Rappels maths pour crypto

David A. Madore

28 novembre 2013

Git : 037edf8 Thu Nov 21 16:35:30 2013 +0100

1 Entiers

1.1 L'anneau des entiers

On appelle $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ l'ensemble des entiers relatifs. Il a pour sous-ensemble $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ l'ensemble des entiers naturels (ou positifs).

Sur $\mathbb{Z}$ on a les opérations : $+$ (addition) et $\times$ (multiplication) ; et les éléments remarquables : 0, 1. Ces données vérifient les propriétés suivantes :

1. Associativité de l'addition : $x + (y + z) = (x + y) + z$
2. Neutralité de zéro pour l'addition : $0 + x = x + 0 = x$
3. Existence d'opposés (=symétriques pour l'addition) : (pour chaque x, il existe un élément noté $-x$ tel que) $x + (-x) = (-x) + x = 0$
4. Commutativité de l'addition : $y + x = x + y$
5. Distributivité de la multiplication sur l'addition : $x(y + z) = xy + xz$ et $(x + y)z = xz + yz$
6. Associativité de la multiplication : $x(yz) = (xy)z$
7. Neutralité de un pour la multiplication : $1x = x1 = x$
8. Commutativité de la multiplication : $yx = xy$

Les trois premières propriétés traduisent le fait que $\mathbb{Z}$ est un *groupe* pour l'addition ; les quatre premières, que $\mathbb{Z}$ est un *groupe abélien* pour l'addition ; les

sept premières propriétés traduisent le fait que $\mathbb{Z}$ est un *anneau* ; les huit propriétés réunies traduisent le fait que $\mathbb{Z}$ est un **anneau commutatif**.

Mieux : c'est un *anneau intègre* : si $uv = 0$ alors $u = 0$ ou $v = 0$ (la réciproque est vraie dans n'importe quel anneau : $0x = x0 = 0$).

Éléments inversibles : un **inversible** ou une **unité** (dans un anneau commutatif) est un élément x tel qu'il existe y tel que $xy = 1$. Dans $\mathbb{Z}$, les inversibles sont 1 et -1.

On a aussi sur $\mathbb{Z}$ une relation d'ordre : c'est-à-dire une relation réflexive (on a toujours $x \leq x$), antisymétrique (si $x \leq y$ et $y \leq x$ alors $x = y$) et transitive (si $x \leq y$ et $y \leq z$ alors $x \leq z$).

1.2 Écriture b-adique

Si $b \geq 2$ est un entier naturel, tout entier naturel A s'écrit de façon unique $A = \sum_{i=0}^{+\infty} a_i b^i$ avec $0 \leq a_i < b$ entiers naturels « presque tous nuls » (c'est-à-dire nuls sauf un nombre fini : donc la somme peut en fait s'écrire $A = \sum_{i=0}^{n-1} a_i b^i$). Les a_i s'appellent les *chiffres* de cette écriture b-adique, a_0 s'appelant le chiffre des *unités* ou chiffre *de poids faible*.

Écriture usuelle : $b = 10$. Informatique : $b = 2$ (les chiffres portent alors le nom de *bits*). Un nombre « de n bits » signifie : inférieur à 2^n.

Multiplier par b revient à décaler tous les chiffres d'un cran vers le poids fort (et mettre un 0 comme nouveau chiffre de poids faible).

1.3 Remarques sur la complexité des opérations

Addition de nombres de n bits : algorithme naïf en $O(n)$.

Multiplication : plus compliqué.

Algorithme naïf en $O(n^2)$ (appris à l'école primaire).

Multiplication de Karatsuba : utilise récursivement l'identité $(a_1 w + a_0)(b_1 w + b_0) = a_1 b_1 w^2 + [(a_1 + a_0)(b_1 + b_0) - a_1 b_1 - a_0 b_0]w + a_0 b_0$ (avec a_0, a_1 les moitiés de poids respectivement faible et fort des chiffres du nombre $A = a_1 w + a_0$ à multiplier et b_0, b_1 les moitiés de poids faible et fort du nombre $B = b_1 w + b_0$; ici, w vaut $2^{n/2}$ si on travaille en binaire sur des nombres de n bits), pour une complexité en $O(n^{\frac{\log 3}{\log 2}})$ (soit $O(n^{1.58\cdots})$). Facile à implémenter.

Multiplication de Strassen : par transformée de Fourier rapide, complexité en $O(n \log^2 n)$, difficile à implémenter. Amélioration de Schönhage : $O(n \log n \log\log n)$ — complètement théorique.

1.4 Divisiblité (exacte)

Si a et b sont deux entiers, on dit que b divise a, et on note $b|a$, lorsqu'il existe $q \in \mathbb{Z}$ tel que $a = bq$.

Cette relation est réflexive (on a $a|a$ pour tout a) et transitive (si $b|a$ et $c|b$ alors $c|a$). Elle n'est pas tout à fait antisymétrique, mais c'est vrai dans les entiers naturels : si a et b sont des entiers naturels tels que $b|a$ et $a|b$ alors $b = a$ (dans les entiers relatifs, on peut aussi avoir $b = -a$).

Note : Les entiers 1 et -1 divisent tous les entiers. L'entier 0 est divisible par tous les entiers.

1.5 Nombres premiers

Un **nombre premier** p est un entier (par convention : positif) divisible seulement par 1, -1, lui-même et son opposé ; mais par convention, 1 et -1 (et 0...) ne sont pas premiers.

Les premiers nombres premiers sont donc : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97...

Sur leur répartition :

Il y en a une infinité (Euclide).

Pour tout $x > 1$, il y a toujours un nombre premier p tel que $x < p < 2x$ (Čebyšëv : « postulat de Bertrand », démontré en 1850). De façon équivalente : si p est premier, alors le nombre premier qui le suit immédiatement est $< 2p$.

Le nombre $\pi(x)$ de nombres premiers $\leq x$ est équivalent à $\frac{x}{\ln x}$ lorsque $x \to +\infty$ (Hadamard & de la Vallée Poussin : « théorème des nombres premiers », démontré en 1896). Moralement : la probabilité qu'un nombre de n bits aléatoire soit premier est environ $\frac{1}{n \ln 2}$.

Beaucoup de questions ouvertes. Par exemple : Conjecture des nombres premiers jumeaux : existe-t-il une infinité de nombres premiers p tels que $p + 2$ soit aussi premier (tels que 3, 5, 11, 17, 29, 41, 59, 71...) ?

Lemme de Gauß : pour p premier, si p divise ab alors p divise a ou p divise b.

1.6 Décomposition en facteurs premiers

Pour tout entier n *non nul*, il existe une écriture *unique* (à l'ordre près) de n comme produit d'une *unité* (1 ou -1) et de nombres premiers : en regroupant les facteurs premiers p,

$$n = u\, 2^{v_2(n)}\, 3^{v_3(n)} \cdots p^{v_p(n)} \cdots$$

Ici, $v_p(n)$ (un entier naturel) est l'exposant de la plus grande puissance de p qui divise n : on l'appelle *valuation p-adique* de n. Presque tous ces nombres sont nuls, ce qui permet de donner un sens au produit infini. Dire que $b|a$ signifie $v_p(b) \leq v_p(a)$ pour tout p.

Quant à u, c'est simplement le signe de n.

Exemple : $7920 = 2^4 \times 3^2 \times 5 \times 11$, c'est-à-dire que $v_2(7920) = 4$, $v_3(7920) = 2$, $v_5(7920) = 1$, $v_7(7920) = 0$, $v_{11}(7920) = 1$, et $v_p(7920) = 0$ pour n'importe quel nombre premier $p \geq 13$.

1.7 Remarques sur la complexité

Toujours pour des nombres de n bits.

Tests de primalité : *polynomiaux*. Un test polynomial *déterministe* est connu depuis seulement récemment (Agrawal-Kayal-Saxena), démontrablement en $O(n^{12})$, sans doute meilleur ($O(n^3)$?). En pratique, des tests probabilistes sont suffisants et plus efficaces (p.e., Miller-Rabin « pratiquement » en $O(n^2)$) éventuellement complétés par des certificats de primalité (p.e., test d'Atkin).

Algorithmes de factorisation : *lents*. Font appel à des résultats difficiles de théorie algébrique et analytique des nombres. La meilleure méthode connue (« méthode du crible général de corps de nombres ») a une complexité « attendue » (et heuristique) en $O(e^{n^{1/3}\,(\log n)^{2/3}\,(\text{cte}+o(1))})$ (avec cte ≈ 2).

On ne pourra donc pas envisager d'utiliser la décomposition en facteurs premiers pour calculer les pgcd.

1.8 Valuation p-adique

Si n est un entier et p un nombre premier, $v_p(n)$ est l'exposant de la plus grande puissance de p qui divise n. Si a/b est un rationnel, on pose $v_p(a/b) = v_p(a) - v_p(b)$ (ne dépend pas de la représentation a/b choisie). Par convention, $v_p(0) = +\infty$.

Quelle est la valuation 2-adique de 192 ? 3-adique ? 5-adique ? Quelles sont les valuations p-adiques de $-\frac{24}{11}$, pour tous les p possibles ?

Propriétés de v_p : produit (cf. lemme de Gauß) : on a $v_p(xy) = v_p(x) + v_p(y)$; inégalité sur la somme : on a $v_p(x + y) \geq \min(v_p(x), v_p(y))$ avec égalité si $v_p(x) \neq v_p(y)$. Dire que $x \in \mathbb{Q}$ est entier signifie exactement $v_p(x) \geq 0$ pour tout p.

Remarque : calculer $v_p(n)$, pour un n donné et un p premier donné, est facile. Ce qui est difficile dans la décomposition en facteurs premiers, c'est de trouver

tous les p tels que $v_p(n) > 0$ (ou en fait, en trouver *un*).

1.9 Division euclidienne

Si a est un entier relatif et b un entier naturel *non nul*, il existe un unique couple (q, r) tel que :

- q est un entier relatif,
- r est un entier naturel tel que $0 \leq r < b$, et
- $a = bq + r$.

