PETITES HAUTEURS DES POLYNOMES PAR L'ALGORITHME LLL

Abderrahmane Nitaj

18 décembre 2003

nitaj@math.unicaen.fr

http://www.math.unicaen.fr/~nitaj

Département de Mathématiques

Université de Caen, France

Contenu

Le cryptosystème de Rabin

Brigitte veut envoyer un message secret à Ali.

- Ali construit son initialisation :
  - Choisit p et q premiers, $p \equiv q \equiv 3 \pmod 4$.
  - Calcule $n = pq$.
  - p et q sont privés, n est public.
- Brigitte envoie le message :
  - prend $m \in \{0, 1, \cdots, n-1\}$.
  - Calcule $c \equiv m^2 \pmod n$.
  - envoie le message c.
  - m est secret.
- Ali procède au décodage :
  - Calcule $m_p \equiv c^{(p+1)/4} \pmod p$.
    $m_q \equiv c^{(q+1)/4} \pmod q$.
  - Calcule $m = Chinois(m_p, m_q)$.
  - Il y a des conditions nécessaires pour retrouver le message d'origine m.
- Equation : $\boxed{x^2 \equiv c \pmod n.}$

Le cryptosystème RSA

Brigitte veut envoyer un message secret à Ali.

- Ali construit son initialisation :
  - Choisit p et q premiers.
  - Calcule $n = pq$.
  - Choisit e, $\gcd(e, \phi(n)) = 1$.
  - Calcule $d \equiv 1/e \pmod{\phi(n)}$.
  - p, q et d sont privés, n et e sont publics.
- Brigitte envoie le message :
  - prend $m \in \{0, 1, \cdots, n-1\}$.
  - Calcule $c \equiv m^e \pmod{n}$.
  - envoie le message c.
  - m est secret.
- Ali procède au décodage :
  - Calcule $m \equiv c^d \pmod{n}$.
- Equation : $\boxed{x^e \equiv c \pmod{n}.}$

Le problème de la factorisation

On veut déterminer un facteur m de n.

- Données :
  - n un entier à factoriser.
  - u, v et d deux entiers.
- But :
  - Trouver deux entiers s et Q tels que $(u+vs)^dQ = n$.
- Equation : $\boxed{(u+vx)^dQ = n.}$

La racine modulaire d'un polynôme

On veut résoudre $h(x_0) \equiv 0 \pmod{n}$.

- Données :
  - $h = h_d x^d + \cdots + h_0 \in \mathbb{Z}[x]$ un polynôme.
  - $d = \deg(h) \geq 1$.
- But :
  - Trouver un enrtier x_0 tel que $h(x_0) \equiv 0 \pmod{n}$.
- Equation : $\boxed{h(x) \equiv 0 \pmod{n}.}$

La norme d'un polynôme

$f(x) = f_d x^d + \cdots + f_1 x + f_0 \in \mathbb{R}[x]$.

- la norme de f est :

$$||f|| = \sqrt{\sum f_i^2}.$$

- Si $X \in \mathbb{R}$, alors :
  - $f(Xx) = f_d X^d x^d + \cdots + f_1 X x + f_0$.
  - La norme de $f(Xx)$ est

$$||f(Xx)|| = \sqrt{\sum f_i^2 X^{2i}}.$$

La racine modulaire d'un polynôme : Le théorème

On veut résoudre $h(x_0) \equiv 0 \pmod{n}$.

- Données :
  - $h = h_d x^d + \cdots + h_0 \in \mathbb{Z}[x]$ un polynôme.
  - $d = \deg(h) \geq 1$.
  - Une borne $X > 0$.
- But :
  - Trouver un entier $x_0 \in \mathbb{Z}$ tel que :
    - $h(x_0) \equiv 0 \pmod{n}$.
    - $|x_0| < X$.
- Théorème : (Håstad, Coppersmith, Howgrave-Graham)
  - $\phi(x) = \phi_w x^w + \cdots + \phi_0 \in \mathbb{R}[x]$,
  - $\deg(\phi) = w \geq 1$.
  - Si
    - $\phi(x_0) \in \mathbb{Z}$,
    - $|\phi(Xx_0)| < 1/\sqrt{w}$,

    alors $\phi(x_0) = 0$.

