La primalité en temps polynomial

F. Morain

morain@lix.polytechnique.fr

`http://www.lix.polytechnique.fr/Labo/Francois.Morain/`

Slide 1

Plan

I. Les règles du jeu.

II. Sur le chemin du déterminisme.

III. Quelques algorithmes randomisés.

IV. Agrawal, Kayal, Saxena (AKS).

V. Et après ?

Slide 2

I. Les règles du jeu

$$N = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

– Comment faire pratiquement ? Jusqu'à quelle taille ?
  Factorisation : crible algébrique
  $O(\exp(c(\log N)^{1/3}(\log\log N)^{2/3}))$; **155 chiffres**.
  Primalité : peut se faire sans factoriser ; **5878 chiffres**.

– À quelle **classe de complexité**, le problème de décision **estPremier ?** appartient-il ?

Au mieux : P (e.g., multiplication d'entiers).

Au pire : RP (e.g., non résidu quadratique dans $(\mathbb{Z}/p\mathbb{Z})^*$).

Slide 3

II. Sur le chemin du déterminisme

Crible : $n \leqslant \sqrt{N}$, $O(\exp((1/2)\log N))$ divisions.

Pépin : $F_n = 2^{2^n} + 1$ est premier ssi $5^{(F_n-1)/2} \equiv -1 \bmod F_n$; $O(\log F_n)$ multiplications modulaires, donc $O((\log F_n)^3)$ opérations.

F_{24} (5050446 chiffres décimaux, Crandall, Mayer, Papadopoulos, 2002).

Lucas-Lehmer : $M_m = 2^m - 1$ est premier ssi la suite $L_0 = 4$, $L_{n+1} = L_n^2 - 2 \bmod M_m$ est tq $L_{m-2} = 0$.

$m = 13466917$ (4053946 chiffres décimaux, M. Cameron – Woltman (GIMPS), 2001).

Slide 4

Premier essai

Slide 5

Thm. N est premier si et seulement si $(\mathbb{Z}/N\mathbb{Z})^*$ est cyclique d'ordre $N-1$:

$$\left.\begin{array}{l} a^{N-1} \equiv 1 \bmod N \\ \forall\ p \mid N-1,\ a^{\frac{N-1}{p}} \not\equiv 1 \bmod N \end{array}\right\} \Rightarrow \mathbf{N} \text{ est premier}$$

Certificat : $(N, \{p \mid N-1\}, a)$.

Thm. (*Pocklington*, 1914) Soit s tel que $s \mid N-1$

$$\left.\begin{array}{l} a^{N-1} \equiv 1 \bmod N \\ \forall\ q \text{ premier } \mid s, \operatorname{pgcd}(a^{\frac{N-1}{q}} - 1, N) = 1 \end{array}\right\} \Rightarrow \forall\ \mathbf{p} \mid \mathbf{N},\ \mathbf{p} \equiv \mathbf{1} \bmod \mathbf{s}$$

Coro. $s > \sqrt{N} \Rightarrow N$ est premier.

Pbs : factorisation non déterministe ; recherche de a non plus (sauf si Riemann).

Exemple d'utilisation

Slide 6

Hyp. On sait diviser par $d \leqslant 100$.

$$\begin{array}{rcl} N_0 &=& 100003,\quad N_0 - 1 = 2 \times 3 \times 7 \times N_1, \\ N_1 &=& 2381,\quad N_1 - 1 = 2^2 \times 5 \times 7 \times 17 \end{array}$$

p	2	5	7	17
$3^{(N_1-1)/p} \bmod N_1$	2380	1347	1944	949

$\Rightarrow N_1$ est premier

$$s = N_1 > \sqrt{N_0}$$

$$2^{N_0-1} \equiv 1 \bmod N_0, \operatorname{pgcd}(2^{(N_0-1)/N_1} - 1, N_0) = 1$$

$\Rightarrow N_0$ est premier

Rem. On a obtenu une **preuve de primalité récursive** de profondeur $O(\log N)$.

Gauss, Jacobi

Slide 7

Les acteurs :

- L. Adleman, C. Pomerance, S. Rumely (1980, 1983).
- H. Cohen, H. W. Lenstra, Jr (1981 – 1984) ; H. Cohen, A. K. Lenstra (1982, 1987). W. Bosma & M.-P. van der Hulst (1990) ; P. Mihăilescu (1998).

