Introduction au problème de la factorisation des entiers

Journée LIESSE Télécom-UPS « Autour de la factorisation des entiers »

David A. Madore
Télécom ParisTech
david.madore@enst.fr

15 mai 2018

Plan
Rappels d'arithmétique
Tests de primalité
Interlude
Factorisation
Généralités
Algorithmes élémentaires
Extensions quadratiques

Plan

Rappels d'arithmétique

Tests de primalité

Interlude

Factorisation
- Généralités
- Algorithmes élémentaires

Extensions quadratiques

Nombres premiers

- Un **nombre premier** est un entier $p \geq 2$ qui n'est divisible que par 1 et lui-même.

On notera $\mathscr{P} := \{p \geq 2 : p \text{ est premier}\}$.

Les plus petits sont (A000040 dans l'OEIS) : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229...$

- **Euclide :** il y en a une infinité.

- **Théorème des nombres premiers** (Hadamard & de la Vallée-Poussin, 1896) :

$$\pi(x) := \#\{p \in \mathscr{P} \text{ et } p \leq x\} \sim \frac{x}{\log x}$$

quand $x \to +\infty$.

La « probabilité que n soit premier » est environ $\frac{1}{\log n}$.

Factorisation
David Madore
Plan
Rappels d'arithmétique
Tests de primalité
Interlude
Factorisation
Généralités
Algorithmes élémentaires
Extensions quadratiques

Décomposition en facteurs premiers (DFP)

$\mathbb{Z}$ est un **anneau factoriel**, soit concrètement :

- Tout entier $n \neq 0$ a une écriture unique sous la forme $n = up_1 \cdots p_k$ où $u \in \{\pm 1\}$ et $p_1, \ldots, p_k$ sont des nombres premiers (non nécess$^{\text{t}}$ distincts ; unicité à l'ordre près).
- **Variante :** $n = u \prod_{p \in \mathscr{P}} p^{v_p(n)}$ où $v_p(n) \in \mathbb{N}$ s'appelle la **valuation p-adique** de n.

Exemple : $137\,703\,491 = 7919 \times 17\,389$

- k, n **premiers entre eux** (noté $k \wedge n = 1$) ssi k et n n'ont aucun diviseur [premier] commun.

En général, $k \wedge n = \prod_{p \in \mathscr{P}} p^{\min(v_p(k), v_p(n))}$

- **Fonction indicatrice d'Euler :**

$$\varphi(n) := \{0 \leq k < n : k \wedge n = 1\} = n \prod_{p \in \mathscr{P},\, p|n} \left(1 - \frac{1}{p}\right)$$

Factorisation
David Madore
Plan
Rappels d'arithmétique
Tests de primalité
Interlude
Factorisation
Généralités
Algorithmes élémentaires
Extensions quadratiques

Entiers modulo n

$\mathbb{Z}/n\mathbb{Z}$ = anneau des entiers modulo n
(ou concrètement, $\{0, \ldots, n-1\}$ avec addition et multiplication suivies du reste de la division euclidienne par n)

- $\mathbb{Z}/p\mathbb{Z}$ est un corps, alors noté $\mathbb{F}_p$, ssi p est premier.
- En général, $(\mathbb{Z}/n\mathbb{Z})^\times := \{k \in \mathbb{Z}/n\mathbb{Z} : k \text{ inversible}\} = \{k \in \mathbb{Z}/n\mathbb{Z} : k \wedge n = 1\}$
Plus précisément : $uk + vn = 1$ revient à $uk \equiv 1 \pmod{n}$
Notamment, $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$
- **Théorème chinois :** si $a \wedge b = 1$ alors
$$\mathbb{Z}/(ab)\mathbb{Z} \to (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$$
est un isomorphisme.

Calcul du pgcd (algorithme d'Euclide)

Donnés $a, b \geq 0$, on cherche à calculer $d := a \wedge b$ (leur pgcd) sans factoriser a et b.