La racine modulaire d'un polynôme : La preuve

On veut montrer que $\phi(x_0) = 0$.

- On a

$$
\begin{aligned}
|\phi(x_0)|^2 &= \left|\sum \phi_i x_0^i\right|^2 = \left|\sum \phi_i X^i \left(\frac{x_0}{X}\right)^i\right|^2 \\
&\leq \left(\sum \left|\phi_i X^i \left(\frac{x_0}{X}\right)^i\right|\right)^2 \\
&\leq w \sum \left(\phi_i X^i\right)^2 \leq 1.
\end{aligned}
$$

- Puisque $\phi(x_0) \in \mathbb{Z}$, alors $\phi(x_0) = 0$

La racine modulaire : La méthode de Håstad

On veut résoudre $h(x_0) \equiv 0 \pmod{n}$.

- Données :
  - $h = h_d x^d + \cdots + h_0 \in \mathbb{Z}[x]$ un polynôme.
  - $d = \deg(h) \geq 1$.
  - Une borne $X > 0$.
- But :
  - Trouver un entier $x_0 \in \mathbb{Z}$ tel que :
    - $h(x_0) \equiv 0 \pmod{n}$.
    - $|x_0| < X$.
- Poser : (Håstad)
  - $g(x) = Xx, \qquad f(x) = \frac{h(Xx)}{n}$.
  - $L = \mathbb{Z} + \mathbb{Z}g + \mathbb{Z}g^2 + \cdots + \mathbb{Z}g^{d-1} + \mathbb{Z}f$.
    - $\dim(L) = w = d + 1$.
- Appliquer l'algorithme LLL au réseau L.
- Si LLL produit $\phi(x) \in \mathbb{R}[x]$, avec $||\phi(x)|| < 1/\sqrt{w}$, alors $\phi(x_0/X) = 0$.

La racine modulaire : La méthode de Håstad (Analyse 1/2)

$L = \mathbb{Z} + \mathbb{Z}g + \mathbb{Z}g^2 + \cdots + \mathbb{Z}g^{d-1} + \mathbb{Z}f.$

- Caractéristiques de L:
  - $\dim(L) = w = d + 1.$
  - $\det(L) = h_d X^{w(w-1)/2}/n$.
- Appliquer l'algorithme LLL à L :
  - Nouvelle base $(b_1(x), b_2(x), \cdots, b_w(x))$, avec
    - $||b_1(x)|| \leq 2^{(w-1)/4} \det(L)^{1/w}.$
- Si $\det(L) < 2^{-w(w-1)/4} w^{-w/2}$, alors :
  - $X < (n/h_d)^{2/(w(w-1))} w^{-1/(w-1)}/\sqrt{2}$.
  - $||b_1(x)|| < 1/\sqrt{w}$.

$\Longrightarrow$ prendre $\phi = b_1$ et résoudre $\phi(x_0/X) = 0$ avec $x_0 \in \mathbb{Z}$.

La racine modulaire : La méthode de Håstad (Analyse 2/2)

$L = \mathbb{Z} + \mathbb{Z}g + \mathbb{Z}g^2 + \cdots + \mathbb{Z}g^{d-1} + \mathbb{Z}f.$

- Caractéristiques de L:
  - $\dim(L) = w = d + 1.$
  - $\det(L) = h_d X^{w(w-1)/2}/n$.
- Appliquer l'algorithme LLL à L :
  $\Longrightarrow$
  - Nouvelle base $(b_1(x), b_2(x), \cdots, b_w(x))$, avec
  - $||b_1(x)|| \leq 2^{(w-1)/4} \det(L)^{1/w}$.
  - Chercher un polynôme court $\phi(x)$ et résoudre $\phi(x_0/X)$ dans $\mathbb{Z}$.

Si on veut $\phi = b_1$, alors :

- $X < (n/h_d)^{2/(w(w-1))} w^{-1/(w-1)}/\sqrt{2}$.
  $\Longrightarrow$
  - $X < \gamma_d (n/h_d)^{2/(d(d+1))}$.
  - $\frac{1}{2\sqrt{2}} \leq \gamma_d < \frac{1}{\sqrt{2}}$.

