Sélection polynomiale non linéaire pour NFS

Paul Zimmermann

November 15, 2012

Le problème

Entrées : entier N à factoriser, entiers d_1 et d_2

Sorties : polynômes $f_1, f_2 \in \mathbb{Z}[x]$ irréductibles de degrés d_1 et d_2, avec racine commune $m \in \mathbb{Z}$ modulo N

Équivaut à $\mathrm{Res}(f_1, f_2) = 0 \bmod N$.

On veut les coefficients de f_1, f_2 aussi petits que possible.

Exemple : RSA-768

$$
\begin{aligned}
N &= 123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341373794080665351419597459856902143413\\
f_1(x) &= 265482057982680x^6\\
&+ 1276509360768321888x^5\\
&- 5006815697800138351796828x^4\\
&- 464778544717278542717267745 0x^3\\
&+ 65254372619359893971096673718947 85x^2\\
&- 1818577935208859435672601886243480 3054x\\
&- 2775652667915438819952161997138011 03343120\\
f_2(x) &= 346610035504925018514458 29x\\
&- 1291187456580021223163547791574810881
\end{aligned}
$$

Impact sur le temps de crible.

Exemple : RSA-512, factorisé en 1999.

2006 : Thorsten Kleinjung trouve des polynômes 32% meilleurs

2009 : Alexander Kruppa trouve des polynômes 46% meilleurs

2010 : Thorsten Kleinjung trouve des polynômes 77% meilleurs

2012 : Jayson King trouve des polynômes 100% meilleurs

Notations

Si $d_2 = 1$, on notera $d = d_1$, $f = f_1$ et $g = f_2 = px - m$.

La racine commune est alors m/p mod N.

On notera alors $f = a_d x^d + a_{d-1} x^{d-1} \cdots + a_1 x + a_0$.

On dira qu'un algorithme est *optimal* quand $\mathrm{Res}(f_1, f_2) = \pm N$.

Skewness

Soit $f(x) = a_d x^d + a_{d-1} x^{d-1} \cdots + a_1 x + a_0$.

Pour une norme donnée, par exemple

$$N(f) := \sqrt{a_d^2 + a_{d-1}^2 + \cdots + a_1^2 + a_0^2},$$

et pour $s > 0$, on peut définir

$$N_s(f) := N(s^{-d/2} f(sx)).$$

La *skewness* de f est la valeur de s donnant le minimum de $N_s(f)$.
Exemple : pour le polynôme f_1 de RSA-768, avec la norme ci-dessus, on a $s \approx 36106.76$ avec $N_s(f) \approx 2.6 \cdot 10^{29}$.

État de l'art

- Murphy 1999 : $d_2 = 1$, définit *size, root properties*, Murphy E
- Montgomery 1999 : cas $d_1 = d_2 = 2$, algorithme optimal
- Kleinjung 2006 : $d_2 = 1$, réduit a_{d-2}
- Kleinjung 2008 : $d_2 = 1$, autre astuce pour réduire a_{d-2}
- Williams 2010 : cas $d_1 = d_2 = 3$, $\mathrm{Res}(f_1, f_2) = O(N^{4/3})$
- Prest, Z., 2011 : cas $d_1 = d_2 = 3$, $\mathrm{Res}(f_1, f_2) = O(N^{5/4})$

Problèmes ouverts

Pour f de degré 6 et g linéaire, « contrôler » le coefficient de degré 3 de f

Pour $d_1 = d_2 = 3$, trouver deux polynômes « optimaux »

Idem pour $d_1 = 5$ et $d_2 = 2$...

Montgomery "two quadratics"

- choisir $p < N^{1/2}$ premier tel que N est un carré modulo p
- soit c tel que $N = c^2 \bmod p$ avec $|c - N^{1/2}| \leq p/2$
- soit $s = 1/c \bmod p$, $c_2 = (c^2 - N)/p$, et $t = c_2 s \bmod p$
- réduire (LLL) les vecteurs

$$a' = \begin{pmatrix} c \\ -p \\ 0 \end{pmatrix}, \qquad b' = \begin{pmatrix} (ct - c_2)/p \\ -t \\ 1 \end{pmatrix}$$

- si les vecteurs courts obtenus sont

$$a = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}, \qquad b = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix},$$

considérer les polynômes $f = a_2 x^2 + a_1 x + a_0$ et $g = b_2 x^2 + b_1 x + b_0$.

