.1) (i.e. (5.12)) coincides with the *unique* descent of the canonical cover $f_{2,F}$ over $\mathbf{Q}$ (up to $\mathbf{Q}$-isomorphism).

(ii) Consider the ramification diagram of $X_0(\mathfrak{p}_2^i)$ in §5.1. Here, "rational" means "rational over F", the field of definition of the canonical covers. The rational point R_7 has two preimages that are ramified of order one by the rational map $f_{1,F}$: Q_7 and Q_7'. So they are quadratic conjugate over F. The formula in equation (5.3) even shows that they have coordinates in $F(\sqrt{-7})$.

Each of these points have a unique preimage by $f_{2,F}$ that is ramified of order one: P_7 and P_7'. So P_7 is defined over $F(\sqrt{-7})$: this shows that the base field extension of the canonical model : $X_0(\mathfrak{p}_2^2)_{F(\sqrt{-7})}$ is an *elliptic curve*. So it is equal to its Jacobian over $F(\sqrt{-7})$.

By arguments with the conductor and the j-invariant, we could determine its equation in the paragraph "Theoretical predictions for the canonical models": VI.(5.2), recalled in (ii).

(ii') Firstly, the whole purpose of (ii') is to give an equation for $f_{2,F(\sqrt{-7})}$ with smaller coefficients than the output of the algorithm of [KVMSV].

But there certainly exists more clever methods than our whole recomputation.

From now on, our goal is to certify that the map $f_{2,F(\sqrt{-7})}$ given in (ii') has the same monodromy as that of the canonical cover: σ_2 or σ_2'. Because then, by the same unicity argument as in (i), they will coincide.

Unfortunately as pointed at the end of "Additional monodromy computations", we were not able to do the same numerical verification as in (i). Hence this time the map $f_{2,F(\sqrt{-7})}$ is not defined over $\mathbf{Q}$ and Maple had trouble with the input given in floating complex numbers. There exists plenty of (privately implemented) numerical methods to overcome this.

But for now in this case, we got along with a cheaper method. At the cost of the following lengthy argumentation:

- Firstly, we know from (ii) the reduction of $X_0(\mathfrak{p}_2^2)$ over $\mathbf{F}_3(\sqrt{-7})$, and also that of $X_0(\mathfrak{p}_2)_{\mathbf{F}_3(\sqrt{-7})} = \mathbf{P}^1_{\mathbf{F}_3(\sqrt{-7})}$;
- Then, an exhaustive computation shows that there exist only two isomorphism classes of covers over $\mathbf{F}_3(\sqrt{-7})$: call them $f_{2,\mathbf{F}_3(\sqrt{-7})}$ and $\overline{f_{2,\mathbf{F}_3(\sqrt{-7})}}$ that have the same ramification pattern than the canonical cover $f_{2,F}$.

(Unicity) Thirdly, an exhaustive search for Hensel liftings shows that there exists *only* two isomorphism classes of covers over $F(\sqrt{-7})$: $f_{2,F(\sqrt{-7})}$ and $\overline{f_{2,F(\sqrt{-7})}}$ with this ramification pattern: the first one is given in (ii'). (We ensured exhaustivity very recently).

(Existence) But, remember that the algorithm of [KVMSV] certifies that there exists two isomorphism classes of covers: $X_0(\mathfrak{p}_2^2)_{F(\sqrt{-7})} \longrightarrow X_0(\mathfrak{p}_2)_F =$

$\mathbf{P}^1_F$ with this ramification pattern, *and whose monodromies are given by* σ_2 *or* σ_2' (this is how we found that $X_0(\mathfrak{p}_2^2)_{F(\sqrt{-7})}$ was the canonical model).

- thus by unicity, the covers $f_{2,F(\sqrt{-7})}$ and $\overline{f_{2,F(\sqrt{-7})}}$ are equal to the latter and thus their monodromies are given by σ_2 and σ_2'. One of them is the canonical one, and the other is isomorphic to the Atkin–Lehner twist. Since we are going to take the fiber product of the two, the ordering is not important.

(iii) The proof of (ii') shows that the two covers $f_{2,\mathbf{F}_3(\sqrt{-7})}$ and $\overline{f_{2,\mathbf{F}_3(\sqrt{-7})}}$ that we started from, are indeed the reduction of the canonical covers! □

6.2 On the form of a rational function on an elliptic curve, by H. Randriam

Proposition 6.1. *Let E be an elliptic curve and f a rational function of degree d. Let O_E be the point at infinity. Denote $div(f) = Z - D$ with avec Z, D prime to one another and effective of degree d. Then*

- *either the points of D with multiplicities sum to zero (and thus Z also), then f can be expressed as a rational fraction u/v of degree d;*
- *or D does not sum to zero. Then f can be expressed as a rational fraction u/v of degree $d+1$*

Proof One first looks for u in $L(dO_E)$ such that $v = fu$ in $L(dO_E)$, which is equivalent to ask for $div(u) = D - dO_E$, possible if and only if D sums to O_E.

If it is not the case, then one chooses u in $L((d+1)O_E)$ such that $div(u) = D + (-P) - (d+1)O$. Then one concludes likewise with $v = fu$ in $L((d+1)O_E)$. □

6.3 Simpler equations for the twisted covers, including over $\mathbf{F}_5$

As mentionned in Remark 5.6, the Atkin–Lehner twists of the covers f_2 could have shorter equations if they were computed directly from their ramification

data. This is what we did, with the help of the previous argument on rational functions (a cover of $\mathbf{P}^1$ is a rational function).

- For $f_{2,\mathbf{Q}} : X_0(\mathfrak{p}_7^2)_{\mathbf{Q}} \longrightarrow X_0(\mathfrak{p}_7)_{\mathbf{Q}}$:

$$f_{2,\mathbf{Q}}(x,y) = 2x + 5x^2 - 3x^3 + (-3 + 3x + x^2)y \text{ branched over} \tag{6.6}$$

$$w_1 \circ f_{2,\mathbf{Q}} \circ w_2 = \frac{1}{(x-2)^4}\Big(x^4 + 4x^3 + 4x^2 + 3 + y\big(x^2 + 3x + 2\big)\Big) \tag{6.7}$$

- For the reduction $f_{2,\mathbf{F}_3(\sqrt{-7})} : X_0(\mathfrak{p}_2^2)_{\mathbf{F}_{3^6}} \longrightarrow X_0(\mathfrak{p}_2)_{\mathbf{F}_{3^6}} = \mathbf{P}^1_{\mathbf{F}_3^6}$, which descends over $\mathbf{F}_3$:

$$f_{2,\mathbf{F}_3}(x,y) = \frac{2x^4 + 2x^2 + x + 2 + y\big(x^3 + x^2 + 2\big)}{x^2 + y\big(x^2 + x + 2\big)} \tag{6.8}$$

$$w_1 \circ f_{2,\mathbf{F}_3} \circ w_2 = \frac{2x^4 + 2x^2 + x + 2 + y\big(2x^3 + 2x^2 + 1\big)}{2x^2 + y\big(x^2 + x + 2\big)} \tag{6.9}$$

- Likewise, the cover $f_{2,\mathbf{F}_5(\sqrt{-7})} : X_0(\mathfrak{p}_2^2)_{\mathbf{F}_{5^6}} \longrightarrow X_0(\mathfrak{p}_2)_{\mathbf{F}_{5^6}} = \mathbf{P}^1_{\mathbf{F}_5^6}$ and its Atkin–Lehner twist luckily descend over $\mathbf{F}_5$:

$$f_{2,\mathbf{F}_5} = \frac{3x^4 + 4x^2 + 4x + 1 + y\big(2x^3 + x + 4\big)}{2x^3 + 3x^2 + 4 + y\big(x^2 + x + 2\big)} \tag{6.10}$$

$$w_1 \circ f_{2,\mathbf{F}_5} \circ w_2 = \frac{2x^4 + x^3 + 3x^2 + 2x + 2 + y\big(2x^2 + x\big)}{x^4 + x^3 + x^2 + x + 3 + y\big(2x^2\big)} \tag{6.11}$$

But our computations to verify the next step $X_0(\mathfrak{p}_2^3)_{\mathbf{F}_{5^2}}$ did not end yet. So we wait a bit before claiming that Theorem B also holds over $\mathbf{F}_5$ with Shimura curves. This would then prove that the figure 4,74 in Table 2.2 can indeed be reached with Shimura curves.

Chapter VII

Explicit symmetric multiplication algorithms

1 Roadmap

As a motivation, consider the inequality (1.2) of Theorem I.1.1 and *fix the degree of the divisor* G. It is equal to $\deg G = \sum_i u_i.d_i$, where d_i is the degree $\deg P_i$. Then –as one sees from table I.2.1– the upper bound on $\mu_q^{\mathrm{sym}}(m)$ given by the RHS of the inequality will be all the more large that the degrees of the points P_i and their multiplicities u_i are big.

We are going to discuss this issue in the symmetric case, because the bound of Corollary 1.2 leaves more room for improvement than the assymmetric bound of Proposition 1.5.

So let us set $D = D_1 = D_2$, and remind recall that the three divisors (G, D, Q) must simultaneously respect the conditions of Theorem I.1.1. Call such an admissible triple (G, D, Q) an *interpolation system*.

Thus, to minimise the symmetric bilinear complexity of the multiplication in $\mathbf{F}_{q^m}$, one is lead to:

1 Collect (and improve) the best bounds for the $\mu_q^{\mathrm{sym}}(m, l)$;

2 Find curves with many points P_i of low degree;

3 For such a curve X, fix a (small) degree $\deg G$ of G such that one hopes the existence of an admissible interpolation system (G, D, Q) on X (as precised in next section). For this candidate value of $\deg G$,

find a combination $(u_i, P_i)_i$ of points and multiplicities that, numerically, minimises the upper bound of Theorem I.1.1 under the constraint $\deg G \geq \sum_i u_i . \deg P_i$;

4 For this fixed candidate value $\deg G$, given such a numerically optimal $G = \sum_i u_i P_i$, check the existence of an interpolation system (G, D, Q).

1 is the motivation for I.2.3. The methods to find the new bounds are described in the next section. 2 is the motivation for the last section. 3 is an integer programme and will be illustrated in §3.2. 4 will be discussed in the next section.