Déf. Soient p, q premiers, $p \mid q-1$; χ caractère d'**ordre** p et **conducteur** q :

$$\begin{array}{rcl} \chi\ : \mathbb{F}_q^* & \to & \langle\zeta_p\rangle \subset \mathbb{Q}(\zeta_p) \\ g^x & \mapsto & \zeta_p^x \end{array}$$

Somme de Gauss : $\tau(\chi) = \sum_{x=1}^{q-1} \chi(x)\zeta_q^x$.

Prop. $\tau(\chi)\tau(\chi^{-1}) = \chi(-1) \cdot q$.

Prop. Si N est premier, $\operatorname{pgcd}(N, pq) = 1$, alors dans $\mathbb{Z}/N\mathbb{Z}[\zeta_p, \zeta_q]$:

$$(*) \qquad \frac{\tau(\chi)^{\mathbf{N}}}{\tau(\chi^{\mathbf{N}})} = \chi(\mathbf{N})^{-\mathbf{N}}$$

L'algorithme (très simplifié)

Slide 8

1. trouver s et t tq $\mathbf{s} = \prod_{\mathbf{q-1}|\mathbf{t}} \mathbf{q} > \sqrt{\mathbf{N}}$;
2. pour tous (p, q) tq $p \mid q-1$ et $q \mid s$, vérifier $(*)$ (+ condition technique) ;
3. si oui, alors tout diviseur r de N s'écrit $N^i \bmod s$ pour un $i \in [1..t]$.

Thm. (Odlyzko-Pomerance) $\exists c_1, c_2 > 0$ tq

$$(\log \mathbf{N})^{\mathbf{c_1} \log\log\log \mathbf{N}} \leqslant \mathbf{t} \leqslant (\log \mathbf{N})^{\mathbf{c_2} \log\log\log \mathbf{N}}.$$

Ex. $s(2^4 \cdot 3 \cdot 5^2 \cdot 7 = 8400) > 3 \cdot 10^{55}$.

Caractéristiques :

- très rapide en pratique, mais pas de certificat vérifiable en temps polynomial.
- Record : $N = 2^{10000} + 177$ a été prouvé en 5 3/4 jours (138 h) sur une Alpha 500 par Mihăilescu, en novembre 1997.

III. Quelques algorithmes randomisés

Slide 9

Un **algorithme de Monte Carlo** pour décider que $X \in \mathbb{A}$ répond **oui** ou **je ne sais pas**.

Il répond **je ne sais pas** avec probabilité $\leqslant \varepsilon$.

Il ne se trompe jamais quand il répond **oui**.

Déf. Un problème de décision est dans **RP** si on lui connait un algorithme de Monte Carlo polynomial.

Rem. Rien à voir avec une probabilité d'erreur sur la réponse ; ou une faille dans le programme ou l'ordinateur.

Rem. Autres notions d'algorithmes probabilistes possibles.

Tests de composition

Slide 10

fonction estComposé(N)

1. Choisir a au hasard dans $\mathbb{Z}/N\mathbb{Z} - \{0\}$.
2. Calculer $g = \mathrm{pgcd}(a, N)$; **si** $g > 1$, **alors** retourner $(\mathtt{oui}, g \mid N)$.
3. **si** $a^{N-1} \not\equiv 1 \bmod N$, **alors** retourner $(\mathtt{oui}, a)$

   sinon retourner `je ne sais pas`.

Prop. La probabilité d'échec est $P(N)/(N-1)$ où $P(\prod_i p_i^{\alpha_i}) = \prod_i \mathrm{pgcd}(p_i - 1, N - 1)$.

Dém. Probabilité de succès :

$$\left(1 - \frac{\varphi(N)}{N-1}\right) + \frac{\varphi(N)}{N-1}\left(1 - \frac{P(N)}{\varphi(N)}\right). \square$$

Nombres de Carmichael : $P(N) = \varphi(N)$, proba d'échec proche de 1.