Montgomery "two quadratics"

Les vecteurs a' et b' sont tous les deux orthogonaux à :

$$c = \begin{pmatrix} p \\ c \\ (c^2 - N)/p \end{pmatrix} = p \begin{pmatrix} 1 \\ m \\ m^2 \end{pmatrix}$$

avec $m = c/p \bmod N$.
Donc les vecteurs a et b sont aussi orthogonaux à c.
Si L est la matrice formée avec les vecteurs a et b, alors le volume du réseau est $V = \det(L^t L)^{1/2} = \sqrt{p^2 + c^2 + c_2^2}$. Les vecteurs courts ont une norme de l'ordre de $V^{1/2}$.
On a $c_2 = (c^2 - N)/p = (c + N^{1/2})(c - N^{1/2})/p = O(N^{1/2})$,
donc les vecteurs courts ont une norme $O(N^{1/4})$.
Le résultant de $a_2x^2 + a_1x + a_0$ et de $b_2x^2 + b_1x + b_0$ est :

$$b2^2\,a0^2 - 2\,b2\,a0\,a2\,b0 + a2^2\,b0^2 - b1\,b2\,a1\,a0 - b1\,a1\,a2\,b0 + a2\,b1^2\,a0 + b0\,b2\,a1^2$$

donc on aura $\mathrm{Res}(f, g) = O(N)$.

Cas général

$f = a_{d_1} x^{d_1} + \cdots + a_0$

$g = b_{d_2} x^{d_2} + \cdots + b_0$

$\mathrm{Res}(f, g)$ est un polynôme homogène de degré total $d_1 + d_2$ en les a_i et b_j, de degré total d_2 en les a_i, de degré total d_1 en les b_j.

Exemple pour $d_1 = 3$, $d_2 = 2$:

$$\begin{aligned} & b_2 a_2^2 b_0^2 - 2 b_2^2 a_2 b_0 a_0 - a_2 b_0^2 a_3 b_1 + b_2^3 a_0^2 + 3 b_2 a_0 a_3 b_1 b_0 \\ & - b_1 b_2 a_1 a_2 b_0 - b_1 b_2^2 a_1 a_0 + b_1^2 a_1 a_3 b_0 + b_2 a_2 b_1^2 a_0 - a_3 b_1^3 a_0 \\ & + b_0 b_2^2 a_1^2 - 2 b_2 a_1 a_3 b_0^2 + a_3^2 b_0^3 \end{aligned}$$

Cas $d_1 = d_2 = d$

Le résultant de f et g est un polynôme de degré $2d$ en les a_i et b_j.

Considérons tous les $|a_i|, |b_j| < N^{1/(2d)}$, soit $\Omega(N^{1+1/d})$ valeurs

On espère $\Omega(N^{1/d})$ résultants égaux à N

Pour $N = 1009$, $d = 3$, on trouve 576 résultants égaux à $\pm N$ avec $|a_i|, |b_j| \leq 3$

Avec $0 \leq a_i, b_j \leq (2N)^{1/(2d)}$, sans compter les symétries, on trouve 2 solutions pour $N = 1009$, 8 solutions pour $N = 10007$, 2 solutions pour $N = 100003$.

Progressions géométriques (Montgomery, 1993)

$$c_0 = c, c_1 = cm \bmod N, ..., c_d = cm^d \bmod N$$

$$M = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \ddots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ Kc_0 & Kc_1 & \cdots & Kc_{d-1} & Kc_d \end{pmatrix}$$

Pour K assez grand, si on réduit M par LLL, on obtiendra des vecteurs courts $[a_0, a_1, \ldots, a_{d-1}, a_d, 0]^t$.
Donc $a_0c_0 + \cdots + a_dc_d = 0$, et $f = a_dx^d + \cdots + a_0$ admet m comme racine modulo N.

$$\det(M^t M) = 1 + K^2(c_0^2 + \cdots + c_d^2)$$

Vecteurs courts : $(Kc)^{1/(d+1)}$.

$K \gg (Kc)^{1/(d+1)} \Longrightarrow K \gg c^{1/d}$.

Vecteurs courts : $c^{1/d}$, résultant c^2.

Pour avoir un résultant $O(N)$, il faut donc trouver une progression géométrique en $O(N^{1/2})$, indépendamment de d.

Algorithme Prest-Z. (2011)

Permet de trouver deux polynômes de degré d ($d = 3$ ici).

Soit c entier proche de $N^{1/3}$, et S entier :

$$L = \begin{pmatrix} c & c^2 & c^3 - N \\ S & 0 & 0 \\ 0 & S^2 & 0 \\ 0 & 0 & S^3 \end{pmatrix}$$

Soit $[-a_0, Sa_1, S^2a_2, S^3a_3]^t$ un vecteur court du réseau engendré par L. Alors $f = a_3x^3 + a_2x^2 + a_1x + a_0$ admet c comme racine modulo N.