- $(m, n, u, v, u', v') \leftarrow (a, b, 1, 0, 0, 1)$.
- Tant que $n \neq 0$, répéter :
  - Division euclidienne de m par n : soit $m = nq + r$.
  - Remplacer $(m, n, u, v, u', v') \leftarrow (n, r, u', v', u - qu', v - qv')$.
- Renvoyer $d = m$ (pgcd de a et b).
- On a de plus $au + bv = d$ (Bézout généralisé).

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

Nombre d'étapes : au plus $\frac{\log b}{\log((1+\sqrt{5})/2)} = O(\log b)$ divisions.

Application : calcul d'inverse dans $\mathbb{Z}/n\mathbb{Z}$

Exponentiation rapide

Soit à calculer a^M modulo n où M est gigantesque :

- calculer a^{2^i} pour $0 \leq i \leq \frac{\log M}{\log 2}$ par élévations au carré successives ($a^{2^{i+1}} = (a^{2^i})^2$),
- si $M = 2^{i_0} + \cdots + 2^{i_r}$ (écriture binaire), alors $a^M = a^{2^{i_0}} \times \cdots \times a^{2^{i_r}}$.

Quelques problèmes algorithmiques

- Donné $n \in \mathbb{N}$, déterminer s'il est premier.

Test de primalité, qui peut être certain ou probabiliste.
« Probabiliste » = la réponse « non-premier » est certaine, tandis que la réponse « premier » est correcte avec probabilité garantie $\geq 1 - \varepsilon$.

Des algorithmes polynomiaux (en $\log n$) sont connus.

- Générer un nombre premier de taille donnée.

Solution évidente : tirer au hasard et tester !

- **Factorisation :** calculer la DFP de $n \in \mathbb{N}$ donné.

Problème conjecturé difficile (non polynomial en $\log n$).
Noter qu'il se ramène à :

- Donné $n \in \mathbb{N}$ composé (=non-premier), trouver un diviseur $1 < d < n$ de n (ou même k t.q. $1 < k \wedge n < n$).

Remarques :

- Donné $p \in \mathscr{P}$ et $n \in \mathbb{N}$, calculer $v_p(n)$ est facile.
- Tester si n est une puissance parfaite ($= m^r$ où $r \geq 2$) est facile.

Petit théorème de Fermat

- **Petit théorème de Fermat :** si p premier et $a \wedge p = 1$ (i.e., $p \nmid a$) alors $a^{p-1} \equiv 1 \pmod{p}$.

Preuve : $\#(\mathbb{Z}/p\mathbb{Z})^\times = p-1$ et l'ordre de a divise l'ordre du groupe.
(Ou, si on préfère, $a^p \equiv a \pmod{p}$ pour *tout* a.)

- Fournit une condition nécessaire pour être premier, algorithmiquement testable par calculs dans $\mathbb{Z}/p\mathbb{Z}$ et exponentiation rapide.
- Malheureusement non suffisante même quantifiée par « pour tout a » (premier à p) :

On a $(\forall a)\ a^{1729} \equiv a \pmod{1729}$, mais $1729 = 7 \times 13 \times 19$.

Preuve : On a $a^{1729} \equiv a \pmod{7}$ car $1729 \equiv 1 \pmod{(7-1)}$, idem pour 13 et 19, et appliquer le théorème chinois pour conclure mod 1729.

De tels nombres s'appellent **nombres de Carmichael** (les plus petits sont $561, 1105, 1729, 2465\ldots$ = A002997).

Test de primalité de Miller-Rabin

- **Observation :** si $\mathbb{F}$ est un corps et si $b^2 = 1$ dans $\mathbb{F}$ alors soit $b = 1$ soit $b = -1$.

Pas vrai dans un anneau quelconque, p.ex., $818^2 \equiv 1 \pmod{1729}$ (on a $818 \equiv \pm 1$ modulo les facteurs premiers de 1729, théorème chinois).