Euler et Solovay-Strassen

Slide 11

fonction estComposé2(N)

1. Choisir a au hasard dans $\mathbb{Z}/N\mathbb{Z} - \{0\}$.
2. Calculer $g = \mathrm{pgcd}(a, N)$; **si** $g > 1$, **alors** retourner $(\mathtt{oui}, g \mid N)$.
3. **Si** $a^{(N-1)/2} \not\equiv \left(\frac{a}{N}\right) \bmod N$ **alors** retourner $(\mathtt{oui}, a)$

   sinon retourner `je ne sais pas`.

Prop. Proba d'échec $\leqslant 1/2$.

Coro. **estPremier ?**$\in \mathbf{co} - \mathbf{RP}$.

Miller (1975) : $a = 2, 3, \ldots$; Ankeny–Montgomery–Lenstra–Bach : si une hypothèse de Riemann adéquate est vraie, alors le plus petit témoin est $< 2(\log N)^2$.

Vers RP

Slide 12

Soit $C/\mathbb{F}_p : Y^2 = f(X)$ hyperelliptique de genre $g \in \{1, 2\}$. Alors

$$(\sqrt{p} - 1)^{2g} < \#\mathrm{Jac}(C/\mathbb{F}_p) < (\sqrt{p} + 1)^{2g}.$$

Principe général : on dispose d'un grand nombre de groupes possibles ; il suffit d'en trouver un pour lequel son cardinal est complètement factorisé, pour prouver la primalité à la Pocklington.

Dans les détails :

- **Loi d'addition** sur $\mathrm{Jac}(C/(\mathbb{Z}/N\mathbb{Z}))$;
- **Calcul de** $\#\mathrm{Jac}(C/(\mathbb{Z}/N\mathbb{Z}))$ **:** algorithmes à la Schoof en temps polynomial déterministe.
- **Théorème de primalité** à la Pocklington.

En genre 1 : Goldwasser–Kilian, 1986

$E(\mathbb{Z}/N\mathbb{Z}) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{Z}/N\mathbb{Z}), y^2 z = x^3 + axz^2 + bz^3\}$,
$\mathrm{pgcd}(4a^3 + 27b^2, N) = 1$.

Thm. Soient m et s deux entiers tels que $s \mid m$, E une courbe elliptique sur $\mathbb{Z}/N\mathbb{Z}$ et P un point sur E. Alors :

Slide 13

$$\left.\begin{array}{l} [m]P = O_E \\ \forall\, q \text{ premier } \mid s \\ [m/q]P = (X : Y : Z), \mathrm{pgcd}(Z, N) = 1 \end{array}\right\} \Rightarrow \forall\, p \mid N, \#E(\mathbb{Z}/p\mathbb{Z}) \equiv 0(s).$$

Coro. $s > (\sqrt[4]{N} + 1)^2 \Longrightarrow N$ est premier.

Certificat : $(E, m, s, \{q \mid s\}, P)$.

Algorithmes de primalité

GK : choisir E au hasard jusqu'à ce que $\#E = 2q$, q premier, et on itère sur q.

Pb : $\{\#E = 2q\} \neq \emptyset$? ? Cf. $\mathbb{P} \cap [x, x + x^{0.525}] \neq \emptyset$ (Baker *et al.*).

Thm. GK termine en temps $O((\log N)^9)$ en moyenne pour les nombres premiers $\leqslant x$, sauf pour ceux de $\mathcal{E}(x)$ de cardinal

Slide 14

$$\#\mathcal{E}(x) \ll \frac{x/\log x}{2^{2^{\frac{\log\log x}{\log\log\log x}}}}.$$

Thm. (Adleman et Huang) **estPremier ?**$\in \mathbf{RP}$.

Idée : courbes de genre 2, pour lesquelles l'intervalle de Hasse-Weil est assez grand.

Primalité pratique : ECPP

Idée d'A. O. L. Atkin – 1986 : utiliser la réduction de courbes elliptiques à multiplication complexe.

Temps de calcul heuristique : $O((\log N)^{5+\varepsilon})$.