2 (Improved) search for optimal multiplication algorithms in $\mathbf{F}_{2^m}[y]/y^l$

2.1 The algorithm

To obtain the new upper and lower bounds, we built on the exhaustive search method introduced in [Oce], then in [BDEZ]. We would like first to share our techniques of implementation and search that contributed to these results. And last, regarding the new lower bounds, we give the arguments that make our computational proofs valid and reproducible, especially when new shortcuts are involved.

Let K be a field, $\mathcal{A} = K^p$ a K-vector space of dimension p and B a (symmetric) K bilinear map, taking here values in $\mathcal{A}$, seen as a tensor in $\mathcal{A}^* \otimes \mathcal{A}^* \otimes \mathcal{A}$. Then, evaluation on the last component $\mathcal{A}$ defines a "coordinate" map[1]:

$$\mathcal{A}^* \to \mathcal{A}^* \otimes \mathcal{A}^* ,$$

whose image is a K-vector subspace noted T. Let $\mathcal{G}$ be the set of (symmetric) bilinear forms of rank one in $\mathcal{A}^* \otimes \mathcal{A}^*$. Thus from k generators of T in $\mathcal{G}$, one deduces explicit decompositions of B of rank k. Then the (partially symmetric) tensor-rank of B is equal to the least number k, of elements of $\mathcal{G}$, necessary to generate T.

Going in the other direction, the incomplete basis theorem implies that: a subspace W of dimension k of $\mathcal{A}^* \otimes \mathcal{A}^*$, which both (i) is generated by

[1] This could be seen as a "tensor-flattening map", but we ignore how far this helps.

elements of $\mathcal{G}$ and (ii) contains T, can be generated by a basis of T completed with elements of $\mathcal{G}$

E.g. in the case where B is the multiplication in a K-algebra $\mathcal{A}$, then one need to complete exactly with $k-n$ elements. Because the subspace T is of dimension n as soon as $\mathcal{A}$ has a unit.

These arguments validate the following algorithm ([BDEZ]), which both: given an integer k, determine if B is of rank strictly greater than k and, if not, find all the decompositions of length k of B.

Algorithm 2.1. *Start with the subspace $W = T$ of $\mathcal{A}^* \otimes \mathcal{A}^*$, of dimension n. Then, for each element $\boldsymbol{g}$ of $\mathcal{G}$ independent from W, complete W by $\boldsymbol{g}$, to obtain $W' = W \oplus \boldsymbol{g}$ of dimension $n+1$. Iterate until the dimension reaches k. Test if the subspace obtained is generated by elements of $\mathcal{G}$. If it is not the case for all the subspaces produced, it thus implies that the (partially symmetric) rank of B is strictly greater than k.*

In practise, the algorithm first produces, by recursion on the dimension, all subspaces W of dimension k in $\mathcal{A}^* \otimes \mathcal{A}^*$, that can be generated from T completed with elements of $\mathcal{G}$. Then, for each subspace, tests if it is generated by elements of $\mathcal{G}$ (the production and testing stages are actually simultaneous, in order to cut nodes of the recursion on the fly).

2.2 Improvements

We describe now three implementation techniques that saved us significant computation time.

(1) When looking for a symmetric decomposition of a symmetric bilinear form B, the entire research can be implemented in the subspace of symmetric bilinear forms;

(2) As pointed by F. Courbier, the final step of the algorithm can be sped up. Instead of systematically computing the rank of $\mathcal{G} \cap W$, one can check beforehand if its cardinality is lower than[2] $\dim W$;

[2]This leads to noticing that, for algebras of dimension greater than 7, letting k be the known upper bound for the tensor rank of multiplication, then a general subspace W of dimension k in $(\mathcal{A}^* \otimes \mathcal{A}^*)^{\mathrm{Sym}}$ will *a priori contain less than 0.01 rank-one tensor. Thus, it would be interesting to know how to restrain the search to subspaces with a higher density of rank-one tensors.*

(3) To avoid testing several times the same subspace, one can fix once for all an ordering on $\mathcal{G} = (g_1, \ldots, g_M)$. Then, at each step of the recursion, complete $W = T \oplus K\boldsymbol{g_{i_1}} \oplus \ldots K\boldsymbol{g_{i_s}}$ by only the vectors $\boldsymbol{g}$ in $\mathcal{G}$ numbered *after* $\boldsymbol{g_{i_s}}$.

Finally, we put apart an observation that, either, helps finding quicklier a decomposition of given length k (and thus an upper bound), or, when none exists, gives a theoretical shortcut to establish this nonexistence[3].

Observation 2.2. *Suppose that a group H of linear transformations of $E = \mathcal{A}^* \otimes \mathcal{A}^*$:*

(i) preserves the set $\mathcal{G}$ of symmetric rank-one bilinear forms;
(ii) preserves the subspace T spanned by the components of the bilinear map B.

Then, given an element $g \in \mathcal{G}$, there exists a subspace W of dimension k solution of the problem (i.e. (a) generated by rank one bilinear forms and (b) containing T), if and only if, for each element $h(g)$ in the orbit of g under H, there exists a subspace W' of dimension k which is a solution of the problem

The observation has the following consequence. Suppose that one wants to perform a recursive search (say for rank k, so a recursion of depth $k-n$). Then it is enough to fix one element $\boldsymbol{\gamma_j} \in \mathcal{G}$ per orbit $\mathcal{O}_j = H.\boldsymbol{\gamma_j}$ (the orbit representatives). And to perform the recursion with the first element g_{i_0} equal to one of the representatives $\boldsymbol{\gamma_j}$. So this greatly narrows the choice of the first element.

Note that the work [Svy] has, since, generalized this observation. Among other improvements, it computes on the fly the stabilizer of the subspace obtained at every step of the recursion.

Here are two examples. In the case of a *finite field extension* $\mathcal{A} = \mathbf{F}_{q^m}/\mathbf{F}_q$, there is one single big orbit in the set $\mathcal{G}$ of symmetric bilinear forms, under the action of the group of invertible elements $H = \mathbf{F}_{q^m}^{\bullet}$ defined by composition with two-side multiplication :

$$b \in \mathbf{F}_{q^m}^{\bullet} : \lambda(\cdot\,,\cdot) \longrightarrow \lambda(b\,\cdot, b\,\cdot) \tag{2.1}$$

Consider now the algebra

$$\mathcal{A} = \mathbf{F}_{q^m}[y]/y^l = \mathbf{F}_q\big\langle (x^i y^j)_{\substack{i=0\ldots m-1 \\ j=0\ldots l-1}} \big\rangle.$$

[3]This method might be an elementary case of tensor decomposition methods. It originated thanks to an apparently innocuous lecture of G. Cohen on cyclic codes.

The dual is $\mathcal{A}^* = \mathbf{F}_{q^m}[y^*]/y^{*,l}$, where $y^{*,j}$ is the linear form that sends x^0y^j to one and the other standard basis elements to zero. The group of invertible elements $H = \mathcal{A}^\bullet$ is equal to the polynomials of valuation zero in y. Consider the action of H on the symmetric tensors of rank one $\mathcal{G} \subset \mathcal{A}^* \otimes \mathcal{A}^*$, defined the same way as previously.

Then there are l orbits $\{\mathcal{O}_0, \ldots, \mathcal{O}_{l-1}\}$. The orbit $\mathcal{O}_j = H.(y^{j,*})^{\otimes 2}$ consists in the symmetric bilinear forms of rank-one expressible $\phi^{\otimes 2}$, where ϕ is a polynomial of degree exactly j in y^*. In particular the largest orbit is $\mathcal{O}_{l-1}$ and consists of elements $\phi^{\otimes 2}$ such that, said otherwise, ϕ is not zero on at least one element in $\mathcal{A}$ of degree $l-1$ in y.

Regarding this last example, notice in addition that any minimal (symmetric) multiplication algorithm will involve at least one element of the greatest orbit $\mathcal{O}_{l-1}$. So this narrows the search for subspaces containing the tensor's space of components T.

2.3 Perspectives

These computations were performed with the C library [M4rie] dedicated to fast linear algebra in characteristic two. But far less computer resources were used than in [BDEZ]. So we hope that these refinements of the method –and more certainly the further improvements of [Svy]– will help find more bilinear formulas. E.g. find if $\mu_4(1,6) \leq 13$?, as proposed in remark I.2.11, or find if $\mu_2(7,1) \leq 18$?, as proposed in remark I.2.13.

3 Best expectable complexity using a given curve

3.1 Best expectable interpolation systems

We introduce new results and tools that help finding optimal interpolation systems on a given curve.

Let X be a curve of genus g over $\mathbf{F}_q$. An *optimal symmetric interpolation system on X with respect to multiplication in a finite field extension* $\mathbf{F}_{q^m}$, is a triple (G, D, Q) that provides a symmetric multiplication algorithm in $\mathbf{F}_{q^m}$, reaching a *lower bound* for the complexity of the Chudnovsky-Chudnovsky interpolation method on X. This will be precised in Definition 3.5.

The first two key-observations were brought to us by H. Randriam.

Observation 3.1. *When $H^1(X, \mathcal{O}(D)) = 0$, the sufficient condition (ii') in Theorem I.1.1 is in fact* equivalent *to (ii). Moreover, it is remarkable that this situation happens, for instance, when* $\deg D \geq 2g - 2$, *by the Riemann-Roch theorem.*

Indeed, one then has the shortened exact sequence :

$$0 \to H^0(X, \mathcal{O}(D-Q)) \to H^0(X, \mathcal{O}(D)) \xrightarrow{ev_Q} \mathcal{O}_{X,Q}/(t_Q) \to \ldots \\ \ldots \to H^1(X, \mathcal{O}(D-Q)) \to 0 \tag{3.1}$$

Observation 3.2. *Let X be a curve of genus g over $\mathbf{F}_q$, m an integer and Q a closed point of degree m. Suppose that there exists an interpolation system (G, D, Q) on X, with Q of degree m, which furthermore satisfies the sufficient condition (ii') of Theorem I.1.1. Then,* $\deg G \geq 2m + g - 1$.