- Donc, si p est premier et $a \wedge p = 1$, et si $p - 1 = 2^s \ell$ avec ℓ impair, alors $a^{2^i \ell}$ modulo p doit valoir
  - $+1$ pour $i = 0$, *ou bien*
  - -1 pour au moins un $0 \leq i < s$.

(Ou encore : $a^{2^i \ell}$ vaut $+1$ pour $i = s$, et vaut ± 1 si $a^{2^{i+1} \ell}$ vaut $+1$.)

$\rightarrow$ Critère « fort » (testable) pour être premier.

- Rabin (1980) : si p est composé (=non-premier), *au moins* $\frac{3}{4}(p-1)$ parmi les a entre 1 et $p-1$ échouent le test.

D'où un test de primalité probabiliste (répéter le test pour beaucoup de a tirés au hasard), « Monte Carlo ».

- Complexité en $O((\log n)^3)$, efficace en pratique.

Divers tests de primalité

- Test de Baillie-Pomerance-Selfridge-Wagstaff (c. 1980) : combine un test de Miller-Rabin de base $a = 2$ et un test par suite de Lucas (cf. plus loin).

  Réponse « premier » non garantie mais aucun contre-exemple connu. Extrêmement efficace.

- Test d'Adleman-Pomerance-Rumely (+Cohen-Lenstra) (c. 1983) : calculs dans des corps cyclotomiques.

  Réponse garantie mais, au choix :

  - algorithme « Las Vegas » : temps de calcul probabiliste (polynomial non garanti), ou
  - temps de calcul garanti mais (légèrement) surpolynomial (en $(\log n)^{O(\log\log\log n)}$).

- Divers tests sur courbes elliptiques (à réponse garantie comme APR).

- Ces tests sont utilisés en pratique (Sage: `is_prime` et `is_pseudoprime`).

Test AKS

- Agrawal-Kayal-Saxena (2004) : $\mathscr{P} \in \mathbf{P}$, i.e., il existe un test déterministe polynomial de primalité.

Algorithme facile à décrire :

- Si n est une puissance parfaite, retourner « composé ».
- Soit r le plus petit tel que $\mathrm{ord}_r(n) > 4(\log n)^2$.
- Si $1 < (a \wedge n) < n$ pour un $a \leq r$, retourner « composé ».
- Si $r \geq n$ retourner « premier ».
- Pour a de 1 à $\lfloor 2\sqrt{\varphi(r)} \log n \rfloor$, si $(X-a)^n \not\equiv X^n - a \pmod{X^r - 1, n}$, retourner « composé ».
- Retourner « premier ».

Mais la preuve est un peu délicate.

Intéressant théoriquement, mais inutilisable en pratique.

Le système de chiffrement RSA

Euler : $m^{\varphi(n)} \equiv 1 \pmod{n}$ si $m \wedge n = 1$.
Preuve : $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ et l'ordre de m divise l'ordre du groupe.

- Alice choisit deux grands nombres premiers p, q et les garde secrets. Elle publie $n := pq$ (le « module RSA »). Elle calcule $\varphi(n) = (p-1)(q-1)$ et le garde secret.
- Elle choisit e (l'« exposant de chiffrement »[†]) et le publie, et calcule l'inverse d de e modulo $\varphi(n)$ (« exposant de déchiffrement ») et le garde secret, disons $ed = 1 + v \cdot \varphi(n)$.

- Si Bob veut chiffrer le message $m \in \mathbb{Z}/n\mathbb{Z}$ pour Alice, il calcule $c := m^e$ modulo n (toutes données publiques).
- Pour déchiffrer, Alice calcule c^d, car $c^d = m^{ed} = m^{1+v\varphi(n)}$ qui vaut m modulo n par le théorème d'Euler (au moins si $m \wedge n = 1$, en fait dans tous les cas par théorème chinois).

[†] Souvent $65\,537$.

RSA (suite)

- **Hypothèse :** « casser » RSA est aussi difficile que factoriser des entiers de la taille de n.
- **Hypothèse :** factoriser de grands entiers est difficile.

(Ceci permet à Alice de garder p et q secret alors qu'elle publie $n = pq$.)