Implantations :

Slide 15

- FM ; 49.45s pour 1024 bits (Pentium 450 MHz).
- Marcel Martin (PRIMO pour windows), dont la version détient le record actuel avec un nombre de **5878 chiffres décimaux** (Jose Luis Gomez Pardo avec Primo 2.0.0 beta 3, 22 semaines sur un processeur AMD XP1800+, terminé le 15/02/03).

Slide 16

```
1628253621821351121473555095......................
..................................................
91425351860523505626513074262261183081972791153927
60186413522011223014475413155451245232618495193937
53990214365654266319334639684674000632737054966942
70706201049313267143600106931578608789284271647721
13918238053455126734592736524508786499162419814030
25404573628691795855082058297859084636689058117667
78320325852167886221591806048296853569091007452347
58412873829540311896270566591593304264046022443751
61032495676088951862954684089860840108005175661322
61238181941054834158908304927905646077242161552251
92707138393025453781508602517778979086738859270050
91039692808110595443925597852557608701513266994211
61115449761857775277007951523795781943818436478311
```

Slide 17

IV. Agrawal, Kayal, Saxena (AKS)

La première idée : (Agrawal, Biswas – 1999)

Prop. N est premier ssi
$P(X) = (X+1)^N - X^N - 1 \equiv 0 \bmod N$.

En pratique : choisir $Q(X) \in \mathbb{Z}/N\mathbb{Z}[X]$ aléatoire de degré $O(\log N)$. Si

$$(X+1)^N \not\equiv X^N + 1 \bmod (Q(X), N)$$

alors N est composé.

La probabilité d'échec est bornée par $1 - 1/(4 \log N)$.

Conjecture : **si N est composé, alors il existe $1 \leqslant r \leqslant \log N$ tel que $P(X)$ n'est pas divisible par $X^r - 1$ modulo N.**

Slide 18

Agrawal, Kayal, Saxena

Thm. Soient N, s des entiers, r un nombre premier et $q = P(r-1)$. Si :

(0)

$$\binom{q-1+s}{s} > N^{2\lfloor\sqrt{r}\rfloor};$$

(i) $N \neq M^k, k > 1$;

(ii) N n'a pas de facteur premier $\leqslant s$;

(iii) $N^{(r-1)/q} \bmod r \notin \{0, 1\}$;

(iv) $\forall\, a, 1 \leqslant a \leqslant s$, $(X-a)^N \equiv X^N - a \bmod (X^r - 1, N)$.

Alors N **est premier**.

Slide 19

Schéma de la démonstration

On suppose que N est composé. Soit p un diviseur premier de N ($p > s$ par (ii)), tq $p^{(r-1)/q} \not\equiv 1 \bmod r$, i.e., $q \mid d := \mathrm{ord}_r(p)$.

Prop. **$\forall i, j,\ \forall a \in 1..s$: $(X-a)^{p^i N^j} = X^{p^i N^j} - a \bmod (X^r - 1, p)$.**

Argument combinatoire : $L = \{p^i N^j, 0 \leqslant i, j \leqslant \lfloor\sqrt{r}\rfloor\}$; tous les éléments de L sont distincts, donc $\#L = (\lfloor\sqrt{r}\rfloor + 1)^2 > r$.

Deux éléments $u_2 > u_1$ sont congrus modulo r :

$$u_1 = p^{i_1} N^{j_1}, u_2 = p^{i_2} N^{j_2} = u_1 + kr, (i_1, j_1) \neq (i_2, j_2).$$

$$(X-a)^{u_2} = X^{u_1+kr} - a = X^{u_1} - a = (X-a)^{u_1} \bmod (X^r - 1, p).$$

Il reste à montrer que $u_1 = u_2$, d'où une contradiction.

Slide 20

$\forall\, a = 1..s, (X-a)^N = X^N - a \bmod (X^r - 1, p)$.

On a aussi $(X-a)^p = X^p - a \bmod (X^r - 1, p)$.

Lemme. Si $(X-a)^{m_1} = X^{m_1} - a \bmod (X^r - 1, p)$ et $(X-a)^{m_2} = X^{m_2} - a \bmod (X^r - 1, p)$, alors $(X-a)^{m_1 m_2} = X^{m_1 m_2} - a \bmod (X^r - 1, p)$.