La borne X est donc assez petite: $X = O\left((n/h_d)^{2/(d(d+1))}\right)$.

La racine modulaire : La méthode de Håstad (Exemple 1/2)

$n = 10^{20} + 39, \qquad c = 7399961 \times 10^{10} + 1369, \qquad h(x) = x^2 - c$

- Caractéristiques :
  - $d = 2, \qquad h_d = 1.$
  - $X \geq 1.$
- Poser :
  - $g(x) = Xx.$
  - $f(x) = \frac{h(Xx)}{n}.$
  - $L = \mathbb{Z} + \mathbb{Z}g + \mathbb{Z}f.$
    - $\dim(L) = w = d + 1 = 3.$
    - $\det(L) = X^3/n.$
- Appliquer LLL

  $\Longrightarrow$
  - Nouvelle base $(b_1(x), b_2(x), b_3(x))$.
  - Chercher un polynôme court $\phi(x)$ et résoudre $\phi(x_0/X)$ dans $\mathbb{Z}$.

La racine modulaire : La méthode de Håstad (Exemple 2/2)

$n = 10^{20} + 39, \qquad c = 7399961 \times 10^{10} + 1369, \qquad h(x) = x^2 - c$

- Si on veut prendre $\phi = b_1$:
  $\Longrightarrow$
  - $X = 10^6 \leq (n/h_d)^{2/(w(w-1))} w^{-1/(w-1)}/\sqrt{2} \approx 1.89 \times 10^6$,
    $\Longrightarrow$ Pas de solution avec b_1.

- Si on connait une partie $X_0 = 10^{15}$ d'une solution :
  - Remplacer x par $X_0 + x$ dans h.
  - Appliquer de nouveau LLL.
    $\Longrightarrow$
    - $\phi = b_1$ avec $n\phi(x/X) = nb_1(x/X) = 68448557 + 39x - 50000x^2$.
    - $\phi(x_0/X) = 0, x_0 \in \mathbb{Z} \qquad \Longrightarrow \qquad x_0 = 37$.
    - Vérification : $h(X_0 + x_0) \equiv 0 \pmod{n}$.

La racine modulaire : La méthode de Coppersmith 1/2

On veut résoudre $h(x_0) \equiv 0 \pmod{n}$.

- Données :
  - $h = h_d x^d + \cdots + h_0 \in \mathbb{Z}[x]$ un polynôme.
  - $d = \deg(h) \geq 1$.
  - Une borne $X \geq 1$.
- But :
  - Trouver un entier $x_0 \in \mathbb{Z}$ tel que :
    - $h(x_0) \equiv 0 \pmod{n}$.
    - $|x_0| < X$.
- Poser : (Coopersmith)
  - $g(x) = Xx, \qquad f(x) = \frac{h(Xx)}{n}$.
  - $m \geq 2$.

La racine modulaire : La méthode de Coppersmith 2/2

$$\begin{aligned} L &= \mathbb{Z} + \mathbb{Z}g + \mathbb{Z}g^2 + \cdots + \mathbb{Z}g^{d-1} \\ &+ \mathbb{Z}f + \mathbb{Z}gf + \mathbb{Z}g^2 f + \cdots + \mathbb{Z}g^{d-1} f \\ &+ \cdots \\ &+ \mathbb{Z}f^{m-1} + \mathbb{Z}gf^{m-1} + \mathbb{Z}g^2 f^{m-1} + \cdots + \mathbb{Z}g^{d-1} f^{m-1}. \end{aligned}$$

- Caractéristiques de L :
  - $\dim(L) = w = dm$..
  - $\det(L) = X^{w(w-1)/2} \left(\frac{h_d}{n}\right)^{w(m-1)/2}$.
- Appliquer l'algorithme LLL à L:
  - Nouvelle base $(b_1(x), b_2(x), \cdots, b_w(x))$, avec :
    - $||b_1(x)|| \leq 2^{(w-1)/4} \det(L)^{1/w}$.
    - Chercher un polynôme court $\phi(x)$ et résoudre $\phi(x_0/X)$ dans $\mathbb{Z}$.