- Variante « signature » de RSA : pour « signer » m, Alice publie $s := m^d$. Bob peut alors vérifier en calculant $s^e = m^{ed} = m^{1+v\varphi(n)}$.

Difficulté de comparer les algorithmes

Il n'est pas possible de dire quel est le « meilleur » algorithme de factorisation connu :

- Veut-on factoriser des entiers quelconques ? (Entiers RSA : $n = pq$ avec p, q premiers de taille comparable.) Des nombres très spéciaux (e.g. $2^m - 1$) ?
- Mesure-t-on la complexité en la taille de l'entier n ou en celle du facteur premier p trouvé ?
- Veut-on une bonne complexité asymptotique ? Ou pour la taille accessible aux calculs pratiques ?
- Veut-on une bonne complexité dans le pire cas ? Une estimation probabiliste ? Une bonne efficacité pratique ?
- Suppose-t-on des résultats comme l'hypothèse de Riemann généralisée ? Des « hypothèses plausibles » ?

RSA-768 (768 bits = 232 chiffres décimaux) factorisé en 2009 par crible du corps de nombres (NFS), en $\sim$2000 CPU·ans ou $\sim 10^{20}$ opérations.

Quelques algorithmes de factorisation

- Algorithme naïf : pour chaque $1 \leq d \leq \lfloor \sqrt{n} \rfloor$, tenter la division (complexité en $O(p\,(\log n)^2) = O(n^{1/2}\,(\log n)^2)$).

Utilisé avant des algorithmes plus sophistiqués pour écarter les « petits facteurs ».

- Autres algorithmes exponentiels :
  - Méthode ρ de Pollard : en $O(p^{1/2}\,(\log n)^2)$ $= O(n^{1/4}\,(\log n)^2)$ (sous conditions).
  - Méthode $p-1$ de Pollard, $p+1$ de Williams : efficace si $p-1$ resp. $p+1$ sont « friables ».
  - Lehman : $O(n^{1/3+\varepsilon})$, garanti rigoureusement.
  - SQUFOF de Shank : en $O(n^{1/4})$

.../...

Quelques algorithmes de factorisation (suite)

.../...

- Algorithmes sous-exponentiels (complexité souvent conjecturale) :
  - Courbe elliptique (ECM) de Lenstra : proche des algos $p-1$ et $p+1$, complexité en $O(\exp\left(c\,(\log p)^{1/2}\,(\log\log p)^{1/2}\right)(\log n)^2)$ où $c<2$.
  - CFRAC : basé sur des calculs de fractions continues, en $O(\exp\left(c\,(\log n)^{1/2}\,(\log\log n)^{1/2}\right))$ où $c=\sqrt{2}$
  - Crible quadratique (QS) de Pomerance, Crible quadratique à polynômes multiples (MPQS) de Montgomery : idem mais c plus petit
  - Crible du corps de nombre (NFS) de Lenstra, Lenstra, Manasse & Pollard, en $O(\exp\left(c\,(\log n)^{1/3}\,(\log\log n)^{2/3}\right))$

Quelques remarques générales

- Donné $n \in \mathbb{N}$ composé, on cherche à trouver un diviseur $1 < d < n$ de n.
- Par l'algorithme d'Euclide, il suffit de trouver $1 < k < n$ non premier avec n (prendre $d = k \wedge n$).
- On peut librement supposer : n non puissance parfaite (tester $n = m^r$ est facile), et n sans « petit » facteur.
- Dans les calculs de a^M modulo n, on testera généralement au préalable si $a \wedge n = 1$ (sinon on a trouvé une factorisation).

- Une idée féconde : faire « comme si » n était premier (p.ex., calculer dans $\mathbb{Z}/n\mathbb{Z}$ « comme si » c'était un corps) et *exploiter* un problème qui pourrait survenir.
- Retenir le théorème chinois pour comprendre $\mathbb{Z}/n\mathbb{Z}$!

