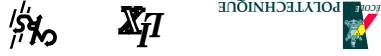


- Slide 2**
- I. Introduction.
 - II. L'âge de Fermat.
 - III. Gauss, Jacobi, etc.
 - IV. Courbes algébriques.
 - V. AKS.

Plan

<http://www.lix.polytechnique.fr/Labo/Francois.Morain/>

morain@lix.polytechnique.fr



F. Morain

La primalité est dans P

- Références**
- [1] P. Ribenboim. *The new book of prime number records*. Springer-Verlag, 1996.
 - [2] D. E. Knuth. *The Art of Computer Programming : Sem numerical Algorithms*. Addison-Wesley, 2nd edition, 1981.
 - [3] H. Cohen. *A course in algorithmic algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1996. Third printing.
 - [4] R. Crandall and C. Pomerance. *Primes – A Computational Perspective*. Springer Verlag, 2000.

Slide 3

I. Introduction

Des nombres premiers . . . pourquoi faire ?

- **Problème fondamental** de la théorie algorithmique des nombres : dans les systèmes de calculs mathématiques.
- **Cryptographie**.

- **Informatique théorique** : à quelle **classe de complexité**, le problème de décision **NP** ? appartient-il ?

Problème pratique : les nombres suivant sont-ils premiers ? Pourquoi ? En combien de temps ?

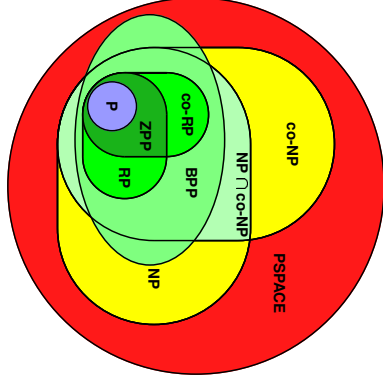
$$89, 341, 1955097530874556503981, 2^{511} + 111, 1263608 + 608, 1263$$

$$2^{10000} + 177, 10^{5019} + 3^2 \cdot 7^5 \cdot 11^{11}, 2^{13166917} - 1.$$

- NP : Pratt (1974);
 - co-RP : Solovay-Strassen (1974, 1977);
 - BPP : Lehman (1982);
 - RP : Adleman & Huang (1986, 1992);
 - P : Agrawal, Kayal et Saxena (2002);
 - Quantique : factorisation ne suffit pas (cf. Chau & Lo, 1997).
- Avant AKS : Adleman, Pomerance, Rumely (1979); Cohen et Lenstra (1984) : $O((\log N)^{c \log \log N})$.
- Test de composition** : permet de décider que N est composé.
- Test de primalité** : on a une preuve que N est premier ou composé.

Slide 6

Primalité et complexité en bret



Slide 5

Primalité et complexité

Thm. $RP \subseteq PSPACE$.
 Dém. diviser N par tous les entiers $\leq \sqrt{N}$. \square

Thm. $RP \subseteq co-NP$.
 Dém. si N n'est pas premier, il existe un certificat vérifiable en temps polynomial (un diviseur de N). \square

1. Choisir $a \neq 0$ au hasard dans $\mathbb{Z}/N\mathbb{Z}$.
2. si $\text{pgcd}(a, N) > 1$, alors retourner (vrai, N n'est pas ppc-a) sinon retourner non prouvé.
3. si (*) n'est pas satisfaite alors retourner (vrai, N n'est pas ppc-a) sinon retourner non prouvé.
- Prop.* (Solovay et Strassen) $RP \subseteq co-RP$.

Slide 8

(*) $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod{N}$

Thm. (Euler) si N premier et $a \in (\mathbb{Z}/N\mathbb{Z})^*$, alors **Solovay-Strassen**

Thm. (Alford, Granville, Pomerance, 1994) Il existe une infinité de nombres de Carmichael, i.e., pp-a pour tout $a \in (\mathbb{Z}/N\mathbb{Z})^*$.

Thm. Il existe une infinité de nombres pseudoprimiers en base a (pp-a).

Contre-ex. $N = 341 = 11 \times 13$, $2^{340} \equiv 1 \pmod{341}$.

Ex. $N = 561 = 3 \times 11 \times 17$.

Slide 7

II. L'âge de Fermat
 A) Une mine de tests de composition

Thm. Si N est premier et $a \in (\mathbb{Z}/N\mathbb{Z})^*$ alors $a^{N-1} \equiv 1 \pmod{N}$.

Thm. (Miller, 1975; Bach 1990) Si une hypothèse de Riemann adéquate est

$\text{er} \exists \mathbb{P} \text{ mod ERH}$
vraie, alors il existe $a < 2^{(\log N)^2}$ tq $a \notin (\mathbb{Z}/N\mathbb{Z})^*$ ou $a \notin E(N)$. \Rightarrow

Autres tests

Artjuhov-Dubois-Seitridge-Miller-Rabin : $\leq 1/4$.