La racine modulaire : La méthode de Coppermith (Analyse)

$L = \mathbb{Z} + \mathbb{Z}g + \mathbb{Z}g^2 + \cdots + \mathbb{Z}g^{d-1}f^{m-1}.$

Si $\det(L) < 2^{-w(w-1)/4}w^{-w/2}$, alors :

- $X < (n/h_d)^{(m-1)/(w-1)}\, w^{-1/(w-1)}/\sqrt{2}$.
- $||b_1(x)|| < 1/\sqrt{w}$.

$\Longrightarrow$ prendre $\phi = b_1$ et résoudre $\phi(x_0/X) = 0$ avec $x_0 \in \mathbb{Z}$.

- Si on veut $\phi = b_1$:
  $\Longrightarrow$
  - $X < \gamma_w\,(n/h_d)^{1/d-\varepsilon}$,
  - $\frac{1}{2\sqrt{2}} \le \gamma_w < \frac{1}{\sqrt{2}}$.
  - $\varepsilon = \frac{d-1}{d(dm-1)}$
    Avec $\lim_{m\to\infty} \varepsilon = 0$.

La borne X est : $X = O\left((n/h_d)^{1/d-\varepsilon}\right).$

La méthode de Coopersmith (Exemple 1/2)

$n = 10^{20} + 39, \qquad c = 7399961 \times 10^{10} + 1369, \qquad h(x) = x^2 - c$

- Caractéristiques :
  - $d = 2, \qquad h_d = 1.$
  - $X \geq 1.$
- Poser :
  - $g(x) = Xx.$
  - $f(x) = \frac{h(Xx)}{n}.$
  - $m = 3.$
  - $L = \mathbb{Z} + \mathbb{Z}g + \mathbb{Z}f + \mathbb{Z}fg + \mathbb{Z}f^2 + \mathbb{Z}gf^2.$
    - $\dim(L) = w = dm = 6.$
    - $\det(L) = X^{w(w-1)/2} n^{-w(m-1)/2}.$
- Appliquer LLL

  $\Longrightarrow$
  - Nouvelle base $(b_1(x), \cdots, b_6(x))$.
  - Chercher un vecteur court $\phi(x) \in L$, avec $||\phi(x)|| < 1/\sqrt{w}$.
  - Résoudre $\phi(x_0/X) = 0$ dans $\mathbb{Z}$.

La méthode de Coppersmith (Exemple 2/2)

$n = 10^{20} + 39, \qquad c = 7399961 \times 10^{10} + 1369, \qquad h(x) = x^2 - c$

- Si on veut prendre $\phi = b_1$:
  $\Longrightarrow$
  - $X = 10^7 \leq (n/h_d)^{(m-1)/(w-1)}\, w^{-1/(w-1)}/\sqrt{2} \approx 4.94 \times 10^7$
    $\Longrightarrow$ pas de solution avec b_1.
- Si on connait une partie $X_0 = 10^15$ d'une solution :
  - Remplacer x par $X_0 + x$ dans h.
  - Appliquer de nouveau LLL.
    $\Longrightarrow$
    - $\phi(x) = b_1(x)$ avec

$$\begin{aligned} n^2\phi(x/X) = n^2 b_1(x/X) \quad = \quad & 8542469956800237056040034227109 \\ & -230877566400006406829953976735x \\ & -173162433701306x^2 \\ & +4679999997262x^3 + 37x^4 + x^5. \end{aligned}$$

    - $\phi(x_0/X) = 0,\ x_0 \in \mathbb{Z} \quad \Longrightarrow \quad x_0 = 37.$
    - Vérification : $h(X_0 + x_0) \equiv 0 \pmod{n}$.

La hauteur d'un nombre rationnel

$$r = \frac{u}{v} \in \mathbb{Q}.$$

- La hauteur de r est :

$$Ht(r) = \max\left(|u|, |v|\right).$$

- Si $f(x) \in \mathbb{Q}$, alors :
  - $f(r) = \frac{u}{v}$.
  - La norme de $f(r)$ est

$$Ht(f(r)) = \max\left(|u|, |v|\right).$$

Exemple Rabin

Equation $x^2 \equiv c \pmod{n}$.