Algorithme ρ de Pollard

- **Idée :** exploiter le « paradoxe des anniversaires » : si X est un ensemble de taille $\#X = m$, et si $f : X \to X$ est « aléatoire », la suite récurrente $x_{i+1} = f(x_i)$ va boucler (dessiner un ρ), soit $x_j = x_i$ où $i < j$, vers $j \approx \sqrt{2m}$.

- On applique ça à $f(x) = x^2 + 1$ (disons) avec x_0 tiré au hasard : si p est le plus petit diviseur > 1 de n, alors la suite x_i va souvent boucler modulo p avant de boucler modulo n, et $x_j - x_i$ sera zéro modulo p donc fournira un diviseur de n.

- Pour trouver la boucle, on calcule x_i et $y_i := x_{2i}$ modulo n. Les deux sont récurrentes : $x_{i+1} = f(x_i)$ et $y_{i+1} = f(f(y_i))$. À chaque étape, on calcule $(y_i - x_i) \wedge n$. S'il vaut $1 < d < n$, on a gagné. S'il vaut n, prendre un nouveau x_0 et recommencer.

- Efficace pour trouver un facteur premier « assez petit ».

Algorithme $p-1$ de Pollard

- Idée très simple : si $p|n$ est premier alors p divise a^M-1 pour M multiple de $p-1$ (Fermat !), donc $(a^M-1)\wedge n$ est aussi multiple de p.

On ne connaît pas p mais on peut essayer $M=B!$ pour B assez grand, ou, mieux, $M=1\vee 2\vee\cdots\vee B$ (ppcm), bref :

- Choisir B, tirer a au hasard, calculer a^M-1 modulo n où $M=\prod_{q\in\mathscr{P}} q^{\lfloor \log B/\log q\rfloor}=1\vee\cdots\vee B$ par exponentiation rapide, et calculer $(a^M-1)\wedge n$.

- Si un facteur premier p de n est tel que $p-1$ soit « B-ultrafriable », i.e., toutes les puissances de premiers q^v divisant $p-1$ sont $\leq B$, alors $(p-1)|M$ et a^M-1 sera multiple de p.

- **Moralité :** les premiers p tels que $p-1$ n'ait pas de grand facteur premier sont cryptographiquement faibles.

Notion d'extension quadratique

Soit A un anneau et $D \in A$. On définit l'anneau $A(\sqrt{D}) = \{x + y\sqrt{D} : x, y \in A\}$ (où $\sqrt{D}$ est un symbole formel) avec addition terme à terme et multiplication : $(x_1+y_1\sqrt{D})(x_2+y_2\sqrt{D}) = (x_1x_2+Dy_1y_2)+(x_1y_2+y_1x_2)\sqrt{D}$

Soit $\mathbb{F}$ un corps de caractéristique $\neq 2$ et $D \in \mathbb{F}^\times$:

- si $D \in \mathbb{F}^{\times 2}$ (=est un carré), alors $\mathbb{F}(\sqrt{D}) \cong \mathbb{F} \times \mathbb{F}$ par $\sqrt{D} \mapsto (d, -d)$ où $D = d^2$,
- si $D \notin \mathbb{F}^{\times 2}$, alors $\mathbb{F}(\sqrt{D})$ est un corps.

Ceci permet de voir les $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{D})$ où $D \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$.
Noter que $\mathbb{F}_{p^2}^\times$ a $p^2 - 1 = (p-1)(p+1)$ éléments :

- Si $\xi \in \mathbb{F}_{p^2}$ alors $\xi^{p+1} \in \mathbb{F}_p$.

Preuve : Si $\xi \neq 0$, on a $\xi^{p^2-1} = 1$ donc $z := \xi^{p+1}$ est racine $(p-1)$-ième de 1 donc dans $\mathbb{F}_p^\times$ (car $z^p = z$).

Suites de Lucas

Soit F un corps de caractéristique $\neq 2$ et $D \in \mathbb{F}$.
Posons $\omega = \frac{t+\sqrt{D}}{2}$ et $\bar{\omega} = \frac{t-\sqrt{D}}{2}$ (éléments de $\mathbb{F}(\sqrt{D})$).