On dit que q est le *quotient* et r le *reste* de la **division euclidienne** de a par b. (On appelle aussi a le *dividende* et b le *diviseur*.)

Si $b \geq 2$, dans l'écriture b-adique de a, le dernier chiffre (a_0 avec les notations précédentes) est égal au reste r de la division euclidienne de a par b.

Dire que $r = 0$ signifie exactement que b divise a (la division euclidienne est alors *exacte*).

Exemple : le reste de la division euclidienne de a (un entier quelconque) par 2 vaut : 0 lorsque a est *pair*, et 1 lorsque a est *impair* ; ce sont les seules deux valeurs possibles.

Algorithme naïf : (celui de l'école primaire) en $O(n^2)$.

Algorithme sophistiqué : en $O(n \log n \log\log n)$ avec Schönhage-Strassen + méthode de Newton (+ subtilités).

Méthode de Newton : on inverse b (en précision fixe) en itérant $x \leftarrow 2x - bx^2$.

Souvent implémentée **en matériel** pour certaines tailles d'entiers (p. ex., division entière de 128 bits par 64 bits).

1.10 PGCD

Si $m_1, \ldots, m_\ell$ sont des entiers, on dit qu'un entier c est un **plus grand commun diviseur** (en abrégé : *pgcd*) des m_i lorsque :

- c divise chaque m_i (i.e, c est un diviseur commun des m_i), et
- tout entier d qui divise chaque m_i (i.e., tout diviseur commun des m_i) divise aussi c.

En principe, le pgcd des m_i est défini au signe près (si c est un pgcd des m_i alors $-c$ l'est aussi) : en imposant qu'il soit positif il devient unique et on parle alors *du* pgcd des m_i.

Exemple : le pgcd de 6 et 10 est 2 ; le pgcd de 6, 10 et 15 est 1.

Le pgcd *existe* toujours : on peut le trouver à partir de la décomposition en facteurs premiers par

$$v_p(\mathrm{pgcd}(m_1, \ldots, m_\ell)) = \min(v_p(m_1), \ldots, v_p(m_\ell))$$

(pour tout nombre premier p). Mais ce n'est pas une méthode efficace de calcul !

Notation : Parfois $m_1 \wedge \cdots \wedge m_\ell$, mais cette notation peut être utilisée pour d'autres sortes de bornes inf. Certains textes anglais utilisent (m, m') pour le pgcd de deux entiers. La notation $\mathrm{pgcd}(\cdots)$ est évidemment la plus claire.

Quelques propriétés :
- le pgcd d'un seul entier m est $|m|$ (et le pgcd de zéro entiers est 0),
- le pgcd est associatif (par exemple $\mathrm{pgcd}(m_1, m_2, m_3) = \mathrm{pgcd}(\mathrm{pgcd}(m_1, m_2), m_3)$),
- le produit est distributif sur le pgcd ($\mathrm{pgcd}(cm_1, \ldots, cm_\ell) = |c|\ \mathrm{pgcd}(m_1, \ldots, m_\ell)$),
- on peut toujours effacer des 0 d'un pgcd,
- dès qu'un des entiers est 1 ou -1, le pgcd est 1,
- le pgcd d'une famille infinie se définit sans difficulté.

1.11 Entiers premiers entre eux

Lorsque $\mathrm{pgcd}(m_1, \ldots, m_\ell) = 1$, on dit que les m_i sont **premiers entre eux** *dans leur ensemble*. Cela signifie qu'il n'existe aucun nombre premier (ou : aucun nombre autre que ± 1) qui divise tous les m_i à la fois.

Lorsque $\mathrm{pgcd}(m_i, m_j) = 1$ pour tous $i \neq j$, on dit que les m_i sont premiers entre eux *deux à deux*.

Bien entendu, pour seulement deux nombres, ces définitions coïncident, et on dit simplement qu'ils sont premiers entre eux.

Exemple : $6, 10, 15$ sont premiers entre eux dans leur ensemble, mais pas deux à deux.

Lemme de Gauß amélioré : Si m et n sont premiers entre eux, être multiple de m et de n équivaut à être multiple de mn.

Dirichlet : La probabilité pour que deux entiers « tirés au hasard » soient premiers entre eux est $\frac{6}{\pi^2}$ (c'est-à-dire que la probabilité que deux entiers tirés au hasard entre 0 et $N-1$ soient premiers entre eux tend vers $\frac{6}{\pi^2}$ quand $N \to +\infty$).

1.12 PPCM

Définition analogue au pgcd (un ppcm de $m_1, \ldots, m_\ell$ est un multiple commun à tous les m_i qui divise n'importe quel autre multiple commun ; par convention, on prend celui qui est positif). Exemple : le ppcm de 6 et 10 est 30 ; le ppcm de 6, 10 et 15 est aussi 30. Lien avec la DFP (pour un nombre fini d'entiers) : $v_p(\mathrm{ppcm}(m_1, \ldots, m_\ell)) = \max(v_p(m_1), \ldots, v_p(m_\ell))$. Le ppcm d'une famille infinie d'entiers est défini, mais parfois surprenant (quel est le ppcm de tous les nombres premiers ?).

Remarque : pour deux nombres, on a $\mathrm{ppcm}(m, m') \times \mathrm{pgcd}(m, m') = |mm'|$ (ceci découle, en comparant les décompositions en facteurs premiers, du fait que $\min(u, v) + \max(u, v) = u + v$ pour tous $u, v \in \mathbb{N}$).

1.13 Relation de Bézout

Si a et b sont premiers entre eux (c'est-à-dire $\mathrm{pgcd}(a, b) = 1$) il existe des entiers u et v tels que $au + bv = 1$ (on verra pourquoi plus loin) : on appelle cette égalité une **relation de Bézout** [1] entre a et b.

Réciproquement, l'existence d'une relation de Bézout entre a et b implique que a et b sont premiers entre eux (et alors les coefficients, u et v, sont aussi premiers entre eux). En effet, tout diviseur commun de a et b doit diviser $au + bv$.

Exemple : $42 \times 38 - 55 \times 29 = 1$ constitue une relation de Bézout entre 42 et 55. On verra plus loin comment obtenir une relation de Bézout.

Naturellement, ajouter b à u et $-a$ à v donne une nouvelle relation de Bézout entre a et b. Donc il n'y a pas unicité.

Si $au + bv = \pm 1$ on dit parfois que les rationnels a/b et $-v/u$ (écrits sous forme irréductible) sont *adjacents*.

Plus généralement, si $\mathrm{pgcd}(a, b) = d$, on peut trouver u et v tels que $au + bv = d$ (en fait, $\mathrm{pgcd}(\frac{a}{d}, \frac{b}{d}) = 1$, et si $\frac{a}{d}u + \frac{b}{d}v = 1$ est une relation de Bézout entre eux, alors on a $au + bv = d$).

1.14 Algorithme d'Euclide

Soit à calculer le pgcd de deux entiers a et b. **L'algorithme d'Euclide** pour ce faire est le suivant :

– Initialiser : $(m, n) \leftarrow (|a|, |b|)$.

1. Étienne Bézout (1730–1783), avec un accent aigu.

– Tant que $n \neq 0$, répéter :
  – Faire $(m, n) \leftarrow (n, r)$ où r est le reste de la division euclidienne $m = nq + r$ de m par n.
– Renvoyer m (le pgcd recherché).

Invariant : $\mathrm{pgcd}(m, n) = \mathrm{pgcd}(a, b)$ (constant) ; l'algorithme termine car n décroît strictement à chaque étape (et reste un entier naturel).

Exemple : soit à calculer le pgcd de $a = 98$ et $b = 77$:
– $(m, n) = (98, 77)$; division euclidienne $98 = 77 \times 1 + 21$;
– $(m, n) = (77, 21)$; division euclidienne $77 = 21 \times 3 + 14$;
– $(m, n) = (21, 14)$; division euclidienne $21 = 14 \times 1 + 7$;
– $(m, n) = (14, 7)$; division euclidienne $14 = 7 \times 2 + 0$;
– $(m, n) = (7, 0)$; on renvoie 7.

Algorithme d'Euclide « étendu » : L'idée est de « remonter » les coefficients dans l'algorithme d'Euclide : la dernière division $m = nq + 1$ donne une relation $1 = m - nq$ puis on remplace n (qui est lui-même un reste de division euclidienne) et ainsi de suite jusqu'à trouver une relation entre les entiers a et b de départ.

En mémoire constante, cela donne :

Soit à calculer une relation de Bézout entre deux entiers a et b (premiers entre eux) :
– $(m, n, u, v, u', v') \leftarrow (|a|, |b|, \mathrm{signe}(a), 0, 0, \mathrm{signe}(b))$.
– Tant que $n \neq 0$, répéter :
  – Division euclidienne de m par n : soit $m = nq + r$.
  – Remplacer $(m, n, u, v, u', v') \leftarrow (n, r, u', v', u - qu', v - qv')$.
– Vérifier $m = 1$ (le pgcd est bien 1).
– Les coefficients recherchés sont u et v (on a $au + bv = 1$).

Invariants : $au + bv = m$ et $au' + bv' = n$.

Dans la pratique, à la main, on procède ainsi : pour calculer une relation de Bézout entre 64 et 47, on effectue les divisions euclidiennes successives $64 = 1 \times 47 + 17$, $47 = 2 \times 17 + 13$, $17 = 1 \times 13 + 4$, $13 = 3 \times 4 + 1$ jusqu'à tomber sur le reste 1. Puis on réécrit ce reste en partant de la dernière division $1 = 13 - 3 \times 4$ et en remplaçant successivement le reste de chaque division (les à l'envers) par une combinaison du dividende et du diviseur : $4 = 17 - 1 \times 13$ donc $1 = 13 - 3 \times (17 - 1 \times 13) = 4 \times 13 - 3 \times 17$ puis $13 = 47 - 2 \times 17$ donc $1 = 4 \times (47 - 2 \times 17) - 3 \times 17 = 4 \times 47 - 11 \times 17$ et enfin $17 = 1 \times 64 - 47$ donc $1 = 4 \times 47 - 11 \times (1 \times 64 - 47) = 15 \times 47 - 11 \times 64$.