Proof Let (G, D, Q) be the interpolation system of the hypothesis, and n (reps. d) the degree of G (resp. D). By condition (i) of Theorem I.1.1, $l(2D - G) = 0$. Thus, the theorem of Riemann–Roch applied to $2D - G$ yields:

$$2d - n \leq g - 1 \tag{3.2}$$

In addition, by condition (ii') of Theorem I.1.1, which is satisfied here by assumption, $i(D - Q) = 0$. Thus, the theorem of Riemann–Roch applied to $D - Q$ yields $d - m \geq g - 1$. Multiplication by -2 of this inequality yields:

$$-2(d - m) \leq -2(g - 1) \tag{3.3}$$

Summing (3.2) with (3.3), leads to $2m - n \leq -g + 1$. □ □

Lemma 3.3. *Let X be a curve of genus g, m an integer and Q a closed point of degree m. Suppose furthermore that $\boldsymbol{m > g}$. Then, any divisor D belonging to an interpolation system (G, D, Q) on X satisfies* $\deg D \geq m + g - 1$.

Proof Note d the degree of D.

First case : suppose $2g - 2 < d < m + g - 1$ (which is not an empty case as soon as g is strictly lower than $m-1$). Then, for degree reasons, $i(D) = 0$. Thus the Riemann-Roch theorem implies $l(D) = d+1-g < m = \dim \mathbf{F}_q(Q)$. Therefore, the evaluation map (ii) of Theorem I.1.1 cannot be surjective, for dimension reasons.

Last case : suppose $d \leq 2g-2 < m+g-1$. Then, K being the canonical divisor of X, the Riemann-Roch theorem and Serre duality imply that $l(D) = l(K-D)+d+1-g$. But $K-D$ being of non-negative degree, we also have the bounding $l(K-D) \leq 2g-2-d+1$. Thus, $l(D) \leq g < m = \dim \mathbf{F}_q(Q)$, thus the same contradiction as previously. □ □

The following consequence was known to H. Randriam before it was published in our paper [Ra, Table 1].

Proposition 3.4 (Properties of optimal interpolation systems)**.** *Let X be a curve of genus g, m an integer and Q a closed point of degree m. Suppose furthermore, as previously, that $\boldsymbol{m > g}$. Then :*

1. *The degree of an interpolation divisor G, belonging to an interpolation system (G, D, Q), cannot be lower than $2m+g-1$;*

2. *For such an interpolation system, i.e. with $\deg G$ attaining the lower bound $2m+g-1$, then the degree of D is necessarily equal to $m+g-1$.*

Proof Let (G, D, Q) be an interpolation system with Q of degree m. Note d the degree of D. Firstly, d being strictly greater than $2g-2$, observation 3.1 applies. Hence, the interpolation system satisfies (ii'). Thus, observation 3.2 applies : G cannot be of degree lower than $2m+g-1$.

For the second part, let (G, D, Q) be an interpolation system as in the assumption, that is with Q of degree m and $\deg G$ attaining the lower bound $2m+g-1$. Then, recall that by inequality (3.2), $2d - \deg G \leq g-1$. Thus here, $d \leq m+g-1$. But by the previous lemma, we also have the opposite inequality : $d \geq m+g-1$. □ □

Definition 3.5. Let X be a curve of genus g over $\mathbf{F}_q$, and m an integer. Suppose furthermore, as previously, that $\boldsymbol{m > g}$. An *optimal interpolation system on X* in degree m is a triple (G, Q, D), with Q of degree m, that satisfies the three following conditions :

1. Satisfies the conditions (i') and (ii') of Theorem I.1.1;

2. $\deg G$ reaches the lower bound $2m+g-1$ of proposition 3.4;

3. G is *numerically optimal*, that is : write $G = u_1P_1 + \cdots u_nP_n$, then, this combination of points P_i and multiplicities u_i minimizes the upper bound on $\mu_q^{\mathrm{sym}}(m)$ given by Theorem I.1.1.

Proposition 3.6 (Effective construction)**.** *Let X be a curve of genus g, such that there exists an optimal interpolation system (G, D, Q), with Q of degree m. Note $\mathrm{Cl}^0(X)$ the zero-class group of X. Then, it is possible to build (G, D, Q) with at most twice $\#\mathrm{Cl}^0(X)$ emptiness-checkings of Riemann–Roch spaces*[4]*.*

Indeed, first notice that, (G, D, Q) being optimal by assumption, the degree of D is $m + g - 1$ by proposition 3.4. In particular by Observation 3.1, the sufficient condition (ii') of Theorem I.1.1 is actually *equivalent* to (ii). Thus, one does not miss any optimal interpolation system (G, D, Q) by checking conditions (i') and (ii') instead of (i) and (ii). Secondly, notice that conditions (i') and (ii') depend only on the class of $D - Q$ (resp. $2D - G$) in $\mathrm{Cl}^0(X)$.

Step 1 : Look for a numerically optimal G, of degree $2m + g - 1$, whose class has not been already produced in the previous runs[5] of Step 1, then proceed to Step 2.

- Step 2 : look for a divisor D, of degree $m+g-1$, such that $l(2D-G) = 0$, and such that the class of D has not been considered yet in the previous runs[6] of Step 2. If such a D exists, proceed to Step 3.
  - Step 3 : find every possible closed point Q of degree m, such that the class of $D - Q$ in $\mathrm{Cl}^{g-1}(X)$ has not been tested yet in the previous runs of Step 3, and then test if $i(D - Q) = 0$[7]. If so, return (G, D, Q).

[4] Actually, both computations for (i') ("Step 1") and (ii') ("Step 2") will here occur in the group Cl^{g-1}, so one can remove the factor 2, as soon as one keeps in memory all the classes of divisors already tested

[5] Enumerating the (classes of) *numerically optimal* divisors on X is performed in two steps : (1) enumerate each collections of integers $(n_{d,u})_{d,u}$ (where $n_{d,u}$ stands for the number of points of degree d involved with multiplicity u in G), that (a) minimise the upper bound of Theorem I.1.1: $\sum_{d,u} n_{d,u}\mu_q^{\mathrm{sym}}(d, u)$, under the constraints that (b) the total degree $\sum_{d,u} n_{d,u}du$ (is greater or) equal to the above lower bound $2m + g - 1$, and (c) for each d, $\sum_u n_{d,u}$ is lower or equal to the number of points of degree d in X. (2) for each collection $(n_{d,u})_{d,u}$, enumerate the divisors involving exactly $n_{d,u}$ points of degree d with multiplicity u

[6] This involves at most $|\mathrm{Cl}^0(X)|$ emptyness checks of Riemann–Roch spaces in $\mathrm{Cl}^{g-1}(X)$ (minus those already performed in the previous runs).

[7] This involves at most $|\mathrm{Cl}^0(X)|$ emptyness checkings of Riemann–Roch spaces in Cl^{g-1}. ($D-Q$ being here of degree $g-1$, the theorem of Riemann–Roch implies that this condition is equivalent to $l(D - Q) = 0$)

  - If we are here, this means that the last run of Step 3 did not return any solution. Assuming that an optimal interpolation system does exist, this implies that there remain classes $(C_1 \dots C_s)$ in $\mathrm{Cl}^m(X)$, which have not been tested yet in the previous runs of Step 3. Thus, return to Step 2.

- If we are here, it means that no divisors D were found in Step 2. Then, the assumption for the existence of an interpolation system implies that: there exists another numerically optimal divisor G'', and another D'', such that there exist classes $(C_1, \cdots, C_s)$ in $\mathrm{Cl}^{g-1}(X)$, that have not been tested in Step 3 and are of the form $(D'' - Q_i)_{i \in I}$. Thus, return to Step 1.

Remark 3.7. Under the additional assumption where points Q of degree m would exist in every single class $\mathrm{Cl}^m(X)$, then the first run of Step 3 always returns a solution as soon as an optimal interpolation system exists. Thus, if no solution is returned, this is a proof that no optimal interpolation system of degree m does exist on X.

It is to be noted that, even if the case of elliptic curves can be dealt with directly, a proof of the additional assumption in this case does exist. Indeed [Sho, Th. 27] states that, for $q \geq 7$ (and presumably ≥ 4 for m sufficiently large), for $m \leq 2^{4096}$, there exists a prime divisor of degree m in every class[8]. Any analogous proof in higher genus would be of interest.

3.2 The example of elliptic curves, over $\mathbf{F}_2$

Lowest expectable value for the degree of G

We first recall the known sufficient conditions to build interpolation algorithms on elliptic curves over a general $\mathbf{F}_q$ ([Ran$_1$, Prop. 4.3]) :

Proposition 3.8. *The notations being as in Theorem I.1.1, let X be an elliptic curve over $\mathbf{F}_q$ and P_∞ the neutral element of the group of points of $X(\mathbf{F}_q)$. Let m be an integer. Suppose that X admits a closed point Q of degree m. Let G be an effective divisor on X, written as:*

$$G = u_1 P_1 + \ldots + u_n P_n \,, \tag{3.4}$$

[8] There is actually a mistake in Lemma 19 of loc. cit.: in the first line of (2), μ is actually meant to be n/v_r. Thus, in the last but one line, μ can actually be equal to 1 when n has no square factors. Anyway this is compensated when, *e.g.*, m is greater than $6! = 720$.

where the P_i are pairwise distinct closed points of degrees $\deg P_i = d_i$, *so* $\deg G = \sum_{i=1}^{n} d_i u_i$. *Then,*

$$\mu_q^{\mathrm{sym}}(m) \leq \sum_{i=1}^{n} \mu_q^{\mathrm{sym}}(d_i, u_i)$$

provided one of the following conditions is satisfied :

(i) $\deg G = 2ml$ *and* $|X(\mathbf{F}_q)| \geq 2$ *and* $\mathrm{Cl}^0(X)$ *is not entirely of 2-torsion.*

(ii) $|X(\mathbf{F}_q)| \geq 2$ *and* $\deg G \geq 2ml + 1$.

Furthermore if the additional criterion on G is satisfied:

$$\textit{the divisor } G - \deg G.P_\infty \text{ is not equivalent to } 0$$

then $\deg G$ *can even be taken equal to* $2ml$.

(iii) $\deg G \geq 2ml + 3$.

Taking the example of $\mathbf{F}_2$, the five equivalence classes of elliptic curves over this base field are given by the following equations.

$$y^2 + y + x^3 + x + 1 = 0 \tag{3.5}$$
$$y^2 + xy + x^3 + x^2 + 1 = 0 \tag{3.6}$$
$$y^2 + y + x^3 = 0 \tag{3.7a}$$
$$y^2 + y + x^3 + x = 0 \tag{3.7b}$$
$$y^2 + xy + x^3 + 1 = 0 \tag{3.7c}$$

In Table 3.1 below, we classify these curves along the previous conditions. For each curve X we give: the number B_1 of integral points, the structure of the group of points $\mathrm{Cl}^0(X)$ and, thus, the smallest degree of G satisfying the previous sufficient conditions: we call this value "upper-bound". In addition, we also bound below the degree $\deg G$ of an interpolation divisor on X (distinguishing whether or not the additional criterion on G is satisfied). Regarding the 2-torsion case, we finally explain why it is in fact nearly always possible to find a divisor G satisfying the additional condition. Before giving proofs, we can notice that all the lower bounds were actually reached by the previously known upper-bounds[9].