On écrit $\omega^n = \frac{1}{2}(V_n + U_n\sqrt{D})$ et $\bar{\omega}^n = \frac{1}{2}(V_n - U_n\sqrt{D})$.

Elles vérifient les récurrences linéaires (où $\mathcal{N} := \frac{1}{4}(t^2 - D)$) :

$$\begin{array}{c|c} U_0 = 0 & V_0 = 2 \\ U_1 = 1 & V_1 = t \\ U_{n+2} = tU_{n+1} - \mathcal{N}U_n & V_{n+2} = tV_{n+1} - \mathcal{N}V_n \\ U_{2n} = U_nV_n & V_{2n} = \frac{1}{2}(V_n^2 + DU_n^2) \end{array}$$

(on a ω et $\bar{\omega}$ racines de $X^2 - tX + \mathcal{N} = 0$; noter $\omega\bar{\omega} = \mathcal{N}$).

Si $D \in \mathbb{F}^\times \setminus \mathbb{F}^{\times 2}$ (donc $\mathbb{F}(\sqrt{D})$ est un corps), on a encore :
$V_n = \omega^n + \bar{\omega}^n$ et $U_n = (\omega^n - \bar{\omega}^n)/(\omega - \bar{\omega})$.

Pour p premier impair et $\mathbb{F} = \mathbb{F}_p$ avec toujours $D \in \mathbb{F}^\times \setminus \mathbb{F}^{\times 2}$ (soit $\left(\frac{D}{p}\right) = -1$), on a vu que $\xi^{p+1} \in \mathbb{F}_p$ si $\xi \in \mathbb{F}_p(\sqrt{D})$, c'est-à-dire notamment $U_{p+1} = 0$ (soit : $\omega^{p+1} = \bar{\omega}^{p+1}$).

Les symboles de Legendre et de Jacobi

Si p est premier impair et $a \in \mathbb{Z}$, on définit $\left(\frac{a}{p}\right)$ comme :

- 0 si p divise a,
- $+1$ si $a \in \mathbb{F}_p^{\times 2}$ (carré d'un inversible mod p),
- -1 si $a \in \mathbb{F}_p^{\times} \setminus \mathbb{F}_p^{\times 2}$ (non carré mod p).

- **Euler :** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$

- **Gauß :** $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ (formule complémentaire) et $\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \cdot \left(\frac{p}{q}\right)$ (loi de réciprocité quadratique)

Généralisation à n impair quelconque (Jacobi) :
$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{v_1} \cdots \left(\frac{a}{p_r}\right)^{v_r}$ si $n = p_1^{v_1} \cdots p_r^{v_r}$
Vérifie l'analogue des formules de Gauß, ce qui permet de le calculer efficacement (analogue à l'algorithme d'Euclide).

Tests de primalité par suite de Lucas

On peut refaire avec les suites de Lucas (basées sur les suites géométriques (ω^i) dans $\mathbb{F}_p(\sqrt{D})$) l'analogue de beaucoup de choses faites sur la suite géométrique (a^i) modulo p.

Petit théorème de Fermat : $a^{p-1} = 1 \in \mathbb{F}_p^\times$ si $a \in \mathbb{F}_p^\times$.

Critère faible de primalité : $a^{p-1} \equiv 1 \pmod{p}$

Observation : $b^2 = 1 \Rightarrow$ $b = \pm 1$ dans un corps.

Critère fort : si $p - 1 = 2^s \ell$ (ℓ impair), alors $a^\ell \equiv +1$, *ou bien* $a^{2^i \ell} \equiv -1$ pour un $0 \leq i < s$.

Lucas : $\xi^{p+1} \in \mathbb{F}_p$ si $\xi \in \mathbb{F}_{p^2}$ (donc $U_{p+1} = 0$ dans récur.).