Rem. Interprétation pas si simple (Brassard et al, probabilité en moyenne à la Kim/Pomerance, etc.).
Autres : suites récurrentes linéaires d'ordre 2, etc.; courbes elliptiques; polynômes; combinaisons de tests ($N \pm 1$, Atkin).

Slide 9

B) Preuve de primalité

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

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

Certificat : $(N; \{d \mid N - 1\}, a) \Rightarrow \text{er} \exists \text{ NP (Pratt)}$.

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

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

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

Rem. Deux problèmes : factorisation ; Riemann.

Slide 10

Nombres de Mersenne

Thm. (Lucas-Lehmer) $N = 2^m - 1$ est premier ssi la suite $L_0 = 4, L_{n+1} = L_n^2 - 2 \text{ mod } N$ est tq $L_{m-2} \equiv 0 \text{ mod } N$.

N	# dd	date	qui	machine
M_{125787}	378632	1996	Slowinski et Gage	SGI/Cray T90
$M_{1388269}$	420921	1996	J. Armengaud *	Pentium 90 MHz
$M_{13466917}$	4053946	2001	M. Cameron *	AMD T-Bird 800MHz

* : avec le programme GIMPS écrit par Woltman. (42j)

Slide 12

Exemple d'utilisation

$$N_0 = 10003, N_0 - 1 = 2 \times 3 \times 7 \times N_1, N_1 = 2381, N_1 - 1 = 2^2 \times 5 \times 7 \times 17$$

p	2	5	7	17
$3^{N_1-1}/p \text{ mod } N_1$	2380	1347	1944	949

$\Rightarrow N_1$ est premier

$$s = N_1 < \sqrt{N_0} \Rightarrow N_0 \text{ est premier}$$

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

$\Rightarrow N_0$ est premier

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

$$R_N = \mathbb{Z}/N\mathbb{Z}[\zeta_p, \zeta_q] :$$

Prop. Si N est premier, $\text{pgcd}(N, pq) = 1$, alors dans

$$P_{\text{prop}} \tau(\chi) \tau(\chi^{-1}) = \chi(-1) \cdot q$$

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

$$\zeta_p^x \mapsto \zeta_p^x$$

$$\chi : \mathbb{F}_q^* \rightarrow R^*$$

Solent p, q premiers, $p \mid q - 1$, $\text{pgcd}(pq, N) = 1$: on travaille dans $R = \mathbb{Z}[\zeta_p, \zeta_q]$: χ caractère d'ordre p et conducteur q

Sommes de Gauss

- pas de certificat de primalité.
- 500 par Mihăilescu, en novembre 1997 ;
- **Record** : $N = 2^{10000} + 177$ a été prouvé en 5 3/4 jours (138 h) sur une Alpha
- très rapide en pratique ;
- temps de calcul : $O((\log N)^{c \log \log \log N})$ déterministe ou probabiliste ;

Caractéristiques :

- Mihăilescu (1998).
- W. Bosma & M.-F. van der Huis (1990).
- H. Cohen, A. K. Lenstra (1982, 1987).
- H. Cohen, H. W. Lenstra, Jr (1981 - 1984).
- L. Adleman, C. Pomerance, S. Rumely (1979, 1983).

Les acteurs :

III. Gauss, Jacobi, etc.

Slide 16

version déterministe inefficace en $O((\log p)^8)$ ou bien probabiliste efficace en $O((\log p)^6)$.

Calcul de $\#E(\mathbb{Z}/p\mathbb{Z})$: algorithme de Schoof, Elkies, Atkin, etc. :

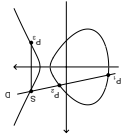
points.

$[-2\sqrt{p}, +2\sqrt{p}]$, il existe une courbe $E(\mathbb{Z}/p\mathbb{Z})$ qui a $p + 1 - t$

Thm. (Deuring, Waterhouse) Pour tout t entier dans

$$|t| < 2\sqrt{p} \quad \#E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - t$$

Le cas des corps finis



$$j = 12^3 \frac{4a^3 + 27b^2}{a^3}$$

$$E(\mathbb{K}) = \{X, Y, 1, Y^2 = X^3 + aX + b\} \cup \{(0, 1, 0)\}$$

$$E : Y^2 Z = X^3 + aXZ^2 + bZ^3$$

Courbes elliptiques :

IV. Courbes algébriques

Goldwasser et Kilian, 1996

fonction $GK(N)$

1. répéter B_1 fois

(a) choisir $a, b \in \mathbb{R}\mathbb{Z}/N\mathbb{Z}$; calculer $g = (4a^3 + 27b^2, N)$;

(b) si $g = N$ alors aller à (a);

(c) si $g \neq 1$ alors retourner (faux, g);

(d) soit $E : y^2 = x^3 + ax + b$;

(e) calculer $m = \#E(\mathbb{Z}/N\mathbb{Z})$ avec Schoof;

(f) si $m = 2q$, avec q probablement premier alors

(a) répéter B_2 fois

• choisir au hasard $P \neq O_E$ sur E ;

• si $[m]P \neq O_E$ alors retourner faux;

• calculer $[q]P = (U : V : W), g = (W, N)$;

• si $g = 1$ alors aller à (β);

• si $1 < g < N$ alors retourner (faux, g);

(β) si $GK(q) = \text{vrai}$ alors retourner vrai;

2. retourner non prouvé.