2 Congruences et entiers modulaires

2.1 Congruence

Soit m un entier fixé pour le moment :

Si x et x' sont entiers, on dit que x et x' sont **congrus** modulo m, noté $x \equiv x' \pmod m$, lorsque $x - x'$ est multiple de m (ou, si on préfère, $x \equiv x' \pmod m$ signifie qu'il existe $k \in \mathbb{Z}$ tel que $x' = x + km$). Cette relation est réflexive (on a $x \equiv x \pmod m$), symétrique (si $x \equiv y \pmod m$ alors $y \equiv x \pmod m$) et transitive (si $x \equiv y \pmod m$ et $y \equiv z \pmod m$ alors $x \equiv z \pmod m$) — on dit qu'il s'agit d'une *relation d'équivalence*.

Lorsque m est clair d'après le contexte, on écrit parfois simplement $x \equiv x'$ pour $x \equiv x' \pmod m$.

Dire $x \equiv 0 \pmod m$ signifie simplement que x est multiple de m.

Compatibilité avec les opérations : (à m fixé,) si $x \equiv x'$ et $y \equiv y'$ alors $x+y \equiv x' + y'$ et $xy \equiv x'y'$. À m variable : si $m|m'$ alors $x \equiv x' \pmod{m'}$ implique $x \equiv x' \pmod m$ (la congruence modulo m' est *plus fine* que modulo m).

La *classe de congruence* modulo m (ou : classe d'équivalence pour la congruence modulo m) d'un entier x est l'ensemble $\{x + km \colon k \in \mathbb{Z}\}$ de tous les entiers congrus à x modulo m (ce sont les valeurs d'une suite arithmétique de raison m). On la note $(\bar{x})_{\mathrm{mod}\, m}$ ou parfois simplement $\bar{x}$ si m est clair dans le contexte.

Représentants : si $m \geq 1$ alors chaque entier est congru modulo m à *un et un seul* des nombres $0, 1, 2, \ldots, (m-1)$ (le reste de sa division euclidienne par m !). On dira que ce sont les *représentants standards* des classes de congruence modulo m.

Pour $m \geq 1$, il y a donc exactement m classes de congruence modulo m (à savoir $\bar{0}, \bar{1}, \ldots, \overline{m-1}$). On notera $\mathbb{Z}/m\mathbb{Z}$ l'ensemble de ces classes (cf. plus bas).

Exemple : $\mathbb{Z}/2\mathbb{Z}$ avec $\bar{0}$ = classe des nombres pairs et $\bar{1}$ = classe des nombres impairs. Remarque : on peut savoir si $x + y$ ou xy est pair ou impair en sachant si x et y le sont — c'est la compatibilité aux opérations vue plus haut — ce qui permet de définir une addition et une multiplication sur $\mathbb{Z}/2\mathbb{Z}$.

On veut définir une addition et une multiplication $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$ de façon analogue : pour ajouter $\bar{x}$ et $\bar{y}$, on consière $\bar{x} + \bar{y} = \overline{x+y}$ et $\bar{x}\,\bar{y} = \overline{xy}$.

2.2 Généralité sur les quotients

Généralité : soit E un ensemble et $\sim$ une relation d'équivalence (i.e., réflexive, symétrique, transitive) sur E, on appelle $E/\sim$ l'ensemble des classes d'équivalence de E modulo $\sim$ (la classe d'équivalence d'un élément $x \in E$ est l'ensemble des éléments $x' \in E$ tels que $x \sim x'$). On note $\pi\colon E \to (E/\sim)$ la fonction qui envoie $x \in E$ sur sa classe d'équivalence $\pi(x) = \bar{x}$. Ainsi : $\pi(x) = \pi(x')$ ssi $x \sim x'$. (Moralement : on a transformé la relation d'équivalence $\sim$ en une vraie égalité.)

Si on a sur E une opération binaire, disons, $\top$, telle que $x \sim x'$ et $y \sim y'$ impliquent $(x \top y) \sim (x' \top y')$ (on dit que $\sim$ est *compatible* avec l'opération $\top$), alors on peut définir une opération binaire $\bar{\top}$ sur $E/\sim$ par $\pi(x) \,\bar{\top}\, \pi(y) = \pi(x \top y)$.

L'application $\pi\colon E \to (E/\sim)$ préserve alors l'opération $\top$ et on dit qu'il s'agit d'un *morphisme* (d'ensembles munis d'une opération binaire $\top$).

2.3 Calculs dans $\mathbb{Z}/m\mathbb{Z}$

Vision concrète de $\mathbb{Z}/m\mathbb{Z}$ pour $m \geq 1$: on travaille avec les nombres $0, \ldots, m-1$ (qui sont des *représentants* arbitraires des m classes de congruences modulo m). Les opérations sont faites dans les entiers mais ensuite on se ramène à une classe représentée par un entier entre 0 et $m-1$ en effectuant une division euclidienne par m.

Exemple : si $m = 10$, on a $\bar{8} + \bar{5} = \bar{3}$ et $\bar{8} \times \bar{5} = \bar{0}$.

(Note : en fait, pour l'addition, il suffit de soustraire éventuellement m si le résultat l'excède : pas besoin de faire une vraie division euclidienne.)

Les ordinateurs travaillent naturellement dans $\mathbb{Z}/2^r\mathbb{Z}$ avec r valant typiquement 16, 32 ou 64.

Note importante : Le choix des représentants $0, \ldots, m-1$ est arbitraire : on pourrait tout aussi bien choisir $1, \ldots, m$ ou bien $-\lfloor \frac{m-1}{2} \rfloor, \ldots, \lfloor \frac{m}{2} \rfloor$ (ou encore des choses tout à fait arbitraires).

Il faut bien comprendre que, si x, y sont deux entiers, alors $\bar{x} = \bar{y}$ dans $\mathbb{Z}/m\mathbb{Z}$ signifie exactement la même chose que $x \equiv y \pmod{m}$.

Et si $m \leq 1$?

- On a $\mathbb{Z}/1\mathbb{Z} = \{\bar{0}\}$, et les opérations sont triviales ($\bar{0} + \bar{0} = \bar{0}$ et $\bar{0} \times \bar{0} = \bar{0}$).
- On a $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.
- Si $m < 0$ alors $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(-m)\mathbb{Z}$.

En général quand on parle de $\mathbb{Z}/m\mathbb{Z}$ on sous-entend $m \geq 1$, parfois même $m \geq 2$!

2.4 Premières propriétés de $\mathbb{Z}/m\mathbb{Z}$

C'est un anneau commutatif. Il n'est *pas intègre* en général : on peut avoir $ab = \bar{0}$ dans $\mathbb{Z}/m\mathbb{Z}$ alors que $a \neq \bar{0}$ et $b \neq \bar{0}$ (exemple : $\bar{2} \times \bar{5} = \bar{0}$ dans $\mathbb{Z}/10\mathbb{Z}$).

Surjection canonique : c'est l'application $\pi\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ qui envoie $x \in \mathbb{Z}$ sur sa classe de congruence modulo m. C'est un *morphisme d'anneaux*, i.e., il préserve l'addition et la multiplication et envoie 0 et 1 sur $\bar{0}$ et $\bar{1}$.

Si $m|m'$, il y a une application naturelle $\mathbb{Z}/m'\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ car les classes modulo m' sont plus fines que modulo m. (Exemple : connaître la congruence modulo 4 permet de connaître la congruence modulo 2.) C'est également un morphisme d'anneaux.

Attention ! le paragraphe précédent signifie que quand $m|m'$, on peut réduire modulo m un élément de $\mathbb{Z}/m'\mathbb{Z}$. Ceci n'a pas de sens sans l'hypothèse $m|m'$! Par exemple, donné un élément de $\mathbb{Z}/20\mathbb{Z}$, il y a un sens à parler de sa classe modulo 5 ou modulo 4 ou modulo 2 (c'est-à-dire dire s'il est pair ou impair...) ; en revanche, il n'y a *aucun sens* à parler de sa classe modulo 3 (ou même à se demander s'il est multiple de 3). Le théorème « chinois » précisera cette idée.

2.5 Inversibles de $\mathbb{Z}/m\mathbb{Z}$

Si a et m sont premiers entre eux, alors on sait qu'on peut trouver une relation de Bézout $au + mv = 1$. On a alors $\bar{a}\bar{u} = \bar{1}$: on dit que $\bar{a}$ est *(multiplicativement) inversible* dans $\mathbb{Z}/m\mathbb{Z}$, ou est une *unité* de cet anneau. Réciproquement, si on peut trouver $\bar{u}$ tel que $\bar{a}\bar{u} = \bar{1}$, alors a est premier à m.

On appelle $(\mathbb{Z}/m\mathbb{Z})^\times$ l'ensemble des inversibles multiplicatifs de $\mathbb{Z}/m\mathbb{Z}$. C'est un groupe pour la multiplication (plus généralement, dans tout anneau commutatif A, l'ensemble des inversibles/unités de A forme un groupe noté $A^\times$).

Si $\bar{a}$ est inversible dans $\mathbb{Z}/m\mathbb{Z}$, on pourra noter $\bar{a}^{-1}$ son inverse (qui est évidemment de nouveau inversible...). On le calcule à partir d'une relation de Bézout. Attention, il n'est pas évident de relier $\bar{a}^{-1}$ avec le rationnel $1/a$!

Exemple : dans $\mathbb{Z}/10\mathbb{Z}$, les éléments $\bar{1}, \bar{3}, \bar{7}, \bar{9}$ sont inversibles, et leurs inverses sont $\bar{1}^{-1} = \bar{1}, \bar{3}^{-1} = \bar{7}, \bar{7}^{-1} = \bar{3}, \bar{9}^{-1} = \bar{9}$.