Dém. Il existe $g(X) \in \mathbb{F}_p[X]$ tq :

$$(X-a)^{m_2} - (X^{m_2} - a) = (X^r - 1) g(X)$$

$$\begin{aligned}(\mathbf{X^{m_1} - a})^{\mathbf{m_2}} - (X^{m_1 m_2} - a) &= (X^{m_1 r} - 1) g(X^{m_1}) \\ &= (X^r - 1) f(X) g(X^{m_1})\end{aligned}$$

$$(X-a)^{m_1 m_2} \equiv (\mathbf{X^{m_1} - a})^{\mathbf{m_2}} \equiv X^{m_1 m_2} - a \bmod (X^r - 1, p). \square$$

Slide 21

Soit $h(X)$ un facteur irréductible de $\Phi_r(X)$ dans $\mathbb{F}_p[X]$.

$F = \mathbb{F}_p[X]/(h(X))$ est un corps fini de degré $d = \mathrm{ord}_r(p) \geqslant q > s$.

On note $\theta = X \bmod (h(X), p)$ et on pose $S = \{\prod_{a=1}^{s}(\theta - a)^{\alpha_a}, \alpha_a \in \mathbb{N}\}$.

Lemme. $\#S \geqslant \binom{q-1+s}{s}$.

Dém. tous les $X - a$ sont irréductibles et distincts dans $\mathbb{F}_p[X]$, puisque $p > s$. Tous les $\prod(X-a)^{\alpha_a}$ avec $\sum \alpha_a < q \leqslant \deg(h)$, sont tous distincts, donc c'est vrai pour les $\prod(\theta - a)^{\alpha_a}$. □

Fin : par construction, si $\beta \in S : \beta^{u_1} = \beta^{u_2}$, i.e., β est racine de $Y^{u_2} - Y^{u_1} = Y^{u_1}Q(Y)$.

$$u_2 - u_1 \leqslant N^{2\lfloor\sqrt{r}\rfloor} < \binom{q-1+s}{s} \leqslant \#S,$$

d'où $Q = 0$ et $u_2 = u_1$. □

Slide 22

Analyse

Coût : s calculs de X^N modulo $(X^r - 1, N)$; un calcul coûte $O(\log N)$ produits de polynômes de degré r, soit :

$$O(sr^2(\log N)^3).$$

Prop. Si $s = \lfloor 2\lfloor\sqrt{r}\rfloor \log N/\log 2\rfloor + 1$ et $q \geqslant 2s$, alors

$$\binom{q-1+s}{s} > N^{2\lfloor\sqrt{r}\rfloor}.$$

Dém.

$$\binom{q-1+s}{s} > (q/s)^s \geqslant 2^s > N^{2\lfloor\sqrt{r}\rfloor}.$$

Coro. $O(r^{5/2}(\log N)^4)$.

Slide 23

Un peu de théorie analytique

Thm. $\mathcal{P}_\delta(\mathbf{x}) = \#\{p \text{ premier } \leqslant x, P(p-1) > p^\delta\} \geqslant \mathbf{K}_\delta \pi(\mathbf{x})$ pour $x \geqslant x_0$.

pour $\delta = 1/2$ (M. Goldfeld) ; $\ldots$; $\delta = 0.6683$ (Fouvry) ; $\delta = 0.676$ (Baker et Harman).

Prop. $\delta \in]0.5, 0.676]$, $\alpha = 2/(2\delta - 1)$. Il existe $c_2 > c_1 > 0$, $c_3 > 0$ tq si $I_\alpha = [c_1(\log N)^\alpha, c_2(\log N)^\alpha]$, alors :

$\#\{r \in I_\alpha, r$ **premier et** $P(r-1) > r^\delta \geqslant 4\sqrt{r}\log N/\log 2\} \geqslant c_3(\log N)^\alpha/(\log\log N)$.

Dém. $(L = \log N)$ Il suffit que :

$$c_1^\delta L^{\alpha\delta} \geqslant (4/\log 2)c_2^{1/2} L^{\mathbf{1}+\alpha/\mathbf{2}}$$

i.e., $c_1 \geqslant (4/\log 2)^{1/\delta} c_2^{1/(2\delta)}$.