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

$\mathbb{Z}/N\mathbb{Z}$ et P un point sur E . Alors :

Thm. Soient m et s deux entiers tels que $s \mid m, E$ une courbe elliptique sur

Utilisation en primalité

Pomerance : il existe un certificat très court avec E tq $N + 1 - 2\sqrt{N} < m < N + 1 + 2\sqrt{N}$ et $m \equiv 0 \pmod{2^k}$ avec $2\sqrt{N} < 2^k < 4\sqrt{N}, \dots$, mais comment le trouver ?

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

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

Rem. totalement théorique.

Dém. améliorations de GK + utilisation de courbes de genre 2. \square

Thm. (Adleman et Huang) $\#P \in \text{RP}$.

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

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

Analyse

Idee d'Atkin : utiliser la réduction de courbes elliptiques à multiplication complexe. *Temps de calcul heuristique* : $O((\log N)^{6+\epsilon})$. Pour plus de détails, cf. page web de FM. *Implantations* :

- ECPP depuis 10 ans sur la page web de FM; actuellement V6.4.5; version intermédiaire dans MAGMA : 0.39s pour 256 bits, 3.42s pour 512, 49.45s pour 1024 (Pentium 450 MHz).
- Marcel Martin (PRIMO pour windows), dont la version détient le record actuel avec un nombre indescriptible (N tq $[N - 233822, N] \cap \mathbb{P} = \emptyset$) 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).

$$O(p^{b/2} \log N)^4 \text{ ou } O(p^{3/2} \log N)^3.$$

puis $q \geq 2s > 4 \lfloor \sqrt{t} \rfloor \log N$.

$$\left(q + s - 1 \right)^s < (q/s)^s$$

Slide 22 Choix de r, s :

avec $\mu = \nu = 1$ si tout est natif, $\mu = \nu = \varepsilon$ si on utilise la FFT.

$$O(s \log N)^{\mu_{1+\mu}} (\log N)^{1+\nu}$$

produits de polynômes de degré r, s :

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

Analyse

Démonstration de la validité de l'algorithme

On suppose que N est composé. Soit p un diviseur premier de N ($> p > s$ par (iii)), tq $q \mid d := \text{ord}_p(p)$.
 On a : $X - a = X^N - a = X^N - a \pmod{X^r - 1, p}$.
 Comme p est premier, on a aussi $X - a = X^p - a \pmod{X^r - 1, p}$.
 Slide 24 Lemme. Si $X - a = X^{m_1} - a \pmod{X^r - 1, p}$;
 $X - a = X^{m_2} - a \pmod{X^r - 1, p}$;
 alors $X - a = X^{m_1 m_2} - a \pmod{X^r - 1, p}$.
 Dém. Il existe $g(X) \in \mathbb{F}_p[X]$ tq :

$$(X - a)^{m_2} - a = (X - a)^{m_1} - a \pmod{X^r - 1, p}$$

Alors N est un nombre premier.

$$(v) \forall b, 1 \leq b \leq s, X - b \equiv X^N - b \pmod{N, X^r - 1}.$$

$$(iii) N^{r-1} \not\equiv \{0, 1\} \pmod{r}$$

(ii) N n'a pas de facteur premier $\leq s$:

$$(i) N \neq M^k, k < 1 : \text{Si :}$$

$$(q - 1 + s)^s > N^{2 \lfloor \sqrt{t} \rfloor}.$$

le plus grand facteur premier de $r - 1$. On suppose que

Tm . Soient N un entier, s un entier positif, r un nombre premier et q

V. Agrawal, Kayal, Saxena (AKS)

Un peu de théorie analytique

$$Tm. P_\delta(x) = \#\{p \text{ premier} \leq x, P(p-1) > x^\delta\} \gg c_\delta \pi(x)$$

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

$$Tm. \delta \in [0.5, 0.676], \alpha = 2/(2\delta - 1). \text{ Il existe } c_2 > c_1 > 0 \text{ tq}$$

$$[c_1 \log N]^\alpha, c_2 \log N]^\alpha \text{ contient un } r \text{ convenable.}$$

Coro. Il existe un algorithme de primalité déterministe dont le temps de calcul est $O((\log N)^{(8\delta+1)/(2\delta-1)})$ si on utilise de l'arithmétique naïve, et $O((\log N)^{\delta/(2\delta-1)})$ si on utilise les FFT.

$$Ex. \delta = 2/3 \text{ (AKS)} : 19, 12 : \delta = 1 \text{ (Sophie Germain - rêve)} : 9, 6.$$

Rem. Non effectif.