On note $\varphi(m)$ le cardinal de $(\mathbb{Z}/m\mathbb{Z})^\times$: la fonction φ s'appelle *fonction indicatrice d'Euler* ; elle compte donc le nombre d'entiers entre 0 et $m-1$ premiers avec m (exemple : $\varphi(10) = 4$). On verra plus loin comment la calculer.

Note : on a deux involutions importantes sur $(\mathbb{Z}/m\mathbb{Z})^\times$: l'une est $\bar{a} \mapsto -\bar{a}$, et l'autre est $\bar{a} \mapsto \bar{a}^{-1}$. Comme la première n'a pas de point fixe (pour $m > 2$), $\varphi(m)$ est toujours *pair* (sauf pour $m = 2$).

Si p est premier, alors tous les nombres entre 1 et $p-1$ sont premiers avec p : $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \ldots, \overline{p-1}\}$ (et notamment $\varphi(p) = p-1$). Tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles sauf $\bar{0}$: on dit que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un *corps* et on le note $\mathbb{F}_p$.

2.6 Théorème chinois

Si m et n sont deux naturels non nuls **premiers entre eux**, considérons l'application dont les composantes sont les deux surjections canoniques :

$$\mathbb{Z}/(mn)\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

Autrement dit, il s'agit de l'application qui envoie un entier z modulo mn sur sa classe modulo m et sa classe modulo n.

Il s'agit d'un *morphisme d'anneaux* (car les surjections canoniques en sont !) :

– il est injectif car un entier multiple de m et de n est multiple de mn (lemme de Gauß),

– il est surjectif car les cardinaux coïncident (mn au départ et à l'arrivée),

c'est donc un **isomorphisme**.

Dresser la table d'isomorphisme de $\mathbb{Z}/10\mathbb{Z}$ avec $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$...

Concrètement, le théorème chinois signifie : lorsque m et n sont premiers entre eux, se donner un entier modulo mn revient au même que se donner cet entier modulo m et modulo n séparément (et, de plus, toutes les combinaisons d'une classe modulo m et d'une classe modulo n sont possibles pour une unique classe modulo mn).

2.7 Théorème chinois explicite

Si on a une relation de Bézout $um + vn = 1$, alors l'isomorphisme chinois a pour réciproque

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) &\to \mathbb{Z}/(mn)\mathbb{Z} \\ (x, y) &\mapsto umy + vnx\end{aligned}$$

(Remarque : dans cette expression, on peut se contenter de calculer uy modulo n avant de le multiplier par m, et de même vx modulo m avant de

le multiplier par n, ce qui est parfois plus efficace que de faire tout le calcul modulo mn.)

Exemple : trouver le nombre entre 0 et 100 congru à 9 modulo 11 et à 3 modulo 13. (Relation de Bézout : $6 \times 11 - 5 \times 13 = 1$; ensuite, $6 \times 11 \times 3 - 5 \times 13 \times 9 \equiv 5 \times 11 - 1 \times 13 \equiv 42 \pmod{11 \times 13}$.)

Généralisations du théorème chinois :

- Si m et n ne sont pas premiers entre eux, toute donnée d'une classe x modulo m et d'une classe y modulo n ne permet pas forcément de retrouver une classe modulo mn (il faut, et il suffit, pour cela, que x et y soient « compatibles », c'est-à-dire congrus modulo $d = \mathrm{pgcd}(m, n)$). Lorsque x et y sont compatibles, alors on retrouve une unique classe modulo $\mathrm{ppcm}(m, n)$ (pour faire le calcul en pratique, diviser les nombres m, n par d', d'' tels que $d'd'' = d$ pour se ramener à deux nombres m/d' et n/d'' premiers entre eux et dont le produit vaut $\frac{mn}{\mathrm{pgcd}(m,n)} = \mathrm{ppcm}(m, n)$).
- Si $m_1, \ldots, m_k$ sont premiers entre eux *deux à deux*, alors la donnée d'une classe modulo le produit $m_1 \cdots m_k$ équivaut à la donnée de classes modulo chacun des m_i (pour faire le calcul en pratique, on utilise les classes modulo m_1, m_2 pour trouver une classe modulo $m_1 m_2$, puis celle-ci et la classe modulo m_3 déterminent une classe modulo $m_1 m_2 m_3$, etc.).
- En combinant ces deux généralisations : connaissant la classe d'un entier modulo $m_1, \ldots, m_k$, on peut retrouver sa classe modulo $\mathrm{ppcm}(m_1, \ldots, m_k)$.

2.8 Calcul de l'indicatrice d'Euler

Si m et n (naturels non nuls) sont premiers entre eux, par le théorème chinois on a $(\mathbb{Z}/(mn)\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, donc

$$\varphi(mn) = \varphi(m)\,\varphi(n)$$

Si p est premier alors $\varphi(p^r) = (p-1)\,p^{r-1}$ (car être premier avec p^r équivaut à être premier à p, et c'est le cas de $p-1$ entiers sur p).

On en déduit :

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

où p parcourt les premiers divisant n.

Exemple : $\varphi(63) = \frac{2}{3} \times \frac{6}{7} \times 63 = 36$.

(Intuitivement : parmi les n entiers de 0 à $n-1$, pour chacun des nombres premiers p divisant n, il y a une proportion $\frac{p-1}{p}$ des nombres qui ne sont pas multiples de p, et toutes ces propriétés sont indépendantes — c'est essentiellement le théorème chinois — donc la proportion des nombres qui ne sont multiples d'aucun des p divisant n est le produit des $\frac{p-1}{p}$.)

Algorithmiquement : *lent* en général (demande de connaître la d.f.p.).

2.9 Notions de théorie des groupes

Un **groupe** est un ensemble G muni d'une opération binaire $\star$ (c'est-à-dire une application $G \times G \to G$ dont on note $g \star g'$ l'image d'un couple (g, g')) et d'un élément remarquable e tels que :

- Associativité de $\star$: $x \star (y \star z) = (x \star y) \star z$
- Neutralité de e pour $\star$: $e \star x = x \star e = x$
- Existence de symétriques : pour chaque x, il existe un élément noté x' tel que) $x \star x' = x' \star x = e$

Lorsque de plus la loi $\star$ est commutative ($y \star x = x \star y$), on parle de *groupe abélien* (ou commutatif).

Exemples : l'addition sur les nombres réels (la loi $\star$ étant l'addition et le neutre e étant le nombre 0), ou sur les complexes, ou sur les entiers ; la multiplication sur les nombres réels non nuls (la loi $\star$ étant la multiplication et le neutre e étant le nombre 1), ou sur les réels strictement positifs, ou sur les complexes non nuls ; la composition des isométries du plan (la loi $\star$ étant la composition et le neutre e étant l'identité).

Contre-exemple : la multiplication sur les entiers (ou même sur les entiers non nuls) *ne forme pas* un groupe, faute d'inverses pour les entiers autres que ± 1.

Généralement, un groupe est noté soit de façon multiplicative (on écrit xy au lieu de $x \star y$ et 1 au lieu de e, et dans ce cas on note x^m l'élément $x \star x \star \cdots x$ avec m fois x et x^{-1} le symétrique de x, alors appelé « inverse »), soit de façon additive (on écrit $x + y$ au lieu de $x \star y$ et 0 au lieu de e, et dans ce cas on note mx l'élément $x + x + \cdots + x$ avec m fois x, et $-x$ le symétrique de x, alors appelé « opposé »). Très souvent on utilise une de ces deux notations de façon implicite.

Attention : il ne faut pas s'imaginer qu'il existe une différence mathématique entre « groupes multiplicatifs » et « groupes additifs » : un groupe est un groupe, il se trouve simplement que pour certains d'entre eux on a plutôt l'habitude de noter multiplicativement et pour certains plutôt additivement. (La notation additive est en principe réservée aux groupes abéliens mais on n'en rencontrera pas de non-

abéliens dans ce cours.)

Un **morphisme** de groupe $\psi\colon G \to G'$ est une application qui préserve la composition ($\psi(x \star y) = \psi(x) \star \psi(y)$), et du coup forcément aussi l'élément neutre ($\psi(e) = e$) et les symétriques (le symétrique de $\psi(x)$ est l'image du symétrique de x).

Un **isomorphisme** de groupes est un morphisme bijectif ; moralement : les groupes G et G' sont abstraitement « le même » (mais éventuellement notés ou étiquetés différemment). Attention ! On aura souvent affaire, par exemple, à un morphisme entre un groupe noté additivement et un groupe noté multiplicativement : dans ce cas, cela signifie $\psi(x + y) = \psi(x)\,\psi(y)$. Exemple : l'exponentielle (de base e, disons) constitue un isomorphisme entre le groupe additif des réels et le groupe multiplicatif des réels strictement positifs.

De façon générale, si g est un élément d'un groupe G, on a un morphisme de groupes $\psi\colon \mathbb{Z} \to G$ défini par $\psi(i) = g^i$ en notation multiplicative (ou, ce qui revient au même en notation additive : $\psi(i) = ig$). L'*image* de ce morphisme, c'est-à-dire l'ensemble de tous les $\psi(i)$ pour i parcourant $\mathbb{Z}$, s'appelle le *sous-groupe engendré par g dans G* (cf. plus bas).

Si on a $g^m = 1$ (on va voir que ceci signifie que m est un multiple de l'ordre de g, cf. plus bas), alors le morphisme $\psi\colon \mathbb{Z} \to G, i \mapsto g^i$ défini ci-dessus vérifie : $\psi(i) = \psi(j)$ si $i \equiv j \pmod m$ (en effet, $j = i + km$ pour un certain $k \in \mathbb{Z}$, donc $g^j = g^i \cdot (g^m)^k = g^i$) ; par conséquent, on peut définir un nouveau morphisme de groupes $\bar\psi\colon \mathbb{Z}/m\mathbb{Z} \to G$ qui envoie $\bar\imath \in \mathbb{Z}/m\mathbb{Z}$ sur $g^i \in G$. On peut donc faire comme si on pouvait élever g à une puissance dans $\mathbb{Z}/m\mathbb{Z}$. Ce morphisme sera extrêmement important dans la suite.