- Données :
  - $n,\ c \in \mathbb{N}$.
- But :
  - Trouver un enrtier x_0 tel que $x_0^2 \equiv c \pmod{n}$.
- Poser : $\psi(x) = \frac{x^2-c}{n}$.
- Hauteur : $\boxed{Ht(\psi(x) = \max\left(|x^2-c|, n\right) / \gcd(x^2-c, n).}$
- Déterminer $x_0 \in \mathbb{Z}$ tel que $Ht\left(\psi(x_0)\right) < \max\left(|x_0^2 - c|, n\right)$.

$\Longrightarrow$

- $\boxed{\psi(x_0) \text{ a une petite hauteur.}}$

Exemple RSA

Equation $x^e \equiv c \pmod{n}$.

- Données :
  - $n = pq \in \mathbb{N}$.
  - $c, e \in \mathbb{N}$.
  - $\gcd(e, \phi(n)) = 1$.
- But :
  - Trouver un enrtier x_0 tel que $x_0^e \equiv c \pmod{n}$.
- Poser : $\psi(x) = \frac{x^e - c}{n}$.
- Hauteur : $\boxed{Ht(\psi(x) = \max\left(|x^e - c|, n\right) / \gcd(x^e - c, n).}$
- Déterminer $x_0 \in \mathbb{Z}$ tel que $Ht\left(\psi(x_0)\right) < \max\left(|x_0^e - c|, n\right)$.

$\Longrightarrow$

- $\psi(x_0)$ a une petite hauteur.

Exemple factorisation

Equation $(u+vx)^d Q = n$.

- Données :
  - $n,\ u,\ v,\ d \in \mathbb{N}$.
- But :
  - Trouver deux entiers x_0 et Q tels que $(u+vx)^d Q = n$.
- Poser : $\psi(x) = \frac{(u+vx)^d}{n}$.
- Hauteur : $\boxed{Ht(\psi(x) = \max\left(|(u+vx)^d|, n\right) / \gcd((u+vx)^d, n).}$
- Déterminer $x_0 \in \mathbb{Z}$ tel que $Ht\left(\psi(x_0)\right) < \max\left(|(u+vx)^d|, n\right)$.

$\Longrightarrow$

- $\boxed{\psi(x_0) \text{ a une petite hauteur.}}$

Exemple racine modulaire

Equation $h(x) \equiv 0 \pmod{n}$.

- Données :
  - $n \in \mathbb{N}$.
  - $h(x) = h_d x^d + \cdots + h_0 \in \mathbb{Z}[x]$.
  - $d \geq 1$.
- But :
  - Trouver un entier x_0 tel que $h(x_0) \equiv 0 \pmod{n}$.
- Poser : $\psi(x) = \frac{h(x)}{n}$.
- Hauteur : $\boxed{Ht(\psi(x)) = \max\left(|h(x)|, n\right) / \gcd(h(x), n).}$
- Déterminer $x_0 \in \mathbb{Z}$ tel que $Ht\left(\psi(x_0)\right) < \max\left(|h(x)|, n\right)$.

$\Longrightarrow$

- $\boxed{\psi(x_0) \text{ a une petite hauteur.}}$

Petites hauteurs

Deux polynômes f et g.

- Données :
  - $d \geq 1$.
  - $f(x) = f_d x^d + \cdots + h_0 \in \mathbb{Q}[x]$.
  - $g(x) = g_1 x + g_0 \in \mathbb{Q}[x]$.
- But :
  - Trouver un rationnel $x_0 \in \mathbb{Q}$ tel que
    - $Ht\,(f(x_0))$ est petit.
    - $Ht\,(g(x_0))$ est petit.

$\Longrightarrow$

- $f(x_0)$ et $g(x_0)$ ont des petites hauteurs.

Le réseau

D.J.Bernstein.