[9]The proofs and results for this column are the same on a general base field $\mathbf{F}_q$. And

Table 3.1: Lower-upper bounds for the degree of the best interpolation divisor G

Curve	B_1	Cl^0	Additional criterion on G	Lower bound on $\deg G$	Upper bound on $\deg G$	Is the additional criterion on G satisfiable ?
(3.5)	1	0	.	$\mathbf{2ml+3}$	$2ml+3$	.
(3.6)	2	$\mathbf{Z}/2$	when false :	$\mathbf{2ml+1}$	$2ml+1$	**yes, for nearly all $m \leq 2^{4096}$**
			when true :	$2ml$	$2ml$	
(3.7a)	3	$\mathbf{Z}/3$	.	$2ml$	$2ml$	.
(3.7b)	5	$\mathbf{Z}/5$				
(3.7c)	4	$\mathbf{Z}/4$				

Demonstrations **Curves** (3.7a)**,** (3.7b)**,** (3.7c) **and [**(3.6) **when criterion on G true]** : the *lower-bounds* settled at $2ml$ are a direct consequence of Prop. 3.4,(1.)[10].

Curve (3.6) **- when criterion on G false** : if $\deg G$ were $2m$, then by Prop. 3.4,2 the degree of D would by m, thus $2D-G$ would be in the zero-class, thus $l(2D-G)$ would be one, which contradicts (i) by Riemann-Roch.

Curve (3.5) : *Firstly*, it is not possible to build a degree $2m$ interpolation divisor G. We reuse the arguments of [Ran_1] 4.7. The evaluation map ev_Q : $L(D) \longrightarrow \mathcal{O}_{X,Q}/(t_Q)$ fits in the long exact sequence

$$(3.8)\quad 0 \to H^0(X,\mathcal{O}(D-Q)) \to H^0(X,\mathcal{O}(D)) \xrightarrow{ev_Q} \mathcal{O}_{X,Q}/(t_Q) \to \ldots \\ \ldots \to H^1(X,\mathcal{O}(D-Q)) \to 0$$

But, D being of degree m by proposition 3.4, the Riemann-Roch theorem

regarding the discussion on the divisor G for the full 2-torsion curve (3.6), such cases of curves arise in finite number (indeed, it is a basic fact that the 2-torsion group of an elliptic curve is included in $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and on the other hand, curves have enough points for q sufficiently large). Furthermore, the classification provided by [BBT] shows that this number is small.

[10] And were probably known since Shokrollahi 1992

implies that $l(D) = m$. Also, the divisor $D - Q$ having degree 0 and (iii) having trivial class group, $D - Q$ is then equivalent to zero, thus $l(D - Q)$ is equal to 1. As a result, dimension-counting implies that the evaluation map ev_Q has image of dimension lower or equal to $m - 1$, thus cannot be surjective.

Secondly, $\deg G$ cannot be equal to $2m + 1$. Indeed, the previous arguments shows that, in order to have the surjectivity of the evaluation at Q map, one must have $d = \deg D > m$. Write $d = m + i$. Then, $\deg(2D - G) = 2i - 1 > 0$. Thus, $i(2D - G) = 0$ for degree reasons. So, by the Riemann-Roch theorem, $l(2D - G) = 2i - g = 2i - 1 > 0$. So the condition (ii') is false. But recall that, by observation 3.1, the degree of D being greater than $2g-2$, condition (ii) of Theorem I.1.1 is also not satisfied.

Finally, $\deg G$ cannot be equal to $2m + 2$. For that, writing again $d = m + i > m$, two cases are possible:

- Either $i > 1$, thus $\deg(2D - G) = 2i - 2 > 0$ so by the same argument as above, condition (ii) of Theorem I.1.1 is not satisfied;

- Or, $i = 1$. But then $\deg(2D - G) = 0$, thus linearly equivalent to zero, by triviality of the zero-class group of curve (iii). Thus $l(2D - G) = 1$, contradicting condition (i) of Theorem I.1.1.

Curve (3.6) **- satisfiability of the condition on G :** Claim : for each degree $m \leq 2^{4096}$, there exists a point P of degree m such that $P - mP_\infty$ does not lie in the zero class.

Proof of the claim: one adapts the estimations in [Sho] that lead to his Theorem 16 (1) (paying attention to a small mistake in the proof: see Footnote 8), replacing q and the p_i-torsion by their values, taking m great enough to compensate the new positive terms, and computationally check the values of m below this threshold.

End of the proof: for nearly all m, given a numerically optimal divisor G of degree $2m$ on Curve (3.6) (furthermore assumed not built using points of degree greater than 2^{4096}), it is possible to deduce a numerically optimal G' that does not lie in the zero-class (by swapping a couple of points and/or multiplicities)[11]. □

[11] Indeed, the possible degrees $\deg G = m_i$ for which this swapping is not possible, lie among those for which all the points P_i of X –up to a certain degree n_i– occur in G with equal multiplicities.

Table 3.2: Today's best possible upper bounds for $\mu_2^{\mathrm{sym}}(m)$ using elliptic curves

m	former upper bound ([BBT])	better bounds - with existing ingredients	best bounds - using improved ingredients
163	906	**905**	905
233	1340	**1339**	1339
283	1668	**1661**	1661
409	2495	**2494**	**2492**
571	3566	**3563**	**3562**

New bounds for the NIST-size extensions of $\mathbf{F}_2$

Five extensions of $\mathbf{F}_2$ are recommended by the NIST in [NIST] to perform elliptic-curve based cryptography, of degrees from $m = 163$ to 571. The best known bounds for the symmetric complexities of the multiplication in these extensions have been set in [BBT]. To achieve this, the authors used interpolation divisors G of the smallest degree given by the previous sufficient conditions 3.8. But we have just shown, in the previous paragraph, that these conditions on $\deg G$ could not be sharpened. Nevertheless, it is still possible to improve these five bounds.

Firstly, the authors seem to have used the value 15 as upper-bound on $\mu_2^{\mathrm{sym}}(1,6)$, although a better value, 14, is known (*cf.* Table I.2.1). Using this value, and interpolating on the curve of equation (3.7b) instead of (3.7a), already provides better bounds for all the five extensions considered. This is shown below in the third column of Table 3.2. Secondly, plugging in the three new bounds given in Table I.2.1, leads to further improved bounds for the two last extension degrees, as shown below in the last column of Table 3.2.

4 Further improvements, with classical modular curves

We are grateful to H. Randriam for guiding this first research work.

4.1 Method

The classical modular curves $X_0(N)_{\mathbf{F}_2}$ of computable size are also candidates to build interpolation systems. Indeed they are numerous and have many points of degree two (although degrees four or six are preferable, as shown by Table I.3.1).

Similarly to the point-counting on the jacobian described in §I.5, the number of $\mathbf{F}_{p^m}$-points of $X_0(N)_{\mathbf{F}_p}$ can be computed from the value of the trace of the Hecke operators T_{p^i}. Precisely, their action on the space of holomorphic differential forms (equivalently of cusp forms), which is of dimension g the genus of $X_0(N)$:

$$S_2 = H^0(\Omega_{X_0(N)}, \mathbf{C}).$$

An explicit formula is provided in [Mo, Cor. 5.10.1]. As a result, this enables to count closed points in the modular curves $X_0(N)_{\mathbf{F}_p}$ with analytic tools.

But computing with cusp-forms expansions cannot be performed in large level N. Instead, the space S_2 is preferably seen in the (twice) larger space of complex differential forms on $X_0(N)_{\mathbf{C}}$. Indeed one can describe, in a purely algebraic fashion, the action of the Hecke operators on the Poincaré dual, $H_1(X_0(N), \mathbf{C})$, using a preferred basis called "Manin symbols". This action is implemented in Sage [Sa]. Then, to retrieve the trace of the Hecke operators on the subspace, $H^0(\omega_{X_0(N)}, \mathbf{C})^*$, the following proposition shows that it suffices to divide by two the total trace:

Proposition 4.1. *There exists a common basis of cusp forms such that the matrices of the Hecke operators:*

$$T_n|_{S_2}$$

have rational coefficients.

Demonstrations The neat reformulation of the following argument greatly owes to H. Randriam. Define the $\mathbf{Q}$-algebra of dimension g generated by the Hecke operators acting on S_2:

$$\mathcal{A} = \langle T_n \rangle|_{S_2} \text{ (noted } \mathbf{T}' \text{ in [Ste, p54])},$$

so that the complexified $\mathcal{A} \otimes_{\mathbf{Q}} \mathbf{C}$ (noted $\mathbf{T}'_{\mathbf{C}}$ in loc. cit.) is a subspace of $\mathrm{End}_{\mathbf{C}}(S_2)$. Define

$$\mathcal{A}^* = \mathrm{Hom}_{\mathbf{Q}}(\mathcal{A}, \mathbf{Q}),$$

then [Ste, Proposition 3.24] states the isomorphism:

$$\begin{aligned} S_2 &\xrightarrow{\sim} \mathcal{A}^* \otimes \mathbf{C} \\ \omega &\longrightarrow \big\{ \cdot \to a_1\big(\cdot(\omega)\big) \big\} \end{aligned}$$

Claim : The natural rational action of $\mathcal{A}$ on $\mathcal{A}^*$, extended by $\otimes_{\mathbf{Q}}\mathbf{C}$ coincides, via this isomorphism, with the action of $\mathcal{A}$ on S_2. Proof: exercice.

End of the proof: the matrices of both actions are thus equal. □

4.2 Results

Data gathering

Having computed the number of closed points of degrees up to 10 on the $X_0(N)_{\mathbf{F}_2}$ for N up to 1300, we selected those which provide the best numerically optimal divisors G, for the same five extension of $\mathbf{F}_2$ as considered in the previous section.

We mainly used the equations given in the tables of [Ga] and [Ya], sometimes helped by Q. Liu's algorithm to find regular models of hyperelliptic curves in characteristic two.

although we recomputed those of $X_0(45)$ and $X_0(73)$ with the canonical embedding method.