Slide 24

Rappel : (Rosser & Schoenfeld) $x/\log x < \pi(x) \leqslant \gamma x/\log x$ pour $x \geqslant 114$.

$$\begin{aligned}\mathcal{R}(N) = {} & \mathcal{P}_\delta(c_2 L^\alpha) - \mathcal{P}_\delta(c_1 L^\alpha) \geqslant \mathcal{P}_\delta(c_2 L^\alpha) - \pi(c_1 L^\alpha) \\ \geqslant {} & \frac{L^\alpha}{\log(c_2 L^\alpha)(\log(c_1 L^\alpha)}(\cdots + (\mathbf{K}_\delta \mathbf{c_2} - \gamma \mathbf{c_1})\alpha \log L).\end{aligned}$$

Il suffit de prendre $c_1 < K_\delta/\gamma c_2$. □

On cherche maintenant un $r \in I_\alpha$ tq $q \mid r - 1$ et $N^{(r-1)/q} \not\equiv 1 \bmod r$.

$$P = (N-1)(N^2-1)\cdots(N^v - 1)$$

a au plus $(\log N^{v(v+1)/2})/\log 2 \leqslant v^2 \log N$ diviseurs premiers.

Si $v = c_4(\log N)^{(\alpha-2)/2}$, alors $v^2 \log N < \mathcal{R}(N)$, et il existe donc r convenable tq $(r-1)/q \leqslant v$ et $r \nmid P$.

$(r-1)/q \leqslant v$ si $c_2^{1-\delta}(\log N)^{(\mathbf{1}-\delta)\alpha} \leqslant c_4(\log N)^{(\alpha-\mathbf{2})/\mathbf{2}}$ i.e., $c_4 \geqslant c_2^{1-\delta}$.
□

Et enfin...

Coro. Il existe un algorithme de primalité déterministe dont le temps de calcul est $O((\log N)^{(8\delta+1)/(2\delta-1)})$.

Rem. Avec de la multiplication rapide sur les entiers et les polynômes, on trouve $O((\log N)^{6\delta/(2\delta-1)+\varepsilon})$.

Slide 25

Ex. (AKS original) $\delta = 2/3$: **19**, **12** ; $\delta = 1$ (Sophie Germain) : **9**, **6**.

Rem. Jacobi $O((\log N)^{c \log\log\log N})$, ECPP $O((\log N)^{4+\varepsilon'})$.

Rem. Non effectif.

V. Et après ?

Slide 26

- Histoire récente foisonnante (cf. note de D. Bernstein).
- Améliorations par **H. W. Lenstra, Jr.** ($\tilde{O}_{eff}((\log N)^{12})$ ou $\tilde{O}((\log N)^{8})$), **S. David**.
- Nouvelle version de **AKS** : $\tilde{O}_{eff}((\log N)^{10.5})$ ou $\tilde{O}((\log N)^{7.5})$.
- **H. W. Lenstra, C. Pomerance** : $\tilde{O}_{eff}((\log N)^{6})$.
- **P. Berrizbeitia / Q. Cheng :** Soit r premier tq $r^\alpha \mid\mid N-1$, $r \geqslant \log^2 N$; $1 < a < N$ tq $a^{r^\alpha} \equiv 1 \bmod N$, $\mathrm{pgcd}(a^{r^{\alpha-1}} - 1, N) = 1$, $(X+1)^N = X^N + 1 \bmod (X^r - a, N)$, alors N est premier. La complexité heuristique serait de $\tilde{O}((\log N)^4)$ pour ces nombres spéciaux.
- **D. Bernstein, P. Mihăilescu :** utiliser $e \mid N^d - 1$; injecter de la cyclotomie, $\tilde{O}((\log N)^4)$.

Conclusions

Slide 27

Quel algorithme pour la primalité ?

- **facile à comprendre/implanter, rapide :** tests de composition ;
- **rapide, prouvé** : Jacobi ;
- **rapide, heuristique** : ECPP ;
- **certificat :** ECPP ;
- **polynomial déterministe :** AKS.

D. Bernstein a fait un premier exemple pour $2^{1024} + 643$ (13 heures sur un PC à 800 MHz, 200 Mo de mémoire).

Le fossé se comblera-t-il rapidement ?