L'**ordre d'un groupe** est simplement son cardinal, lorsque celui-ci est fini.

L'**ordre d'un élément** g dans un groupe fini est le plus petit $m \geq 1$ tel que $g^m = 1$ (en notation multiplicative ; en notation additive, cela s'écrirait : $mg = 0$). Autrement dit, c'est le plus petit m tel qu'en composant m fois l'élément g on retombe sur l'élément neutre.

Si m est l'ordre de g, alors le morphisme $\bar\psi\colon \mathbb{Z}/m\mathbb{Z} \to G$ est *injectif*, c'est-à-dire que les $\bar\psi(\bar\imath)$ sont tous distincts quand $\bar\imath$ parcourt $\mathbb{Z}/m\mathbb{Z}$ (en effet, si $\bar\psi(\bar\imath) = \bar\psi(\bar\jmath)$ avec $\bar\imath \neq \bar\jmath$, on peut supposer $0 \leq i < j < m$ et alors $g^{j-i} = 1$, ce qui contredit la minimalité de m). Autrement dit, $\bar\psi$ définit un isomorphisme entre $\mathbb{Z}/m\mathbb{Z}$ et le groupe $\{g^i\colon i \in \mathbb{Z}\}$ des puissances de g.

En particulier, l'ordre d'un élément g est le nombre $\#\{g^i\colon i \in \mathbb{Z}\}$ de puissances distinctes de cet élément.

Par ailleurs, si on a $g^n = 1$, cela signifie que l'ordre de g *divise* n (en effet, $\bar{\psi}(\bar{n}) = \bar{\psi}(\bar{0})$ signifie $\bar{n} = \bar{0}$ dans $\mathbb{Z}/m\mathbb{Z}$ où m est l'ordre de g, c'est-à-dire que n est *multiple* de m). Il y a donc équivalence entre : $g^n = 1$ et n est multiple de l'ordre de g.

Un **sous-groupe** H d'un groupe G est un sous-ensemble de G qui est lui-même un groupe pour la même opération et le même élément neutre ; c'est-à-dire, c'est une partie H de G telle que $1 \in H$ et que $x, y \in H \Rightarrow xy \in H$ et que $x \in H \Rightarrow x^{-1} \in H$ (cette dernière partie étant d'ailleurs automatique si le groupe G est fini). (Exemple : pour la multiplication, les nombres réels strictement positifs forment un sous-groupe du groupe des nombres réels non nuls.)

Le sous-groupe engendré par une partie E d'un groupe G est le plus petit sous-groupe contenant E (c'est-à-dire l'intersection de tous les sous-groupes de G contenant E). On utilisera cette notion seulement dans le cas suivant : le *sous-groupe engendré par un unique élément* g de G : c'est l'ensemble $\{g^i : i \in \mathbb{Z}\}$ des puissances de g. Comme on l'a vu ci-dessus, l'ordre $m = \#\{g^i : i \in \mathbb{Z}\}$ de ce sous-groupe est égal à l'ordre de g (ce qui justifie le fait d'utiliser le même mot « ordre » pour les deux notions), et ce sous-groupe est isomorphe à $\mathbb{Z}/m\mathbb{Z}$, par l'isomorphisme $\bar{\imath} \mapsto g^i$.

Théorème de Lagrange : Dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe. En particulier, l'ordre d'un élément divise l'ordre du groupe : si G est un groupe fini et $g \in G$ alors $g^{\#G} = 1$.

2.10 Groupes cycliques

On dit qu'un groupe fini G est **cyclique** lorsqu'il existe un élément g (appelé *générateur* de G) tel que tout élément de G soit de la forme g^k (une puissance de g, en notation multiplicative ; en notation additive, cela s'écrirait : kg, i.e., un multiple de g), autrement dit : le sous-groupe engendré par g est G tout entier. Ou encore : G est cyclique de générateur g si et seulement si l'ordre de g est égal à l'ordre de G.

Le groupe *additif* $\mathbb{Z}/m\mathbb{Z}$ est cyclique, avec pour générateur 1 (mais ce n'est pas le seul possible ! cf. ci-dessous). Réciproquement, on a vu que tout groupe cyclique est isomorphe à $\mathbb{Z}/m\mathbb{Z}$, avec m l'ordre d'un générateur g (qui est donc aussi l'ordre du groupe et ne dépend pas du générateur), l'isomorphisme $\mathbb{Z}/m\mathbb{Z} \to G$ étant donné par $\bar{\imath} \mapsto g^i$.

D'où une autre définition possible : un groupe cyclique G [de générateur g] est un groupe isomorphe à $\mathbb{Z}/m\mathbb{Z}$ [avec 1 correspondant à g].

Quels sont tous les générateurs de $\mathbb{Z}/m\mathbb{Z}$ (comme groupe additif !) ? Réponse : ce sont précisément les classes modulo m des entiers premiers à m, c'est-à-dire les inversibles de $\mathbb{Z}/m\mathbb{Z}$ (comme anneau !). (Démonstration : si $\bar{a}$ engendre le groupe additif $\mathbb{Z}/m\mathbb{Z}$, alors en particulier il doit engendrer $\bar{1}$, c'est-à-dire qu'on peut écrire $\bar{1} = \bar{a}+\bar{a}+\cdots+\bar{a}$, avec u fois $\bar{a}$ disons, donc $\bar{a}\bar{u} = \bar{1}$ dans l'anneau $\mathbb{Z}/m\mathbb{Z}$, et $\bar{a}$ y est bien inversible. Réciproquement, si $\bar{a}\bar{u} = \bar{1}$, et si $\bar{a} + \bar{a} + \cdots + \bar{a} = 0$, avec k fois $\bar{a}$, alors en multipliant par $\bar{u}$ on a $\bar{1} + \bar{1} + \cdots + \bar{1} = 0$, soit $\bar{k} = 0$, donc k est multiple de m : ceci prouve que l'ordre de $\bar{a}$ ne peut pas être plus petit que m.)

Ainsi, pour m entier naturel non nul et a entier, il y a équivalence entre :
- les entiers a et m sont premiers entre eux,
- l'élément $\bar{a}$ a pour ordre (additif) m dans le groupe $\mathbb{Z}/m\mathbb{Z}$,
- l'élément $\bar{a}$ est générateur du groupe $\mathbb{Z}/m\mathbb{Z}$,
- l'élément $\bar{a}$ est inversible dans l'anneau $\mathbb{Z}/m\mathbb{Z}$,
- l'élément $\bar{a}$ appartient au groupe $(\mathbb{Z}/m\mathbb{Z})^\times$ des inversible de l'anneau $\mathbb{Z}/m\mathbb{Z}$.

En particulier, $\mathbb{Z}/m\mathbb{Z}$ admet $\varphi(m)$ générateurs. Comme un groupe cyclique d'ordre m est la même chose que (un groupe isomorphe à) $\mathbb{Z}/m\mathbb{Z}$, on en déduit : le nombre de générateurs de n'import quel groupe cyclique d'ordre m est $\varphi(m)$.

Attention ! on parlera aussi, plus loin, des générateurs du groupe *multiplicatif* $(\mathbb{Z}/m\mathbb{Z})^\times$ (et de la question de savoir s'il y en a). Il ne faut pas confondre !

De façon générale, l'ordre additif de $\bar{a}$ dans $\mathbb{Z}/m\mathbb{Z}$ vaut exactement $m/\operatorname{pgcd}(a, m)$. (Et réciproquement, les éléments de $\mathbb{Z}/m\mathbb{Z}$ dont l'ordre divise d, pour d un diviseur de m, sont les [classes des] multiples de m/d.)

2.11 Théorème d'Euler

Si m est un entier naturel non nul et a un entier premier à m, alors

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Démonstration : l'élément $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ a un ordre qui d'après Lagrange doit diviser l'ordre du groupe, i.e. $\varphi(m)$.

Attention ! ne pas confondre l'ordre (« additif ») d'un élément du groupe additif $\mathbb{Z}/m\mathbb{Z}$ et l'ordre (« multiplicatif ») d'un élément du groupe multiplicatif $(\mathbb{Z}/m\mathbb{Z})^\times$. Exemple : quel est l'ordre de 2 dans $\mathbb{Z}/7\mathbb{Z}$? (réponse : 7 car $2+2+2+2+2+2+2 = 0$ dans $\mathbb{Z}/7\mathbb{Z}$ et qu'on ne trouve pas 0 avant) ; et dans $(\mathbb{Z}/7\mathbb{Z})^\times$? (réponse : 3 car $2 \times 2 \times 2 = 1$ dans $(\mathbb{Z}/7\mathbb{Z})^\times$ et qu'on ne trouve pas 1 avant).

Pour que l'ordre multiplicatif d'un élément x dans $\mathbb{Z}/m\mathbb{Z}$ soit défini, il faut (et il suffit) que cet élément x soit dans $(\mathbb{Z}/m\mathbb{Z})^\times$ (car c'est lui le groupe multiplicatif), et dans ce cas l'ordre additif vaut forcément m car x est un générateur du groupe cyclique $\mathbb{Z}/m\mathbb{Z}$.

Cas particulier du théorème d'Euler : le « petit théorème de Fermat » : si p est premier, alors $a^{p-1} \equiv 1 \pmod{p}$ lorsque a n'est pas multiple de p ; donc, pour tout entier a on a

$$a^p \equiv a \pmod{p}$$

Ceci fournit une condition *nécessaire* mais non suffisante pour qu'un nombre soit premier.

2.12 Éléments primitifs

Soit m un entier naturel non nul. On dit que $g \in (\mathbb{Z}/m\mathbb{Z})^\times$ est (un résidu) **primitif** (modulo m) lorsqu'il engendre $(\mathbb{Z}/m\mathbb{Z})^\times$ (comme groupe abélien multiplicatif) — ce qui entraîne que $(\mathbb{Z}/m\mathbb{Z})^\times$ est cyclique.