In addition, we used the plane integral model of the genus four hyperelliptic curve $X_0(47)_{\mathbf{Q}}$ provided in [Ya], because this one had good reduction over $\mathbf{F}_2$.

However we could not find a model with good reduction modulo two for the interesting curves $X0(59)$ and $X_0(73)$ of genus five (which explains the empty fifth column of the following Table 4.1), nor for the interesting $X_0(141)$ of genus six.

It finally remains to check that these divisors G do belong to an optimal interpolation system, using the construction described in 3.6. This can be done in a timely manner, using a well-known proprietary software ([Ma]), which implements an algorithm of Hess for Riemann-Roch spaces computations.

Outcome and one example

The following Table 4.1 gives the best bounds obtained, using curves up to genus 6, for the $X_0(N)_{\mathbf{F}_2}$ which could actually be computed.

Table 4.1: Upper bounds on $\mu_2^{\mathrm{sym}}(m)$, sorted by the genera of the curves used

$m\backslash g$	1 (Tab. 3.2)	2	3	4	5	6
163	905	903	901	.	.	**900**
233	1339	1336	.	**1335**	.	.
283	1661	1660	.	**1654**	.	.
409	2492	2491	.	**2486**	.	.
571	3562	3561	3560	**3555**	.	.

Let us describe a reproducible run of algorithm 3.6, leading to the best entry (in bold) 900, for the extension degree $m = 163$. It is performed on the genus 6 curve $X = X_0(71)_{\mathbf{F}_2}$. The lowest expectable degree for G is $2\times163+6-1 = 331$ and, in this case, D should be of degree $163+6-1 = 168$. Setting the random seed to 0 in Magma, we fix once for all an enumeration of the points of X (up to degree 8). At this stage, it results from the bound of Theorem I.1.1 that a numerically optimal G would lead to 900.

Let us fix an isomorphism of the class group of X with $\mathbf{Z}/315\mathbf{Z}\oplus\mathbf{Z}$: the first generator (of degree 1) being called D_1 and the second (of degree 0), D_2.

Step 1 : (using the notations of Footnote 5) (1) (a) fix an optimal collection of integers : $n_{1,5} = 1$, $n_{1,6} = 3$, $n_{2,4} = 3$, $n_{3,1} = 4$, $n_{4,1} = 6$, $n_{5,1} = 4$, $n_{6,1} = 10$, $n_{8,1} = 21$, (b) which is of total degree 331 (c) and is compatible with the number of points on X of respective degrees up to 8. (2) Build a divisor G from this collection. A first attempt is to use the points in the order in which they were enumerated (so that, for the four points of degree one on X, the first is given multiplicity 5 and the three remaining multiplicity 6).

- Step 2 Building the class of D as $i.D_1 + 168.D_2$, with a varying coefficient i for D_1, it happens that for $i = 2$, the condition $l(2D - G) = 0$ is satisfied.

– Step 3 : With various random seeds, we generate random points Q of degree m in several classes[12]. It happens that with seed one, $i(D-Q)=0$, thus giving an optimal interpolation system (G,D,Q).

Perspectives

These computations, that date back to 2014, could now be updated by:

(i) Atkin–Lehner quotients of modular curves. Indeed these quotients contain as much supersingular points as the initial curve, but have a lower genera. In particular, a recent preprint of P. Mercury enlarged the tables of [Ga];

(ii) The curve of genus five over $\mathbf{F}_2$ with many points of degree *six* $X_0(\mathfrak{p}_7^3)_{\mathbf{F}_2}$ computed in §VI.5.3.

[12] In practise this is achieved by splitting only the place at infinity, so we do not know if this leads to every possible class for points of degree m.

Appendix A

Annexes

1 Shorter proofs for other descent criterions

Lemma 1.1. *Let*

$$(\dagger) \qquad 1 \longrightarrow N \longrightarrow G \underset{\pi}{\overset{s}{\rightleftarrows}} \Gamma \longrightarrow 1$$

be a split exact sequence of groups. The section s induces an action of Γ, by conjugacy, on the subgroups of G. Then one has the following bijection of sets:

$$\begin{array}{ccc} \{H,\ \Gamma \subset H \subset G\} & & \{H' \subset N \text{ with } H \text{ stable under } \Gamma\} \\ H & \overset{f}{\longmapsto} & H \cap N \\ \langle H', \Gamma \rangle & \overset{g}{\longmapsfrom} & H' \end{array}$$

Demonstrations La suite exacte étant scindée, elle est isomorphe à :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & N \rtimes_s \Gamma & \longrightarrow & \Gamma & \longrightarrow & 1 \\ & & & & (1,\gamma) & \overset{s}{\dashleftarrow} & \gamma & & \end{array}$$

Avec cette description, un sous-groupe H de G contenant Γ est égal à $\{(h,\gamma),\ h \in N \cap H \text{ et } \gamma \in \Gamma\}$. Par conséquent le sous-groupe

$$f(H) = H \cap N = \{(h,\gamma),\ h \in H \cap \Gamma\}$$

est bien stable sous Γ.

$\boxed{f \circ g = \mathrm{id}}$ Avec les expressions précédentes de H et de $N \cap H$, il reste à montrer que le sous-groupe

$$\langle N \cap H, \Gamma \rangle = \{(h, \gamma),\ h \in N \cap H \text{ et } \gamma \in \Gamma\}$$

est égal à H, ce qui est tautologique.

$\boxed{g \circ f = \mathrm{id}}$ C'est le sens moins évident. Il s'agit de vérifier que si H' est un sous-groupe de N stable sous Γ, alors le groupe engendré $\langle H', \Gamma \rangle$ est en fait réduit à l'ensemble

$$(H, \Gamma) = \{(h, \gamma),\ h \in N \cap H \text{ et } \gamma \in \Gamma\}.$$

Pour le voir, il suffit de remarquer que le produit

$$(h_1, \gamma_1).(h_2, \gamma_2) = (h_1.\gamma_1 h_2 \gamma_1^{-1},\ \gamma_1\gamma_2)$$

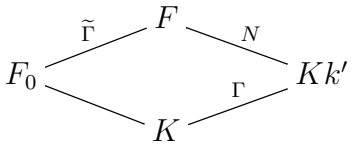
est encore dans (H, Γ) par hypothèse. □

The following proposition was communicated by H. Randriam:

Proposition 1.2. *Let k be a field and k' a Galois extension with group $\Gamma = \mathrm{Gal}(k'/k)$. Let K be an extension of k (for example $k(T)$) and F/K a finite Galois extension of group G, such that the sequence V.*(Seq/Split) *has a splitting s (for example under the hypotheses of Proposition V.2.6) :*

$$1 \longrightarrow N \longrightarrow G \underset{\overset{s}{\curvearrowleft}}{\longrightarrow} \Gamma \longrightarrow 1$$

with $N = \mathrm{Gal}(F/Kk')$ being again the fixator subgroup of Kk'. Define F_0 the sub-extension of F/K fixed by $\widetilde{\Gamma} = s(\Gamma)$:



Then one has the following bijection between two subsets of sub-extensions of $F \supset K$:

$$\left\{\begin{array}{c}\textit{sub-extensions } L_0, \\ K \subset L \subset F_0\end{array}\right\} \quad \left\{\begin{array}{c}\textit{sub-extensions } L',\ Kk' \subset L' \subset F, \textit{ such that} \\ \textit{the fixator subgroup } H' \subset N \textit{ is stable under } \widetilde{\Gamma}\end{array}\right\}$$

$$L_0 \overset{\varphi}{\longmapsto} L_0k'$$

$$F^{\langle \Gamma, H' \rangle} \overset{\psi}{\longmapsto} L' = F^{H'}$$

In particular if G is abelian, every subextension L', $Kk' \subset L' \subset F$, comes from an extension L/K of the same degree.

Demonstrations On remarque d'abord que φ préserve le degré des extensions (autrement dit que toute sous-extension de F_0/K est régulière). Pour des raisons de degré, il suffit de le montrer pour F_0/K. C'est à dire de montrer que $F_0k' = F$. Mais F_0k' est aussi une sous-extension de F/F_0, qui est galoisienne de groupe $\tilde{\Gamma}$. Donc pour conclure, il suffit de remarquer que le sous-groupe de $\tilde{\Gamma}$ fixateur de $\varphi(F_0)k'$, est réduit à $\{1\}$. C'est immédiat puisque $\tilde{\Gamma}$ agit sur k'/k par Γ.

On remarque ensuite que le premier ensemble correspond aux sous-extensions de F/K dont le groupe H contient $\tilde{\Gamma}$.

Enfin pour montrer la proposition, en vertu du lemme, il suffit de montrer que $\varphi(F^H) = F^{H\cap N}$. On a déjà l'inclusion $\boxed{\mathrm{Fix}(F^Hk') \supset H \cap N}$ car soit $(x_i)_i$ une base de L sur K, alors l'élément général de F^Hk' est $y = \sum_i \lambda_i x_i$, où les coefficients λ_i sont dans Kk'. Mais par définition N fixe les λ_i, H fixe les x_i donc $H \cap N$ fixe y.