Slide 23

Fin pop. : tout élément de S est racine de $X^{m_1} - X^{m_2} = X^{m_2-m_1}P(X)$. Or $|m_1 - m_2| \leq N^2 \lfloor \sqrt{r} \rfloor^{s-1} > \#S$, d'où $P \equiv 0$ et $m_1 = m_2$. \square

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

Lemme. $\#S \geq (q^{-1+s})$.

$$S = \left\{ \prod_{s=1}^{m-1} (X - a^{\alpha_a}, \alpha_a \in \mathbb{N}) \right\}$$

$\forall a \in 1..s, (X - a)_{m_1} = (X - a)_{m_2} \pmod{h(X); d}$.
 $d = \text{ord}_p(r) \geq q < s$. On pose $\theta = X \pmod{h(X); d}$.

Lemme. (classique) Soit $h(X)$ un facteur irréductible de $(X^r - 1)/(X - 1)$

dans $\mathbb{F}_q[X]$; $r = \#X \pmod{h(X); d}$ est un corps fini de degré

Slide 26

L'après AKS

cf. note de Bernstein.

- Améliorations par H. W. Lenstra, Jr. $O_{eff}((\log N)^{12})$ ou $\tilde{O}((\log N)^8)$,

- S. David.

- Rumeurs : HWL+Pomerance $O((\log N)^6)$.

- P. Berrizbeitia / Q. Cheng :

Soit r premier tq $r^{\alpha} \parallel N - 1, r \geq 10^8 N; 1 < a < N$ tq $a^{r^{\alpha}} \equiv 1 \pmod{N}$, $\text{pgcd}(a^{r^{\alpha-1}} - 1, N) = 1$.

$(X + 1)_N = X_N + 1 \pmod{X^r - a, N}$, alors N est premier.

Idée : si $N - 1$ ne convient pas, alors on utilise ECFP pour trouver

$N' \in [N + 1 - 2\sqrt{N}, N + 1 + 2\sqrt{N}]$ convenable. La complexité

heuristique serait de $O((\log N)^4)$.

- Efficace un jour ??

Slide 25

Mais $X^r - 1 \mid X^{m_1 r} - 1$, d'où

$$(X^{m_1} - a)^{m_2} - (X^{m_1 r} - 1)g(X^{m_1}).$$

$(X - a)_{m_1 m_2} = (X - a)_{m_1} - a \pmod{X^r - 1, d}$. \square

Coro. $\forall i, j, \forall a \in 1..s : (X - a)^{p^i N^j} = X^{p^i N^j} - a \pmod{X^r - 1, d}$.

Argument combinatoire : $T = \{p^i N^j, 0 \leq i, j \leq \lfloor \sqrt{r} \rfloor\}$:

$\#T = (\lfloor \sqrt{r} \rfloor + 1)^2 < r$, donc deux éléments sont congrus modulo r :

$$m_1 = p^{i_1} N^{j_1}, m_2 = p^{i_2} N^{j_2} = m_1 + kr, (i_1, j_1) \neq (i_2, j_2).$$

$(X - a)_{m_2} = X^{m_1 + kr} - a = (X - a)_{m_1} \pmod{X^r - 1, d}$.

Prop. $m_1 = m_2$.

Fin de la preuve : N est une puissance de p , contradiction.

$\Rightarrow e = O((\log N)^{2+o(1)})$, $d = \exp(O(\log_3 N \log_4 N))$, $\tilde{O}((\log N)^4)$.

Ex : $S = \{1\}$; $e \geq d(\log N)^2/3$; Adleman-Pomerance-Rumely

Coût : $\tilde{O}(\#S)d^e(\log N)^2$.

$s \in S \subset R$.

Vérifier $(X - s)_{N^d} = X_{N^d} - s$ dans $R[X]/(X^e - r)$ pour tout

$$R = \mathbb{Z}/N\mathbb{Z}[X]/(f(X)), \deg(f) = d,$$

- D. Bernstein (29/01/03) : $e \mid N^d - 1$;

Encore plus récemment

Slide 28

- P. Mináč : rajouter de la cyclotomie.

Conclusions

On a beaucoup de réponses aux problèmes de départ. Tout dépend de ce que l'on cherche :

- facile à comprendre/implanter : AD5MR;
- rapide, même si non prouvé : Jacobi, ECPP;
- certifié : ECPP;
- disponible : ECPP (MAGMA);
- polynomial déterministe : AKS.

Slide 29