Autrement dit, $g^{\varphi(m)} = 1$ est *optimal* : dire que g est primitif modulo m signifie que son ordre multiplicatif est *exactement* $\varphi(m)$ (et pas un autre diviseur de $\varphi(m)$).

Exemple : les puissances de $\bar{2}$ modulo 9 sont : $\bar{2}, \bar{4}, \bar{8}, \bar{7}, \bar{5}, \bar{1}$; il y en a bien $\varphi(9) = 6$ donc 2 est primitif modulo 9.

Attention ! Ne pas confondre :

- $\mathbb{Z}/m\mathbb{Z}$ (groupe *additif*, d'élément neutre 0) est d'ordre m et est *toujours* cyclique (avec pour générateurs au moins 1 et -1, et tous les éléments de $(\mathbb{Z}/m\mathbb{Z})^\times$).
- $(\mathbb{Z}/m\mathbb{Z})^\times$ (groupe *multiplicatif*, d'élément neutre 1) est d'ordre $\varphi(m)$ et est *parfois* cyclique (auquel cas ses générateurs s'appellent éléments *primitifs* et il y en a $\varphi(\varphi(m))$).

Théorème :

- Si p est un nombre premier impair, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, i.e., *il existe* des éléments primitifs modulo p. (Il en existe exactement $\varphi(p-1)$.)
- Si p est un nombre premier impair et $r \geq 2$, alors $(\mathbb{Z}/p^r\mathbb{Z})^\times$ est cyclique, i.e., il existe des éléments primitifs modulo p^r. (Il en existe exactement $\varphi(p^{r-1}(p-1))$.) *Mieux* : g est primitif modulo p^r si et seulement si il l'est modulo p^2.
- Si $p = 2$ et $1 \leq r \leq 2$, alors $(\mathbb{Z}/2^r\mathbb{Z})^\times$ est trivialement cyclique.

– Si $p = 2$ et $r \geq 3$, alors $(\mathbb{Z}/2^r\mathbb{Z})^\times$ *n'est pas* cyclique : il est produit d'un groupe cyclique d'ordre 2 engendré par -1 et d'un groupe cyclique d'ordre 2^{r-2} engendré par 5 (l'ordre maximal possible d'un élément est 2^{r-2}).

Attention à ne pas faire l'erreur suivante : si on a $g^{\varphi(m)} = 1$, cela *ne signifie pas* que g soit primitif, et d'ailleurs c'est le cas pour tout élément inversible de $\mathbb{Z}/m\mathbb{Z}$ d'après le théorème d'Euler : pour pouvoir dire que g est primitif, la condition importante est que $g^i \neq 1$ lorsque $0 < i < \varphi(m)$.

3 Polynômes

3.1 Définition, structure d'anneau et degré

Soit k un anneau commutatif quelconque (par exemple : $\mathbb{Z}$), typiquement un corps (exemples importants : $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ou bien $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

Un **polynôme** en t à coefficients dans k est une somme formelle $f = a_0 + a_1 t + a_2 t^2 + \cdots$ avec $a_i \in k$ où *seul un nombre fini* des a_i est non nul (sinon on parle de **série formelle**). Autrement dit, on peut écrire $f = a_0 + a_1 t + \cdots + a_n t^n$ pour un certain n (et si on impose $a_n \neq 0$, ceci définit n, qui s'appellera alors le degré de f).

Opérations :

– Addition : terme à terme ($c_i = a_i + b_i$).

– Multiplication : « produit de Cauchy » en développant formellement ($c_i = \sum_{j=0}^{j=i} a_j b_{i-j}$).

Si k est un anneau commutatif, alors $k[t]$ aussi.

Degré d'un polynôme : $\deg f =$ le plus grand i tel que $a_i \neq 0$ (le degré du polynôme nul est question de convention). On peut donc écrire un polynôme de degré $\leq N$ comme $a_0 + \cdots + a_N t^N$; si $a_N = 1$ on dit que f est **unitaire**. Plus généralement, le coefficient $a_{\deg f}$ s'appelle *coefficient dominant* de f.

Propriétés du degré :

– $\deg(f + g) \leq \max(\deg f, \deg g)$ (avec égalité si $\deg f \neq \deg g$)

– $\deg(fg) = \deg f + \deg g$ (dès que k est *intègre*, en particulier sur un corps)

Si k est un anneau commutatif intègre, alors $k[t]$ aussi.

Attention, $k[t]$ n'est jamais un corps ! (Car t n'a pas d'inverse pour la multiplication.)

À souligner : *analogie* importante entre les polyômes, notamment dans $\mathbb{F}_p[t]$, et l'écriture en base p des entiers. Différence importante : pas de retenue pour les polynômes.

Complexité des opérations : cf. entiers.

3.2 Opérations spécifiques aux polynômes

Évaluation de polynômes : si $f = a_0 + \cdots + a_N t^N$ et x est dans k ou $k[t]$ (ou plus généralement une « k-algèbre »), on définit $f(x) = a_0 + \cdots + a_N x^N$.

Cas particulier : **composition** : si $g \in k[t]$, on note $f \circ g$ plutôt que $f(g)$.

Racines : si $f(x) = 0$ avec $x \in k$, on dit que x est une *racine* du polynôme f.

Attention : On peut très bien avoir $f(x) = 0$ pour tout $x \in k$ sans pour autant que f soit nul (e.g., $f = t^p - t$ dans $\mathbb{F}_p[t]$).

(Mais on va voir que si k est un corps, le nombre de racines de f dans k est inférieur ou égal au degré de f.)

Dérivée : si $f = a_0 + a_1 t + \cdots + a_N t^N$ alors $f' = a_1 + 2a_2 t + \cdots + N a_N t^{N-1}$.

Attention : On peut avoir $f' = 0$ sans avoir f constant (e.g., $f = t^p$ dans $\mathbb{F}_p[t]$).

Dérivées successives : $f^{(i+1)} = (f^{(i)})'$ pour $i \in \mathbb{N}$.

3.3 Polynôme interpolateur

Dans cette section, soit k un *corps* et $f \in k[t]$.

Fait fondamental : lorsque deux polynômes de degré $\leq N$ coïncident en (au moins) $N + 1$ points, ils sont égaux ; de façon équivalente, si un polynôme de degré $\leq N$ s'annule en $\geq N + 1$ points, alors c'est le polynôme nul.

Réciproquement, si $a_0, \ldots, a_N \in k$ sont deux à deux distincts, et $b_0, \ldots, b_N \in k$ sont quelconques, alors

$$\sum_{i=0}^{N} b_i \frac{\prod_{j \neq i}(t - a_j)}{\prod_{j \neq i}(a_i - a_j)}$$

(*polynôme interpolateur de Lagrange*) est un polynôme de degré $\leq N$ prenant en a_i la valeur b_i. D'après ce qu'on vient de dire, c'est *le* seul polynôme de degré $\leq N$ prenant en chaque a_i la valeur b_i.

Ceci permet de reconstruire un polynôme à partir de ses valeurs en suffisamment de points.

3.4 Division euclidienne de polynômes

Sauf mention du contraire, k est maintenant un **corps**.

Division euclidienne analogue à celle des entiers :
Si $f \in k[t]$ et $g \in k[t]$ est *non nul*, il existe un unique couple (q, r) tel que :
– $q \in k[t]$,
– $r \in k[t]$ est (nul ou) de degré $\deg r < \deg g$ et
– $f = gq + r$.

Algorithme « naïf » de division euclidienne : procéder par puissances *décroissantes* :
Soit $f = a_N t^N + \cdots + a_0$ et $g = b_D t^D + \cdots + b_0$ où $b_D \neq 0$ (donc $\deg g = D$) :
– si $N < D$ on renvoie $q = 0$ et $r = f$;
– sinon, on pose $c = a_N / b_D$, on définit $f^* = f - ct^{N-D}g$, donc $\deg(f^*) < N$, on applique l'algorithme pour diviser f^* par g, soit $f^* = gq^* + r$ et on a $f = gq + r$ où $q = ct^{N-D} + q^*$.

Cas très important : Le reste de la division euclidienne de f par $t - a$ (où $a \in k$ est une constante) est $f(a)$. (En effet, c'est clair lorsque $a = 0$, et on en déduit le cas général par translation.)

Exercice : Effectuer la division euclidienne de t^7 par $2t^3 + 1$ dans $\mathbb{F}_7[t]$. (Réponse : $t^7 = (2t^3 + 1)(4t^4 + 5t) + 2t$.)

3.5 Arithmétique des polynômes

Relation de **divisibilité** : exactement analogue aux entiers. Dire qu'un polynôme f admet a pour racine signifie exactement que $t - a$ divise f.

Les **unités** (ou inversibles) de $k[t]$ sont les éléments de $k^\times$ (polynômes constants non nuls).

Polynômes **irréductibles** : définition analogue aux nombres premiers : on dit que f est irréductible lorsque $\deg f \geq 1$ et qu'il n'existe pas d'écriture $f = gh$ avec $\deg g \geq 1$ et $\deg h \geq 1$. On les choisira normalement *unitaires* ; par convention, 0 et les constantes ne sont pas irréductibles. Les polynômes $t - a$ (unitaires de degré 1) sont *toujours* irréductibles. Lorsque ce sont les seuls, le corps k est dit *algébriquement clos*.

Le corps $\mathbb{C}$ est algébriquement clos. Le corps $\mathbb{R}$ ne l'est pas : les polynômes irréductibles sur $\mathbb{R}$ sont les $t - a$ et les $t^2 - bt + c$ où $b^2 - 4c < 0$. Les corps finis (notamment $\mathbb{F}_p$ déjà vu) ne sont pas algébriquement clos (« encore moins » que $\mathbb{R}$).

Décomposition en facteurs irréductibles : Écriture unique de tout $f \in k[t]$ non nul comme $c\prod_P P^{v_P(f)}$ où $c \in k^\times$ est le coefficient dominant de f et $v_P(f) \in \mathbb{N}$ pour tout P irréductible (presque tous nuls).