On a ensuite l'égalité pour des raisons de degré : en effet F/L (respectively F/F_0) étant galoisienne, son degré est $|H|$ (respectively $|\tilde{\Gamma}|$). Donc le degré de F_0/L est $|H|/|\tilde{\Gamma}|$. Qui est égal à $|H/\tilde{\Gamma}|$, car H contient $\tilde{\Gamma}$ par la deuxième remarque. Donc par le lemme, l'intersection $H \cap N$ s'identifie à $\{(h, 1),\ h \in H \cap N\}$. Donc $|H/\Gamma| = |H \cap N|$. □

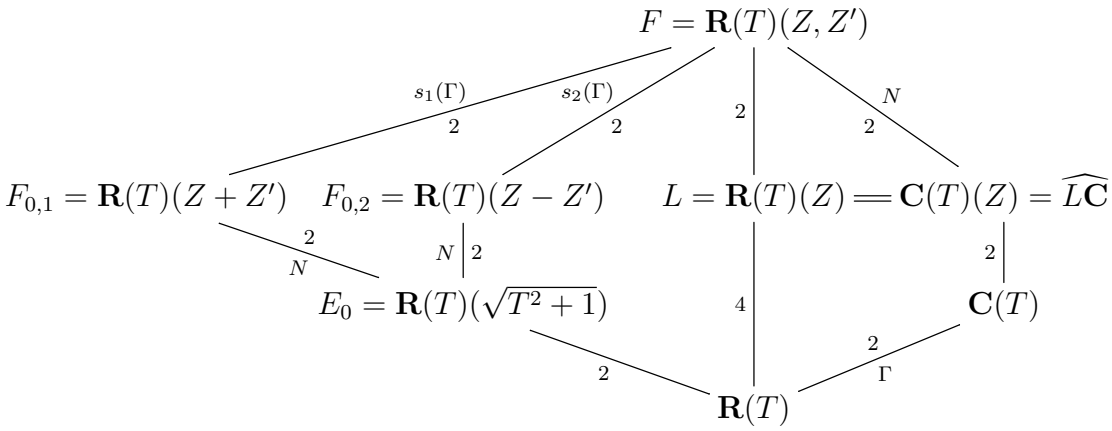
The following corollary was singled out by Randriam:

Corollary 1.3. *With the same hypotheses, let L/K be a finite extension, then the Galois closure $\widehat{Lk'}$ of Lk'/Kk' comes from an extension E_0/K of the same degree. In particular if Lk'/Kk' is finite Galois, then it comes from an extension E_0/K of the same degree.*

Demonstrations Let us embed $\widehat{Lk'}$ in a finite extension F Galois on K, with group $G = \mathrm{Gal}(F/K)$. By the proposition, the subgroup $H \subset G$ fixator of Lk'/K, is stabe under $s(\Gamma)$. But then the subgroup of G fixator of $\widehat{Lk'}/K$, equal to the intersection of the conjugates of H : $\bigcap_{g\in G} gHg^{-1}$, is also stable under Γ. □

Example 1.4. Consider $K = \mathbf{R}(T)$, $Kk' = \mathbf{C}(T)$, note $Z = \sqrt{T^2 + i}$ and $Z = \sqrt{T^2 - i}$, and fix a Galois closure $F = \mathbf{R}(Z, Z')/\mathbf{R}(T)$ of the extension $L =$

$\mathbf{R}(T)(Z)/\mathbf{R}(T)$. Consider the complex conjugation $\begin{cases} \tau : \mathbf{C}(T) \longrightarrow \mathbf{C}(T) \\ i \to -i \end{cases}$, and $\Gamma =< 1, \tau >$. Then among the 8 automorphisms of $F = \mathbf{R}(Z, Z')/\mathbf{R}(T)$, 4 extend τ of which 2 are of order two : $\begin{cases} \widetilde{\tau_1} : Z \longrightarrow Z' \\ Z' \to Z \end{cases}$, and $\begin{cases} \widetilde{\tau_2} : Z \longrightarrow -Z' \\ Z' \to -Z \end{cases}$. Thus both define sections of the exact sequence V.(Seq/Split): s_1 and s_2. Hence two subextensions $F_{0,1} \subset F$ and $F_{0,2} \subset F$. The corollary thus provides two possible regular descents of $\widehat{L\mathbf{C}} = L\mathbf{C}/\mathbf{C}(T)$, which occur as the subfield of $F_{0,1}$ (respectively $F_{0,2}$) fixed by $N =< 1, \sigma >$, with $\sigma : Z' \to -Z'$. In this case they actually coincide, because $E_0 = \mathbf{R}(T)(\sqrt{T^2+1})$ (exercice).



Counterexamples 1.5. The previous example provides two cautions with respect to the corollary :

- Lk'/Kk' finite Galois does not imply that L/K itself Galois. Consider $L/\mathbf{R}(X) = \mathbf{R}(\sqrt{T+i})/\mathbf{R}(X)$ and $L\mathbf{C} = \widehat{L\mathbf{C}}/\mathbf{C}(T)$.

- $\widehat{Lk'}/Kk'$ finite Galois does not imply that the regular extension E_0/K, provided by the corollary, be Galois over K. Consider this time $F = F\mathbf{C}/\mathbf{C}(T)$. Then neither of the two possible descents provided by the corollary : $F_{0,1}\mathbf{R}(Z + Z')/\mathbf{R}(T)$, nor $F_{0,2}\mathbf{R}(Z - Z')/\mathbf{R}(T)$, is Galois (exercice).

The following theorem is traditionally credited to Coombes & Harbater.

Here is a short demonstration due to Randriam[1]:

Proposition 1.6. *Let k be a field and k' a Galois extension with group $\Gamma = \mathrm{Gal}(k'/k)$. Let K be an extension of k (for example $k(T)$) and F/K a finite Galois extension containing Kk' with groups $G = \mathrm{Gal}(F/K)$ and $N = \mathrm{Gal}(F/Kk')$, such that the sequence V.*(Seq/Split) *has a splitting s (for example under the hypotheses of Proposition V.2.6) :*

Consider E/Kk' a Galois extension (for example if N is abelian) such that k is the field of moduli of E as mere extension of Kk'. Then L comes from a regular Galois *extension of K.*

Demonstrations Consider F a Galois closure of K containing E/Kk' and s a section of V.(Seq/Split). Thanks to Proposition 1.2 (applied with $L' = E$), it suffices to show that the fixing group $H \lhd N$ of $Kk' \subset E \subset F$ is stable under $s(\Gamma)$. Let τ be in Γ, then by the field of moduli assumption there exists x in N such that

$$s(\tau)Hs(\tau)^{-1} = xHx^{-1}$$

which is equal to H because here H is distinguished in N. □

2 Formulas

The notations are as in equation (1.2) of §I.1.1. For the sake of completeness, we also gave in the tabulars below the matrix forms of the squares of the linear forms ϕ_i:

$$\phi_i \otimes \phi_i : (x_1, x_2) \longrightarrow \phi_i(x_1).\phi_i(x_2).$$

The algebra considered are $\mathbf{F}_{q^m}[y]/y^l$ (q equals 2 or 4). But in our formulas of the two last sections where $q = 4$ and $m = 1$, we allowed ourselves to use the symbol y^i for the *linear form that takes a polynomial in y and returns the coefficient in y^i* (with value in $\mathbf{F}_4$).

2.1 $\mu_2(3, 2)$

The extension $\mathbf{F}_{2^3}/\mathbf{F}_2$ is generated by t, of minimum polynomial X^3+X+1. The algebra considered is

$$\mathcal{A}/\mathbf{F}_2 = \mathbf{F}_{2^3}[y]/y^2\,.$$

[1] A similar statement can also be found in Völklein th. 3.6 but with many more restrictions.

We express the linear forms ϕ_i in terms of the ordered basis of $\mathcal{A}^*/\mathbf{F}_2$:

$$c_{0,0}, c_{0,1}, c_{0,2}, c_{1,0}, c_{1,1}, c_{1,2}\ ,$$

where $c_{i,j}$ returns the coefficient in $y^i t^j$ of an element of $\mathcal{A}$ (the coefficients take values in $\mathbf{F}_2$).

i	ϕ_i	$\phi \otimes \phi$	w_i
0	$c_{0,0} + c_{0,1} + c_{0,2} + c_{1,0} + c_{1,1} + c_{1,2}$	$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$(t^2 + t)\, y + t$
1	$c_{0,0} + c_{1,0} + c_{1,2}$	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$	$ty + t^2$
2	$c_{1,1} + c_{1,2}$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$	$(t^2 + t + 1)\, y$
3	$c_{0,0} + c_{1,0} + c_{1,1} + c_{1,2}$	$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$	$t^2 y + t$
4	$c_{0,0} + c_{1,2}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	y
5	$c_{0,1} + c_{1,0} + c_{1,2}$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$	$(t^2 + t + 1)\, y + t^2$

6	$c_{0,0} + c_{0,1} + c_{1,2}$	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$	$t^2 y$
7	$c_{0,0} + c_{0,1} + c_{1,0} + c_{1,2}$	$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$	$y + t^2$
8	$c_{1,0} + c_{1,2}$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$	$t^2 y + t^2$
9	$c_{1,0} + c_{1,1} + c_{1,2}$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$	t
10	$c_{0,1} + c_{0,2} + c_{1,2}$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$	$(t^2 + 1)\, y$

11	$c_{0,1} + c_{0,2} + c_{1,0} + c_{1,1} + c_{1,2}$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$ty + t$
12	$c_{0,0} + c_{0,2}$	$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$(t^2 + t + 1)\, y + t^2 + 1$
13	$c_{0,0} + c_{0,1} + c_{0,2}$	$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$y + t + 1$
14	$c_{0,0} + c_{0,1}$	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$ty + t^2 + t + 1$
15	$c_{0,2} + c_{1,1} + c_{1,2}$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$	$(t^2 + t + 1)\, y$

2.2 $\mu_4(1,4)$

The extension $\mathbf{F}_{2^2}/\mathbf{F}_2$ is generated by a, of minimum polynomial X^2+X+1. The algebra considered is

$$\mathcal{A}/\mathbf{F}_4 = \mathbf{F}_4[y]/y^4.$$

i	ϕ_i	$\phi_i \otimes \phi_i$	w_i
0	1	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$ay^3 + ay^2 + 1$
1	$y^2 + ay + 1$	$\begin{bmatrix} 1 & a & 1 & 0 \\ a & a+1 & a & 0 \\ 1 & a & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$ay^3 + y^2 + y$
2	$y^2 + y + 1$	$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$ay^2 + y$
3	$ay^2 + y + 1$	$\begin{bmatrix} 1 & 1 & a & 0 \\ 1 & 1 & a & 0 \\ a & a & a+1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$y^3 + ay$
4	$ay^2 + 1$	$\begin{bmatrix} 1 & 0 & a & 0 \\ 0 & 0 & 0 & 0 \\ a & 0 & a+1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$ay^3 + y^2 + ay$
5	$(a+1)\,y^3 + ay^2 + y$	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & a & a+1 \\ 0 & a & a+1 & 1 \\ 0 & a+1 & 1 & a \end{bmatrix}$	y^3
6	$ay^3 + y^2 + (a+1)\,y + 1$	$\begin{bmatrix} 1 & a+1 & 1 & a \\ a+1 & a & a+1 & 1 \\ 1 & a+1 & 1 & a \\ a & 1 & a & a+1 \end{bmatrix}$	$(a+1)\,y^3$