Critère faible de primalité : $U_{p+1} = 0$

Observation : $\omega^{2n} = \bar{\omega}^{2n} \Rightarrow$ $\omega^n = \pm \bar{\omega}^n$ dans un corps.

Critère fort : si $p + 1 = 2^s \ell$ (ℓ impair), alors $U_\ell = 0$, *ou bien* $V_{2^i \ell} = 0$ pour un $0 \leq i < s$.

Plan

Rappels d'arithmétique

Tests de primalité

Interlude

Factorisation

Généralités

Algorithmes élémentaires

Extensions quadratiques

Digression sur les nombres de Mersenne

Lucas-Lehmer : $p \geq 3$ est premier ss'il existe a tel que $a^{p-1} \equiv 1 \pmod{p}$ et $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ pour tout diviseur premier q de $p-1$.
(Élément d'ordre multiplicatif exactement $p-1$.)

Soit $p = 2^s - 1$ et $\omega = 2 + \sqrt{3}$ (soit $D = 12$ et $t = 4$ et $\mathcal{N} = 1$) : la suite de Lucas $V_n = \omega^n + \bar{\omega}^n$ vérifie alors

$$V_{2n} = V_n^2 - 2$$

On peut donc calculer directement V_{2^i} par récurrence sur i.

Lucas-Lemer : $p = 2^s - 1$ est premier *ssi* $V_{2^{s-1}} = 0$ (modulo p).

Utilisé par Lucas (1842–1891) pour prouver la primalité de $2^{127} - 1$ en 19 ans de calcul (fini en 1876).

Algorithme de factorisation $p+1$ de Williams

Analogue de l'algorithme $p-1$ de Pollard sur une suite de Lucas avec $\mathcal{N}=1$ soit $\omega\bar{\omega}=1$ (soit $D=t^2-4$) : on doit alors avoir $V_{p+1}=2$ (en plus de $U_{p+1}=0$) car $\omega^{p+1}=\bar{\omega}^{p+1}=1$.

Même si $(\mathbb{Z}/n\mathbb{Z})(\sqrt{D})$ n'est pas un corps, les suites de Lucas sont encore définissables avec les mêmes formules récurrentes (+ calcul de U_{2n}, V_{2n}) que précédemment !

- Choisir B, tirer t au hasard définissant une suite de Lucas (V_i). Calculer V_M modulo n où $M=\prod_{q\in\mathscr{P}} q^{\lfloor \log B/\log q\rfloor}$ par formules de Lucas, et calculer $(V_M-2)\wedge n$.
- Ceci révélera un éventuel facteur premier p de n est tel que $p+1$ soit « B-ultrafriable ».
- **Moralité :** les premiers p tels que $p+1$ n'ait pas de grand facteur premier sont cryptographiquement faibles.

Un mot sur le crible quadratique

- **Idée grossière :** chercher x, y tels que $x^2 \equiv y^2 \pmod{n}$, soit $(x-y)(x+y) \equiv 0$, et alors $(x-y) \wedge n$ a des chances de donner un diviseur. Mais comment trouver x, y ?
- Choisir une « petite » borne B et produire « assez » de relations $x_i^2 \equiv z_i \pmod{n}$ (voire $z_i = x_i^2 - n$) où z est « B-friable » (= tous ses facteurs premiers sont $\leq B$).
- Utiliser l'algèbre linéaire sur $\mathbb{F}_2$ pour combiner multiplicativement les relations $x_i^2 \equiv z_i$ de sorte que le produit des z_i soit un carré, ce qui donne $x^2 \equiv y^2$ voulu.
- Pour produire les relations, on peut utiliser $x_i = (\lceil \sqrt{n} \rceil + i)$ (donc $z_i = (\lceil \sqrt{n} \rceil + i)^2 - n \approx 2i\sqrt{n}$).
- Une technique plus sophistiquée (« crible ») utilise des premiers p tels que $\sqrt{n}$ soit dans $\mathbb{Z}/p\mathbb{Z}$ pour assurer d'emblée la divisibilité de z_i par eux.