Cas où k est algébriquement clos : tout $f \in k[t]$ non nul s'écrit de façon unique comme $c\prod_{a\in k}(t-a)^{v_a(f)}$ où $c \in k^\times$ est le coefficient dominant de f et $v_a(f) \in \mathbb{N}$ est l'ordre du zéro de f en a.

PGCD, algorithme d'Euclide, relations de Bézout, Euclide étendu : exactement analogue aux entiers.

Attention cependant : de même que le pgcd de deux entiers est choisi positif par convention, le pgcd de deux polynômes est choisi unitaire par convention. Dans l'algorithme d'Euclide, il faut donc au final diviser le dernier reste par son coefficient dominant pour le rendre unitaire ; notamment, si le reste final est une *constante* non nulle (pas nécessairement 1), les polynômes sont premiers entre eux (par exemple, le pgcd de $t+2$ et t dans $\mathbb{R}[t]$ est 1, ces polynômes sont premiers entre eux, or si le reste de la division de $t+2$ par t est 2).

3.6 Anneaux $k[t]/(P)$

Analogues exacts de $\mathbb{Z}/m\mathbb{Z}$. Vision abstraite : on définit $f \equiv g \pmod P$ ssi P divise $f-g$, et on quotiente. Vision concrète : les éléments de $k[t]/(P)$ sont représentés de façon unique par des polynômes à coefficients dans k de degré strictement inférieur au degré de P, et on se ramène à $\deg f < \deg P$ par division euclidienne après chaque opération (en fait, on n'a besoin de prendre le reste de la division euclidienne par P qu'après une multiplication, puisque l'addition des polynômes ne fait jamais monter leur degré).

Pour tout $c \in k^\times$, on a $k[t]/(cP) = k[t]/(P)$. Autrement dit, multiplier P par une constante ne change rien, donc on aura tendance à supposer que P est unitaire quand on écrit $k[t]/(P)$.

Les éléments de k se voient comme des éléments de $k[t]/(P)$ (les constantes).

Élément très important : $\bar{t}$. Il vérifie $P(\bar{t}) = 0$ (car le reste de la division euclidienne de $P(t) = P$ par P est 0).

Si on sait ce que ça signifie : $k[t]/(P)$ est un espace vectoriel de dimension $\deg P$ sur k. Si k est fini alors $k[t]/(P)$ est aussi fini, et de cardinal $(\#k)^{\deg P}$ (concrètement, se donner un élément de $k[t]/(P)$ revient à se donner un élément de $k[t]$ de degré $< \deg P$, donc à se donner $\deg P$ coefficients, chacun pouvant prendre $\#k$ valeurs).

Théorème chinois : si P et Q sont premiers entre eux, on a $k[t]/(PQ) \cong$

$(k[t]/(P)) \times (k[t]/(Q))$ (même démonstration que pour les entiers, avec un petit peu d'algèbre linéaire).

Exemple idiot : $k[t]/(t) \cong k$ (ici, $\bar{t} = 0$). En fait, $k[t]/(t-a) \cong k$ où $\bar{t}$ devient a. Exemples moins idiot : $\mathbb{R}[t]/(t^2+1) \cong \mathbb{C}$, et $\mathbb{R}[t]/(t^2-1) \cong \mathbb{R}[t]/(t-1) \times \mathbb{R}[t]/(t+1) \cong \mathbb{R} \times \mathbb{R}$ (théorème chinois en utilisant la factorisation $t^2 - 1 = (t-1)(t+1)$; noter que ce n'est pas un corps).

Exercice : dresser les tables de $\mathbb{F}_2[t]/(t^2+t+1)$. Vérifier qu'il s'agit d'un *corps* à 4 éléments. On le notera $\mathbb{F}_4$. (*Attention !* Ce n'est pas $\mathbb{Z}/4\mathbb{Z}$, car ce dernier n'est pas un corps !)

Important : $k[t]/(P)$ est un corps *si et seulement si* $P \in k[t]$ est irréductible. Lorsque c'est le cas, on l'appelle **corps de rupture** de P sur k.

4 Corps finis

4.1 Sous-corps premier et caractéristique

Si $\mathbb{F}$ est un corps fini, alors l'ensemble $\{0_\mathbb{F}, 1_\mathbb{F}, 1_\mathbb{F}+1_\mathbb{F}, 1_\mathbb{F}+1_\mathbb{F}+1_\mathbb{F}, \ldots\}$ est fini. Cet ensemble a la structure d'un $\mathbb{Z}/p\mathbb{Z}$ avec p premier : on dit qu'il s'agit du **(sous-)corps premier** de $\mathbb{F}$, et que p en est la **caractéristique**. Autrement dit, ce p est l'ordre additif de l'élément 1 de $\mathbb{F}$, et il s'agit toujours d'un nombre premier.

Si q est le cardinal de $\mathbb{F}$, alors q est toujours une puissance de p (par exemple, si on sait ce que ça signifie, parce que $\mathbb{F}$ est un espace vectoriel de dimension finie d sur son corps premier $\mathbb{F}_p$) ; on note typiquement $q = p^d$, et alors d s'appelle le **degré** de $\mathbb{F}$ au-dessus de son corps premier $\mathbb{F}_p$, ou simplement « degré absolu » de $\mathbb{F}$.

En particulier, le nombre d'éléments d'un corps fini est toujours une puissance $q = p^d$ d'un nombre premier p (il n'y a pas de corps à 6 ou 10 éléments !), et tout corps fini contient un $\mathbb{Z}/p\mathbb{Z}$.

4.2 Petit théorème de Fermat, unicité des corps finis

Dans un corps $\mathbb{F}$ à q éléments, on a $a^{q-1} = 1$ pour tout $a \in \mathbb{F}^\times$ (par Lagrange appliqué au groupe multiplicatif $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ qui a $q-1$ éléments). On a donc $a^q = a$ pour tout $a \in \mathbb{F}$ (« petit théorème de Fermat » généralisé aux corps finis).

Ceci peut aussi se dire : le polynôme $t^q - t \in \mathbb{F}[t]$ s'annule en tout point de $\mathbb{F}$

(tout élément de $\mathbb{F}$ en est racine). Comme il est de degré q, on a sa factorisation :

$$t^q - t = \prod_{a \in \mathbb{F}} (t - a)$$

Cette factorisation étant valable dans n'importe quel corps L (fini ou non) contenant $\mathbb{F}$, on voit que $\mathbb{F}$ peut se définir (dans n'importe quel corps L le contenant) comme l'ensemble des éléments x vérifiant $x^q = x$ (plus explicitement : le petit théorème de Fermat signifie que tout élément de $\mathbb{F}$ vérifie $x^q = x$, mais réciproquement tout élément de L vérifiant cette équation est automatiquement dans $\mathbb{F}$).

Ceci constitue une forme d'unicité des corps finis : un corps L donné ne peut contenir qu'*au plus un* sous-corps $\mathbb{F}$ ayant q éléments (pour n'importe quel q) — dès qu'il en contient un, ce corps est complètement déterminé (comme l'ensemble des éléments vérifiant $x^q = x$).

En particulier, le sous-corps premier $\mathbb{F}_p$ d'un corps fini L de caractéristique p est $\mathbb{F}_p = \{x \in L : x^p = x\}$.

On admet également l'unicité à isomorphisme près : deux corps finis à q éléments, pour le même q, sont isomorphes. (C'est-à-dire qu'il s'agit abstraitement du même objet, mais dont les éléments peuvent être « nommés » différemment.) On notera $\mathbb{F}_q$ le corps à q éléments, s'il existe (on va voir que c'est le cas pour toute puissance q d'un nombre premier).

4.3 Morphisme de Frobenius, conjugués d'un élément

Si $\mathbb{F}$ est un corps fini de caractéristique p alors l'application $\mathrm{Frob} : \mathbb{F} \to \mathbb{F}, x \mapsto x^p$ (parfois notée Frob_p pour plus de clarté) est appelée **(morphisme de) Frobenius** de $\mathbb{F}$ (au-dessus de $\mathbb{F}_p$). C'est un morphisme de corps : il vérifie $\mathrm{Frob}(x + y) = \mathrm{Frob}(x) + \mathrm{Frob}(y)$ et $\mathrm{Frob}(xy) = \mathrm{Frob}(x)\,\mathrm{Frob}(y)$ (le second est évident, et le premier est est vrai car on est en caractéristique p donc, quand on développe $(x + y)^p$, tous les coefficients binomiaux intermédiaires sont multiples de p donc nuls). C'est aussi une bijection de $\mathbb{F}$ sur lui-même (c'est-à-dire que Frob permute les éléments de $\mathbb{F}$, chacun ayant un unique antécédent ou racine p-ième).

En appliquant plusieurs fois successivement le morphisme Frob à un élément $x \in \mathbb{F}$ où $\mathbb{F}$ est un corps fini à $q = p^d$ éléments, on obtient successivement : $x = \mathrm{Frob}^0(x)$, $\mathrm{Frob}^1(x) = x^p$, $\mathrm{Frob}^2(x) = (x^p)^p = x^{p^2}$, $\mathrm{Frob}^3(x) = (x^{p^2})^p = x^{p^3}$, ... $\mathrm{Frob}^i(x) = x^{p^i}$. Ces éléments x^{p^i} s'appellent les **conjugués** de x (au-dessus de $\mathbb{F}_p$).

On a vu plus haut que $x^{p^d} = x$ (c'est le petit théorème de Fermat), autrement dit, au bout de d applications du Frobenius on retombe sur l'élément x de départ ; il se peut qu'on retombe sur x plus tôt : le plus petit r tel que $x^{p^r} = x$, qui est aussi le nombre de conjugués distincts de x, s'appelle le **degré** absolu de x (ou : degré de x au-dessus de $\mathbb{F}_p$), et ce degré r divise d (qu'on a appelé le degré de $\mathbb{F}$). Tous les conjugués de x ont bien sûr le même degré que x.