- Données :
  - $d \in \mathbb{N},\ d \geq 1$.
  - $k \in \mathbb{N},\ k \geq 1$.
  - $m \in \mathbb{N},\ m \geq dk + 1$.
  - $f(x) = f_d x^d + \cdots + h_0 \in \mathbb{Q}[x]$.
  - $g(x) = g_1 x + g_0 \in \mathbb{Q}[x]$.
- Le réseau :

$$
\begin{aligned}
L = L(f,g) \quad = \quad & \mathbb{Z} + \mathbb{Z}g + \mathbb{Z}g^2 + \cdots + \mathbb{Z}g^{d-1} \\
& + \mathbb{Z}f + \mathbb{Z}gf + \mathbb{Z}g^2 f + \cdots + \mathbb{Z}g^{d-1} f \\
& + \cdots \\
& + \mathbb{Z}f^{k-1} + \mathbb{Z}gf^{k-1} + \mathbb{Z}g^2 f^{k-1} + \cdots + \mathbb{Z}g^{d-1} f^{k-1} \\
& + \mathbb{Z}f^k + \mathbb{Z}gf^k + \mathbb{Z}g^2 f^k + \cdots + \mathbb{Z}g^{m-dk-1} f^k.
\end{aligned}
$$

$\Longrightarrow$

- $\dim(L) = m$.
- $\det(L) = g_1^{m(m-1)/2} \left(g_1^d / f_d\right)^{dk(k+1)/2 - mk}$.

Le théorème de Bernstein

Deux polynômes f et g.

- Données :
  - $d \in \mathbb{N},\ d \geq 1$.
  - $k \in \mathbb{N},\ k \geq 1$.
  - $m \in \mathbb{N},\ m \geq dk + 1$.
  - $f(x) = f_d x^d + \cdots + h_0 \in \mathbb{Q}[x]$.
  - $g(x) = g_1 x + g_0 \in \mathbb{Q}[x]$.
  - $r \in \mathbb{Q}$.
  - $R(x) = r^{m-1}x^{m-1} + r^{m-2}x^{m-2} \cdots + 1 \in \mathbb{Q}[x]$.
  - $M = \max(d-1, m-kd-1)$.
- Théorème (Bernstein) :
  - $\psi(x) = \psi_{m-1}x^{m-1} + \cdots + \psi_0 \in \mathbb{Q}[x]$.
  - Si :
    - $\psi(x) \in L(f,g)$,
    - $(denom(f(r)))^k\,(denom(g(r)))^M < ||R||^{-1}||\psi||^{-1}$,

    alors $\psi(r) = 0$.

Le théorème de Bernstein : La preuve

On veut montrer que $\psi(r) = 0$.

- $\psi(r) = \psi_{m-1} r^{m-1} + \cdots + \psi_0$.
- On a $|\psi(r)|^2 = \left(\sum \psi_i^2\right) \left(\sum r^{2i}\right)$.

$\Longrightarrow$

- $|\psi(r)| \leq ||R||||\psi|| < (denom(f(r)))^{-k} (denom(g(r)))^{-M}$
- Puisque $\psi(r) \in L(f,g) = \mathbb{Z} + \mathbb{Z}g + \cdots + \mathbb{Z}g^{m-ddk-1} f^k$, alors $\psi(r) \in (denom(f(r)))^{-k} (denom(g(r)))^{-M} \mathbb{Z}$.

$\Longrightarrow \psi(r) = 0$.

Travaux précédents

Le théorème de Bernstein peut généraliser.

- Racines de $\psi(r) = \frac{r+uw}{n}$.
  $\Longrightarrow$
  - Lenstra,
  - Rivest,
  - Shamir,
  - Coppersmith
- Racines de $\psi(r) = \frac{h(r)}{n}$.
  $\Longrightarrow$
  - Håstad,
  - Girault, Toffin, Vallée,
  - Coppersmith,
  - Howgrave-Graham,
  - Boneh.
- Racines de $\psi(r) = \frac{(r+u)^d}{n}$.
  $\Longrightarrow$
  - Boneh,
  - Durfee,
  - Howgrave-Graham.

Références

3 articles fondateurs.

- J. Håstad :
  - Solving Simultaneous Modular Equations of Low Degree, SIAM Journal on Computing,
    1988, Vol. 17, No 2, pp 336-341.
- D. Coppersmith :
  - Small solutions to polynomial equations, and low exponent RSA vulnerabilities.
    J. Cryptology 10, No.4, 233-260 (1997).
- D.J. Bernstein :
  - Reducing lattice bases to find small-height values of univariate polynomials.
    `http://cr.yp.to/papers.html#smallheight.`