Pour $S \approx N^{1/12}$, le "coefficient médian" de f vaut $O(^{5/24})$, ce qui donne un résultant $O(N^{5/4})$.

Que peut-on espérer ?

Stage de Nathan Lecoanet, juin-juillet 2012.
Soit N à factoriser, ayant n bits.
Soit f_1 de degré d_1 avec des coefficients de s_1 bits.
Soit f_2 de degré d_2 avec des coefficients de s_2 bits.
$\mathrm{Res}(f_1, f_2)$ a $d_1 s_2 + d_2 s_1$ bits :

$$d_1 s_2 + d_2 s_1 = n$$

Le nombre de tels polynômes doit être au moins 2^n :

$$(d_1 + 1)s_1 + (d_2 + 1)s_2 \geq n$$

On veut avoir des normes aussi équilibrées que possible :

$$s_1 + 32d_1 - 32 = s_2 + 32d_2$$

Pour $n = 768$:

$d_1 + d_2$	$s_1 + s_2$	$s_1 + 32d_1 - 32$	$s_2 + 32d_2$	$(d_1 + 1)s_1 + (d_2 + 1)s_2$
$6 + 1$	$77 + 116$	**237**	148	771
$5 + 2$	$64 + 129$	192	**193**	771
$2 + 5$	$129 + 64$	161	**227**	771
$4 + 3$	$110 + 110$	**206**	**206**	990
$3 + 4$	$137 + 73$	**201**	**201**	913
$3 + 3$	$144 + 112$	**208**	**208**	1024

$d_1 = 6$, $d_2 = 1$ (polynômes du record) : 1.72s/r
$d_1 = 6$, $d_2 = 1$ ($s_1 = 77$, $s_2 = 116$) : 0.85s/r
$d_1 = 5$, $d_2 = 2$ ($s_1 = 64$, $s_2 = 129$) : 0.24s/r
$d_1 = 2$, $d_2 = 5$ ($s_1 = 129$, $s_2 = 64$) : 0.25s/r
$d_1 = 4$, $d_2 = 3$ ($s_1 = 110$, $s_2 = 110$) : 2.3s/r
$d_1 = 3$, $d_2 = 4$ ($s_1 = 137$, $s_2 = 73$) : 1.14s/r
$d_1 = 3$, $d_2 = 3$ ($s_1 = 144$, $s_2 = 112$) : 7.3s/r

Algorithme de Kleinjung (2008)

Lemme. Si $N \equiv a_d m^d \bmod \ell$, alors on peut décomposer

$$N = a_d m^d + a_{d-1} m^{d-1} \ell + \cdots + a_2 m^2 \ell^{d-2} + a_1 m \ell^{d-1} + a_0 \ell^d,$$

avec $|a_i| < m + \ell$ pour $i < d$.

Soit $r_d = N$ et $r_i = (r_{i+1} - a_{i+1} m^{i+1})/\ell$.

On choisit pour a_i l'entier le plus proche de r_i/m^i tel que $r_i - a_i m^i$ soit divisible par ℓ.

a_i entier le plus proche de r_i/m^i : $|r_i - a_i m^i| \leq m^i/2$ donc $|a_{i-1}| \leq m/2$.

$r_i - a_i m^i$ divisible par ℓ : ajoute au pire ℓ à a_i.

Cherchons $N = m^d + a_{d-2}m^{d-2}\ell^2 + \cdots + a_1 m\ell^{d-1} + a_0\ell^d$.

$N \equiv m^d \bmod \ell^2$

On prend $\ell = p_1 p_2$ avec $P \leq p_1, p_2 \leq 2P$

On veut donc $N \equiv m^d \bmod p_1^2$ et $N \equiv m^d \bmod p_2^2$

Algorithme de Kleinjung (2008)