2.3 $\mu_4(1,5)$

The extension $\mathbf{F}_4/\mathbf{F}_2$ is generated by t, of minimum polynomial X^2+X+1. The algebra considered is

$$\mathcal{A}/\mathbf{F}_4 = \mathbf{F}_4[y]/y^5\,.$$

i	ϕ_i	$\phi_i \otimes \phi_i$	w_i
0	c_0	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$ay^4 + ay^2 + 1$
1	$c_0 + c_1 + (a+1)c_2$	$\begin{bmatrix} 1 & 1 & a+1 & 0 & 0 \\ 1 & 1 & a+1 & 0 & 0 \\ a+1 & a+1 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$(a+1)\,y^4 + ay^3 + (a+1)\,y^2 + (a+1)\,y$
2	$c_0 + (a+1)c_1 + (a+1)c_2$	$\begin{bmatrix} 1 & a+1 & a+1 & 0 & 0 \\ a+1 & a & a & 0 & 0 \\ a+1 & a & a & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$(a+1)\,y^4 + (a+1)\,y^3 + y^2 + (a+1)\,y$
3	$c_1 + a.c_2$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & a & 0 & 0 \\ 0 & a & a+1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$(a+1)\,y^3 + ay$
4	c_2	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$y^4 + (a+1)\,y^2 + y$

5	$c_0 + (a+1)c_2 + c_3$	$\begin{bmatrix} 1 & 0 & a+1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ a+1 & 0 & a & a+1 & 0 \\ 1 & 0 & a+1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	y^3
6	$c_2 + a.c_3$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & a & 0 \\ 0 & 0 & a & a+1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$y^4 + ay^3$
7	$c_0 + (a+1)c_1 + a.c_2 + (a+1)c_3 + a.c_4$	$\begin{bmatrix} 1 & a+1 & a & a+1 & a \\ a+1 & a & 1 & a & 1 \\ a & 1 & a+1 & 1 & a+1 \\ a+1 & a & 1 & a & 1 \\ a & 1 & a+1 & 1 & a+1 \end{bmatrix}$	$(a+1)\,y^4$
8	$c_0 + (a+1)c_2 + c_3 + a.c_4$	$\begin{bmatrix} 1 & 0 & a+1 & 1 & a \\ 0 & 0 & 0 & 0 & 0 \\ a+1 & 0 & a & a+1 & 1 \\ 1 & 0 & a+1 & 1 & a \\ a & 0 & 1 & a & a+1 \end{bmatrix}$	ay^4
9	$c_0 + c_1 + c_4$	$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$	$(a+1)\,y^4$

Bibliography

[AM] B. Angles & C. Maire, A Note on Tamely Ramified Towers of Global Function Fields. Finite Fields and Their Applications, 2002.

[Ar] N. Arnaud, Évaluation dérivée, multiplication dans les corps finis et codes correcteurs. PhD thesis, Université de Marseille - IML, 2006.

[Bal$_1$] S. Ballet, Curves with many points and multiplication complexity in any extension of $\mathbf{F}_q$. Finite fields and their applications, 1999

[Bal$_2$] Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of $\mathbf{F}_q$. Finite fields and their applications, 2003.

[BB] A. Bassa, P. Beelen, The Hasse-Witt invariant in some towers of function fields over finite fields. Bull. Brazilian Math society, 2010.

[BBCM] A. Bernardi, J. Brachat, P. Comon and B. Mourrain, Tensor decomposition, moment matrices and applications. J. Symbolic Comput., 2013.

[BBGS] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, Towers of Function Fields over Non-prime Finite Fields. Mosc. Math. J. , 2015.

[BBR] S. Ballet, D. le Brigand, R. Rolland, On an application of the definition field descent of a tower of function fields, AGCT 2005, 2009.

[BBT] S. Ballet, A. Bonnecaze and M. Tukumuli, On the construction of Chudnovsky-type algorithms for multiplication in large extensions of finite fields. Journal of algebra and its Applications, 2016.

[Be] Laurent Berger, Quand Google m'aide à écrire mes articles. Images des Mathématiques, CNRS, 2009.

[Bir] Bryan Birch, Noncongruence Subgroups, Covers and Drawings. In The Grothendieck Theory of Dessins d'Enfants, London Math. Soc. lecture notes 200, 1994.

[BL] C. Birkenhake, H. Lange, Complex Abelian Varieties. Grundlehren Math. Wiss. , Springer, 2004.

[BCP] S. Ballet, J. Chaumine & J. Pieltant, Shimura Modular Curves and asymptotic symmetric tensor rank of multiplication in any finite field. CAI 2013.

[BP] S. Ballet and J. Pieltant, On the tensor rank of multiplication in any extension of $\mathbf{F}_2$. Journal of Complexity, 2011.

[BP_2] S. Ballet and J. Pieltant, Tower of algebraic function fields with maximal Hasse-Witt invariant and tensor rank of multiplication in any extension of $\mathbf{F}_2$ and $\mathbf{F}_3$. Accepted in J. Pure Appl. Algebra, 2017.

[BR] S. Ballet, R. Rolland, Multiplication algorithm in a finite field and tensor rank of the multiplication. Journal of Algebra, 2004.

[BR_2] S. Ballet, R. Rolland, Families of curves over any finite field attaining the generalized Drinfeld-Vladut bound. Pub. Math. Besançon, 2011.

[BDEZ] R. Barbulescu, Jérémie Detrey, Nicolas Estibals and Paul Zimmermann, Finding optimal formulae for bilinear maps. WAIFI 2012.

[BPRS] S. Ballet, J. Pieltant, M. Rambaud, J. Sijsling, On some bounds for symmetric tensor rank of multiplication in finite fields. Contemp. Math. 2017

[BRR] S. Ballet, C. Ritzenthaler, R. Rolland, On the existence of dimension zero divisors in algebraic function fields defined over $\mathbf{F}_q$. Acta Arithmetica, 2010.

[Brou] M. Broué, Generalities on modules categories. Lecture notes https://webusers.imj-prg.fr/~michel.broue/1genMod.pdf, 2008.

[BSSVY] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight, D. Yasaki, A database of genus 2 curves over the rational numbers. LMS J. Comput. Math., 2016.

[Car] Henri Carayol, Sur la mauvaise réduction des courbes de Shimura. Compositio Mathematica, 1986.

[CCX] I. Cascudo, R. Cramer, and Chaoping Xing. The torsion-limit for algebraic function fields and its application to arithmetic secret sharing. CRYPTO 2011.

[CCX_2] I. Cascudo, R. Cramer, and Chaoping Xing. Torsion limits and Riemann-Roch systems for function fields and applications. IEEE Trans. Inform. Theory, 2014.

[CCXY] I. Cascudo, R. Cramer, C. Xing, and A. Yang. Asymptotic bound for multiplication complexity in the extensions of small finite fields. IEEE Trans. Inform. Theory, 2012.

[Ch^2] D. V. Chudnovsky and G. V. Chudnovsky, Algebraic complexities and algebraic curves over finite fields. Journal of Complexity, 1988.

[CH] K. Coombes and D. Harbater. Hurwitz families and arithmetic galois groups. Duke Math. J. , 1985.

[CHN] M. Cenk and A. Hasan and C. Negre, Improved three-way split formulas for binary polynomial and Toeplitz matrix vector products. IEEE Trans. Comput. , 2013.

[Cl] Pete Clark, PhD Thesis. Harvard, 2003.

[Cl$_1$] Pete Clark, Lecture 10: Quaternionic Moduli. http://math.uga.edu/~pete/SC10-Moduli.pdf, 2006.

[CMSV] E. Costa, N. Mascot, J. Sijsling and J. Voight, Rigorous computation of the endomorphism ring of a Jacobian. https://arxiv.org/abs/1705.09248, 2017

[CO$_0$] M. Cenk and F. Özbudak, Improved polynomial multiplication formulas over $\mathbf{F}_2$ using CRT. IEEE Trans. Comput. - brief contributions, 2009

[CO$_1$] M. Cenk and F. Özbudak, On multiplication in finite fields. Journal of Complexity, 2010.

[CO$_2$] M. Cenk and F. Özbudak, Multiplication of polynomials modulo x^n. Theoretical Computer Science, 2011.

[Cr] J. E. Cremona, Algorithms for modular elliptic curves (second edition). Cambridge university press, 1997.

[Dèb$_1$] P. Dèbes, Méthodes topologiques et analytiques en théorie inverse de Galois: Théorème d'existence de Riemann. In SMF Séminaires et Congrès 5, 2001.

[Dèb$_2$] P. Dèbes, Arithmétique des revêtements de la droite (notes de cours de M2 en ligne)

[DèbDo] P. Dèbes, J.-C. Douai, Algebraic covers : field of moduli versus field of definition. Ann. Sci. ENS 1997.

[DE] P. Dèbes, M. Emsalem, On fields of moduli of curves. J. Algebra, 1999.

[Del] P. Deligne, Travaux de Shimura. Séminaire Bourbaki 1969.

[DemDo] L. Dembélé and S. Donnelly, Computing Hilbert modular forms over fields with nontrivial class group. ANTS 2008.

[DH] B. Deconinck and M. van Hoeij, Computing Riemann Matrices of Algebraic Curves. Physica D Vol. 152-153, 2001.

[DN] K. Doi and H. Naganuma. On the algebraic curves uniformized by arithmetical automorphic functions, Ann. of Math. , 1967.

[Don] S. Donaldson, Riemann surfaces. Oxford GTM, 2011.

[DS] Fred Diamond and Jerry Shurman, A First Course in Modular Forms. Springer, 2004.

[Duc] V. Ducet, Construction of algebraic curves with many rational points over finite fields. PhD thesis, Université d'Aix-Marseille - IML, 2013.

[DM] I. Duursma & K.H. Mak, On lower bounds for the Ihara constants A(2) and A(3). Compos. Math. , 2013.

[DV] L. Dembélé & J. Voight, Explicit Methods for Hilbert Modular forms. In Elliptic Curves, Hilbert Modular Forms and Galois Deformations, CRM Barcelona 2013.

[El_1] N.D. Elkies, Explicit modular towers. In Tamer Basar and Alexander Vardy, editors, Proceedings of the Thirty-fifth annual Allerton conference on communication, control and computing, 1997.

[Elk_2] N.D. Elkies, Shimura curves computations, ANTS 1998.

[Elk06] N.D. Elkies, Shimura curves arising from the (2,3,7) triangle group, ANTS 2006.