Attention ! si $\mathbb{F}$ est un corps fini à $q = p^d$ éléments, ne pas confondre les trois choses suivantes :

- L'ordre additif d'un élément x dans $\mathbb{F}$ (groupe additif) : cet ordre vaut toujours p sauf pour $x = 0$ (auquel cas c'est 1).
- L'ordre multiplicatif d'un élément $x \neq 0$ dans $\mathbb{F}^\times$ (groupe multiplicatif des éléments non nuls) : cet ordre divise $q - 1$ puisque le groupe $\mathbb{F}^\times$ est d'ordre $q - 1$.
- Le degré r d'un élément x au-dessus de $\mathbb{F}_p$ qu'on vient de définir : ce degré divise d.

Il y a cependant des rapports : par exemple, si $x \neq 0$ est de degré r alors son ordre multiplicatif divise $p^r - 1$ (car on a $x^{p^r} = x$ par définition de r, donc $x^{p^r-1} = 1$) ; notamment, si x est d'ordre $q-1 = p^d-1$ (on va voir qu'il existe de tels éléments, ce sont les éléments primitifs) alors x est de degré d (mais la réciproque n'est pas vraie).

4.4 Existence et inclusions des corps finis

Pour tout nombre premier p et tout $d \geq 1$, il existe un corps à $q = p^d$ éléments, qu'on peut noter $\mathbb{F}_q$. On peut le voir comme $\mathbb{F}_q \cong \mathbb{F}_p[t]/(f)$ pour un certain polynôme $f \in \mathbb{F}_p[t]$ irréductible de degré d (l'affirmation importante est qu'il en existe !).

Moralement, le fait de choisir tel ou tel polynôme f irréductible de degré d (unitaire, disons) ne change pas le corps $\mathbb{F}_q$ qu'on obtient comme $\mathbb{F}_p[t]/(f)$, cela change uniquement la valeur de l'élément représenté comme $\bar{t}$.

Si $q = p^d$ et $q' = p'^{d'}$, alors $\mathbb{F}_q$ est contenu dans $\mathbb{F}_{q'}$ (plus proprement : $\mathbb{F}_{q'}$ contient un sous-corps ayant q éléments) si et seulement si : (1) $p = p'$ et (2) $d|d'$. Cela équivaut encore à : q' est une puissance de q. (Exemple : $\mathbb{F}_4$ est contenu dans $\mathbb{F}_{16}$ mais pas dans $\mathbb{F}_8$.)

Rappelons que lorsque c'est le cas (que q' est une puissance de q), on peut retrouver $\mathbb{F}_q$ dans $\mathbb{F}_{q'}$ comme l'ensemble $\{x : x^q = x\}$ des racines de $t^q - t$, ou

encore comme l'ensemble des éléments dont le degré au-dessus de $\mathbb{F}_p$ divise d (car $x^q = x$ signifie $\mathrm{Frob}^d(x) = x$).

4.5 Test de Rabin, factorisation de $t^{p^d} - t$

Test d'irréductibilité de Rabin : Étant donné $f \in \mathbb{F}_p[t]$ de degré d, il est irréductible si et seulement si les deux conditions suivantes sont vérifiées :

(a) f divise $t^{p^d} - t$, et

(b) f est premier avec $t^{p^e} - t$ pour tout diviseur strict e de d (en fait, on peut se contenter de tester pour les diviseurs *immédiats*, c'est-à-dire les $e = d/\ell$ avec ℓ premier divisant d).

(Remarque : la condition (a) s'écrit $t^{p^d} \equiv t \pmod f$, et pour la vérifier on applique un algorithme d'exponentiation rapide [2] pour calculer $\bar{t}^{p^d}$ dans $\mathbb{F}_p[t]/(f)$. De même, la condition (b) se teste avec l'algorithme d'Euclide en commençant par calculer t^{p^e} modulo f.)

Exercice : Vérifier que $f = t^4+t+1$ est irréductible dans $\mathbb{F}_2[t]$. (On a $t^4 \equiv t+1 \pmod f$ donc $t^8 \equiv t^2 + 1$ donc $t^{16} \equiv t^4 + 1 \equiv t$ donc le premier critère est vérifié. Pour le second, $t^4 - t \equiv 1 \pmod f$ donc l'algorithme d'Euclide termine immédiatement et $t^4 - t$ et f sont bien irréductibles.) Vérifier que $g = t^4 + t^3 + 1$ est irréductible dans $\mathbb{F}_2[t]$. (On a $t^4 \equiv t^3+1 \pmod g$ donc $t^8 \equiv t^6+1 \equiv t^3+t^2+t$ donc $t^{16} \equiv t^6 + t^4 + t^2 \equiv t$ donc le premier critère est vérifié. Pour le second, $t^4 - t \equiv t^3 + t + 1 \pmod g$ puis $g = t^4 + t^3 + 1 \equiv t^2 \pmod{t^3 + t + 1}$ puis $t^3 + t + 1 \equiv t + 1 \pmod{t^2}$ et enfin $t^2 \equiv 1 \pmod{t + 1}$, donc $t^4 - t$ et g sont bien irréductibles.)

Le nombre de polynômes unitaires irréductibles de degré d dans $\mathbb{F}_p[t]$ vaut approximativement $\frac{1}{d}p^d$ (plus exactement, c'est $\frac{1}{d}p^d + O(p^{d/2})$ lorsque $d \to +\infty$). Ceci signifie que parmi les p^d polynômes unitaires de degré d sur $\mathbb{F}_p$, il y en a une proportion d'environ $\frac{1}{d}$ qui sont irréductibles.

Ainsi, pour générer un polynôme irréductible, il est raisonnable de tirer un polynôme (unitaire) au hasard, et de tester son irréductibilité, et de recommencer jusqu'à obtenir un irréductible.

Polynôme minimal d'un élément : Pour tout $x \in \mathbb{F}_q$, où $q = p^d$, il existe un unique polynôme unitaire irréductible $f \in \mathbb{F}_p[t]$ (noter que x est dans $\mathbb{F}_q$ mais que f est à coefficients dans $\mathbb{F}_p$) tel que $f(x) = 0$. Ce polynôme s'appelle le *polynôme minimal* de x. Son degré δ est égal au degré absolu de x, dont on

2. Par exemple, dans ce cas, tout simplement élever d fois successivement à la puissance p.

rappelle qu'il est défini comme le nombre de conjugués $\mathrm{Frob}^i(x)$ de x ; et les racines de f dans $\mathbb{F}_q$ sont exactement les conjugués $\mathrm{Frob}^i(x)$ en question : on a $f = \prod_{i=0}^{\delta-1}(t - \mathrm{Frob}^i(x))$ (on rappelle que le degré absolu δ de x divise le degré absolu d de $\mathbb{F}_q$).

Si $\mathbb{F}_q$ est vu comme $\mathbb{F}_p[t]/(f)$ avec f un polynôme unitaire irréductible de degré d sur $\mathbb{F}_p$, alors le polynôme minimal de $\bar{t}$ est précisément f. Réciproquement, si $x \in \mathbb{F}_q$ a pour degré d (le degré absolu de $\mathbb{F}_q$, c'est-à-dire le d tel que $q = p^d$) et polynôme minimal f (de degré d, donc), alors il existe un unique isomorphisme de corps $\psi\colon \mathbb{F}_p[t]/(f) \to \mathbb{F}_q$ tel que $\psi(\bar{t}) = x$.

On a vu plus haut que sur le corps $\mathbb{F}_q$ (lorsque $q = p^d$), le polynôme $t^q - t$ se factorise en irréductibles comme $t^q - t = \prod_{a\in\mathbb{F}_q}(t - a)$. Il est utile de savoir ce qu'il en est sur $\mathbb{F}_p$:

Le polynôme $t^q - t$ (où $q = p^d$) se factorise dans $\mathbb{F}_p[t]$ comme le produit de *tous* les polynômes unitaires irréductibles dont le degré δ divise d. (Chacun de ces facteurs f est égal, dans $\mathbb{F}_q[t]$, au produit des $(t - a)$ pour les δ conjugués a d'un élément de degré δ.) Ce fait peut servir à dénombrer de façon précise les polynômes unitaires irréductibles de n'importe quel degré sur $\mathbb{F}_p$.

Note : Contrairement à la situation dans les entiers, on peut effectuer efficacement la factorisation des polynômes sur les corps finis.

4.6 Éléments primitifs

Théorème : Le groupe multiplicatif d'un corps fini est cyclique.

Autrement dit, si $\mathbb{F}$ est un corps fini, il existe des éléments g, dits **primitifs**, qui engendrent le groupe multiplicatif $\mathbb{F}^\times$ des éléments non nuls de $\mathbb{F}$, c'est-à-dire tels que tout élément non nul de $\mathbb{F}$ soit une puissance de g. Un élément primitif de $\mathbb{F}_q$ est un élément de $\mathbb{F}_q^\times$ dont l'ordre multiplicatif vaut exactement $q - 1$.

Le nombre d'éléments primitifs est bien sûr $\varphi(q-1)$ (puisque, une fois qu'on sait que $\mathbb{F}^\times$ est cyclique, comme il est d'ordre $q - 1$, le nombre d'éléments qui l'engendrent est connu).

Si $g \in \mathbb{F}_q$ est primitif, alors tout élément de $\mathbb{F}_q$ est soit 0 soit de la forme g^i pour un entier i (cet entier est défini de façon unique modulo $q - 1$; l'application $\psi\colon \mathbb{Z}/(q-1)\mathbb{Z} \to \mathbb{F}_q^\times$ donnée par $\bar{\imath} \mapsto g^i$ définit un isomorphisme de groupes). La représentation des éléments de $\mathbb{F}_q^\times$ sous la forme g^i permet facilement de calculer des produits, mais ne permet pas de calculer des sommes.

Le problème consistant à retrouver i connaissant (l'élément primitif g et) g^i s'appelle le *problème du logarithme discret*, et il est algorithmiquement difficile.