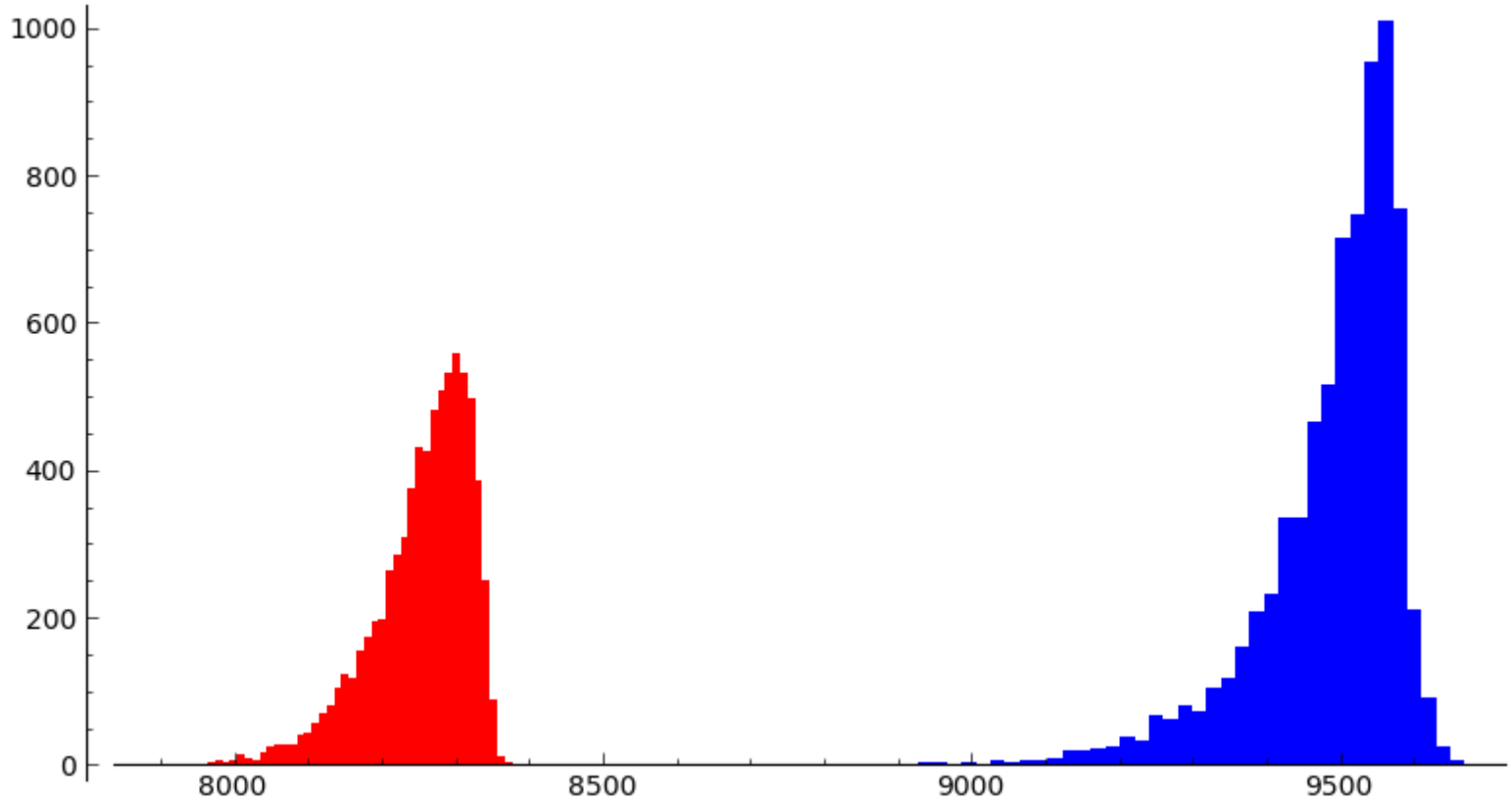
Soit $m = \lfloor N^{1/d} \rceil$.

Pour chaque premier $p \in [P, 2P]$
  pour chaque racine i de $N \equiv (m+i)^d \bmod p^2$
    ajouter (p, i) dans une table de hachage indexée par i

Chaque collision (p_1, i), (p_2, i) donne $N \equiv (m+i)^d \bmod \ell^2$ avec $\ell = p_1 p_2$

Le coefficient a_{d-2} est borné par $dm/P^2 + \ell$ au lieu de $m + \ell$

Normes de 7482 polynômes trouvés pour RSA-896 avec l'algorithme de Kleinjung (2008) et $P = 10^7$:



Projections pour RSA-896 ($d = 6$)

Étant donné a_6, on note $m_0 = (N/a_6)^{1/6}$

L'algorithme de Kleinjung (2008) donne en théorie $a_4 \approx 24 m_0/P^2$ (en pratique plutôt $0.84 m_0/P^2$)

Si la *skewness* optimale est donnée par $a_6 - a_3$, alors avec K collisions on peut espérer $a_3 \approx m_0/K$ (en pratique $0.3 m_0/K$)

Pour éviter que le coefficient a_2 soit trop grand, il faut que la *skewness* soit plus grande que K.

K	a_6 max	P	$\log a_3$
$1e3$	$1.7e28$	$1.4e3$	84.5
$1e4$	$6.3e24$	$1.4e4$	83.5
$1e5$	$2.4e21$	$1.4e5$	82.5
$1e6$	$8.8e17$	$1.4e6$	81.6
$1e7$	$3.3e14$	$1.4e7$	80.6
$1e8$	$1.2e11$	$1.4e8$	79.6
$1e9$	$4.6e7$	$1.4e9$	78.6