[Ga] S.D. Galbraith, Equations For Modular Curves. PhD thesis, Oxford, 1996.

[Gek] E.-U. Gekeler. Invariants of Some Algebraic Curves Related to Drinfeld modular curves. J. Number Theory 90 (2001), no. 1, 166–183.

[Gek_2] E.-U. Gekeler. Asymptotically Optimal Towers of Curves over Finite Fields. In Algebra, Arithmetic and Geometry with Applications, Springer 2002.

[GS] A. Garcia and H. Stitchtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. Invent. Math. , 1995.

[GSR] A. Garcia, H. Stitchtenoth and Hans-Georg Ruck. On tame towers over finite fields. J. Crelle, 2003.

[dGr] H. de Groote, Characterization of division algebras of minimal rank and the structure of their algorithm varieties. SIAM J. Comput., 1983.

[GV] M. Greenberg, J. Voight, Computing systems of Hecke eigenvalues associated to Hilbert modular forms. Math. Comp., 2011.

[Hal] E. Hallouin, Computation of a cover of Shimura curves using a Hurwitz space. J. Algebra, 2009.

[Has] T. Hasegawa, An Explicit Shimura Tower of Function Fields over a Number Field: An Application of Takeuchi's List. preprint, 2017.

[Hes] Computing Riemann-Roch spaces in algebraic function fields and related topics. J. Symbolic Comput., 2001.

[HS] L.L. Hall-Seelig, New lower bounds for the Ihara function A(q) for small primes. J. Number Theory, 2013.

[Iha$_1$] Y. Ihara, Congruence relations and Shimūra curves. In Automorphic forms, representations and L-functions. Proc. Corvallis, 1979.

[Iha$_2$] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields. J. Math. Sci. Univ. Tokyo, 1981.

[JS] G. Jones, D. Singerman, Complex functions. Cambridge Univ. Press, 1987.

[Kah] Bruno Kahn, Fonctions zêta et L de variétés et de motifs. arxiv 1512.09250, 2016.

[Kat] S. Katok, Fuchsian Groups. University of Chicago Press, 1992.

[Leb] P. Lebacque, Quelques résultats effectifs concernant les invariants de Tsfasman-Vladut. Ann. Inst. Fourier, 2015.

[Lam] T. Y. Lam, Lectures on modules and rings. Springer, 1999.

[Lan] S. Lang, Introduction to algebraic and abelian functions. Springer, 1995.

[LMFDB] The LMFDB Collaboration, The L-functions and Modular Forms Database, http://www.lmfdb.org, 2013.

[LV] B. Linowitz & J. Voight, Small Isospectral And Nonisometric Orbifolds Of Dimension 2 And 3. Math. Z., 2015.

[LM] W. Li, H. Maharaj, Coverings of Curves with Asymptotically many Rational Points. J. Number theory, 2002.

[LZ] P. Lebacque and A. Zykin, Asymptotic methods in number theory and algebraic geometry. Publ. Math. Besançon, 2011.

[M] D. Mumford, Abelian varieties. Tata institute

[M4rie] M. Albrecht, The M4rie library for dense linear algebra over small fields with even characteristic. Arxiv 1111.6900, 2011.

[Ma] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I : the user language. J. Symbolic Comput., 1997.

[Mag] W. Magnus, Non Euclidean Tesselations and their Groups. Academic Press, New York 1974.

[Maz] B. Mazur, Open problems regarding rational points. In Galois representations in arithmetic algebraic geometry, London Math. Soc. lecture notes 254, 1997.

[MilJV] James S. Milne, Jacobian varieties. In Arithmetic geometry (Storrs, Conn., 1984), 1986.

[MilClo] J.S. Milne, Canonical Models of (Mixed) Shimura Varieties and Automorphic Vector Bundles, in Automorphic forms, Shimura varieties, and L-functions, 1988.

[MilDe] J.S. Milne, Descent for Shimura Varieties. Michigan Math. J. , 46 (1999), pp. 203–208;

[MilAG] J.S. Milne, Algebraic geometry. online notes.

[MilAV] J.S. Milne, Abelian Varieties. In Arithmetic Geometry (Proc. Conference on Arithmetic Geometry, Storrs, online edited version), 1986.

[MilJV] J.S. Milne, Jacobian Varieties. In Arithmetic Geometry (Proc. Conference on Arithmetic Geometry, Storrs, online edited version), 1986.

[MilSV] J.S. Milne, Introduction to Shimura varieties. online notes, 2004.

[Miy] T. Miyake, Modular Forms. Springer, 1989.

[Mo] C.J. Moreno, Algebraic Curves on Finite Fields. Cambridge tracts in maths, 1993.

[Mon] P.L. Montgomery, Five, six and seven-term Karatsuba-like formulae. IEEE Trans. Comput. , 2005.

[Moo] B. Moonen, Models of Shimura varieties in mixed characteristics. In Galois representations in arithmetic algebraic geometry, Cambridge Univ. Press, 1998.

[Mor] Y. Morita. Reduction modulo $\mathfrak{P}$ of Shimura curves. Hokkaido Mathematical Journal, 1981.

[NIST] NIST, FIPS 186-4, page 88, 2013.

[Oce] I. Oceledets, Optimal Karatsuba-like formulae for certain bilinear forms in GF(2). Linear Algebra and its Applications, 2008.

[Ogg] A.P. Ogg, Real Points on Shimura Curves. In Volume 35 of Progress in Mathematics, 1983.

[PR] J. Pieltant and H. Randriam, New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields. Mathematics of Computation, 2015.

[Ra] M. Rambaud, Finding optimal Chudnovsky and Chudnovsky multiplication algorithms. WAIFI 2014, LNCS 2015.

[Ran_0] H. Randriam, Hecke operators with odd determinant and binary frameproof codes beyond the probabilistic bound? IEEE Information Theory Workshop (ITW) Dublin, 2010.

[Ran_1] H. Randriam, Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. Journal of Complexity, 2012.

[Ran$_2$] H. Randriam, Diviseurs de la forme 2D-G sans sections et rang de la multiplication dans les corps finis. preprint, 2012.

[Rot] V. Rotger, Thesis. Universitat de Barcelona, 2002.

[Sa] SageMath, the Sage Mathematics Software System (Version 6.3), The Sage Developers. `http://www.sagemath.org`, 2014.

[Se$_0$] J.-P. Serre, Corps Locaux, Hermann 1968

[Se$_1$] J.-P. Serre, Galois Cohomology, Springer monographs in maths, 1996.

[Se$_2$] J.-P. Serre, Topics in Galois Theory. Research Notes in Mathematics, 1997.

[Sh$_0$] G. Shimura, On analytic families of abelian varieties and automorphic functions. Ann. of Math. , 1967.

[Sh$_1$] G. Shimura, Construction of class fields and zeta functions. Ann. of Math. 1967.

[Sh$_2$] G. Shimura, On canonical models of arithmetic quotients of bounded symmetric domains. Ann. of Math. , 1970.

[Sh$_3$] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Princeton Univ. Press, 1971.

[Sh$_4$] G. Shimura, Abelian Varieties with Complex Multiplication and Modular Functions. Princeton Univ. Press, 1998.

[Shih] K. Shih, Conjugations of Arithmetic Automorphic Function Fields. Invent. Math. 1978.

[Sho] A. Shokhrollahi, Optimal algorithms for multiplication in certain finite fields using algebraic curves. SIAM J. Comput. , 1992.

[Sho] M. A. Shokrollahi, Counting prime divisors on elliptic curves and multiplication in finite fields. In Coding theory and Cryptography (David Joyner ed.), 2000.

[Sij$_1$] J. Sijsling, Equations for arithmetic pointed tori. PhD thesis, Utrecht University, 2010.

[Sij$_2$] J. Sijsling, Magma programs for arithmetic pointed tori. Available at: `https://sites.google.com/site/sijsling/programs`, 2010.

[Sij$_3$] J. Sijsling, Canonical models of arithmetic $(1; e)$-curves. Math. Z. , 2013.

[Sil] J. Silverman, The Arithmetic of Elliptic Curves (2nd edition). Springer, 2008.

[Sti] H. Stichtenoth, Algebraic Function Fields and Codes (2nd edition). Springer, 2008.

[STV] I. Shparlinski, M. Tsfasman & S. Vladut. Curves with many points and multiplication in finite fields. In AGCT3, Springer LNM 1518, 1992.

[SV_1] J. Sijsling, J. Voight, On computing Belyi maps. Pub. Univ. Franche Compté, 2014.

[SV_2] J. Sijsling, J. Voight, On explicit descent of marked curves and maps. Res. Number Theory, 2016.

[Ste] W. Stein, Modular Forms, a Computational Approach. AMS, 2006.

[Svy] S. Covanov, Improved method to find optimal formulae for bilinear maps. preprint, 2017.

[Sza] T. Szamuely, Galois groups and fundamental groups. Cambridge, 2009.

[Tak] K. Takeuchi, Commensurability classes of arithmetic triangle groups. J. Math. Sci. Univ. Tokyo 1977

[Vig] Marie-France Vignéras, Arithmétique des algèbres de quaternions. LNM n°800, 1979.

[Vig_2] Marie-France Vignéras, Variétés Riemanniennes Isospectrales et non Isométriques. Ann. Math. 1980.

[Voi_0] J. Voight, Three lectures on Shimura curves, 2006.

[Voi_1] J. Voight, PhD thesis, 2006.

[Voi_2] J. Voight, Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups, ANTS 2006.

[Voi_3] J. Voight, Computing fundamental domains for Fuchsian groups. J. Théor. Nombres Bordeaux, 2009.

[Voi_4] J. Voight, Shimura curves of genus at most two. Math. Comp., 2009.

[Voi_5] J. Voight, Quaternion algebras. Book, v0.9.2.

[KVMSV] M. Klug, M. Musty, S. Schiavone and J. Voight, Numerical computation of three-point covers of the projective line. LMS J. Comput. Math. 2014.

[Wi] Shmuel Winograd, On multiplication in algebraic extension fields. Theoret. Comput. Sci. , 1979.

[Wol] J. Wolfart, The obvious part of Belyi's theorem and Riemann surfaces with many automorphisms, in Geometric Galois actions vol.1.

[Ya] Y. Yang, Defining equations of modular curves. Adv. Math. , 2006.

[Zi] T. Zink, Degeneration of Shimura surfaces and a problem in coding theory. In Proc. 19th Fundam. Comput. Theory, 1985.