Calculs de logarithmes discrets dans $\mathbb{F}_{p^n}$ avec le crible de corps de nombres

Aurore Guillevic

Inria Nancy, Loria, CNRS, Université de Lorraine

12 février 2019
Séminaire d'algèbre et théorie des nombres de Besançon
Travaux avec Shashank Singh, IISER Bhopal, Inde

Calculs de logarithmes discrets

Notation : p nombre premier, $q = p^n$, $n > 0$ entier.

Logarithme discret

Étant donné un corps fini $\mathbb{F}_q$, un générateur g de $\mathbb{F}_q^*$, et une cible h, calculer un entier x tel que

$$g^x = h \text{ et } 0 \leqslant x \leqslant q - 1 \ .$$

Algorithmes génériques dans un groupe cyclique de cardinal r :

- Pohlig-Hellman : en parallèle dans chaque sous-groupe d'ordre premier
- Shanks en temps et mémoire $O(\sqrt{r})$
- Pollard-ρ en temps $O(\sqrt{r})$ et mémoire $O(\log r)$

Crible de corps de nombres

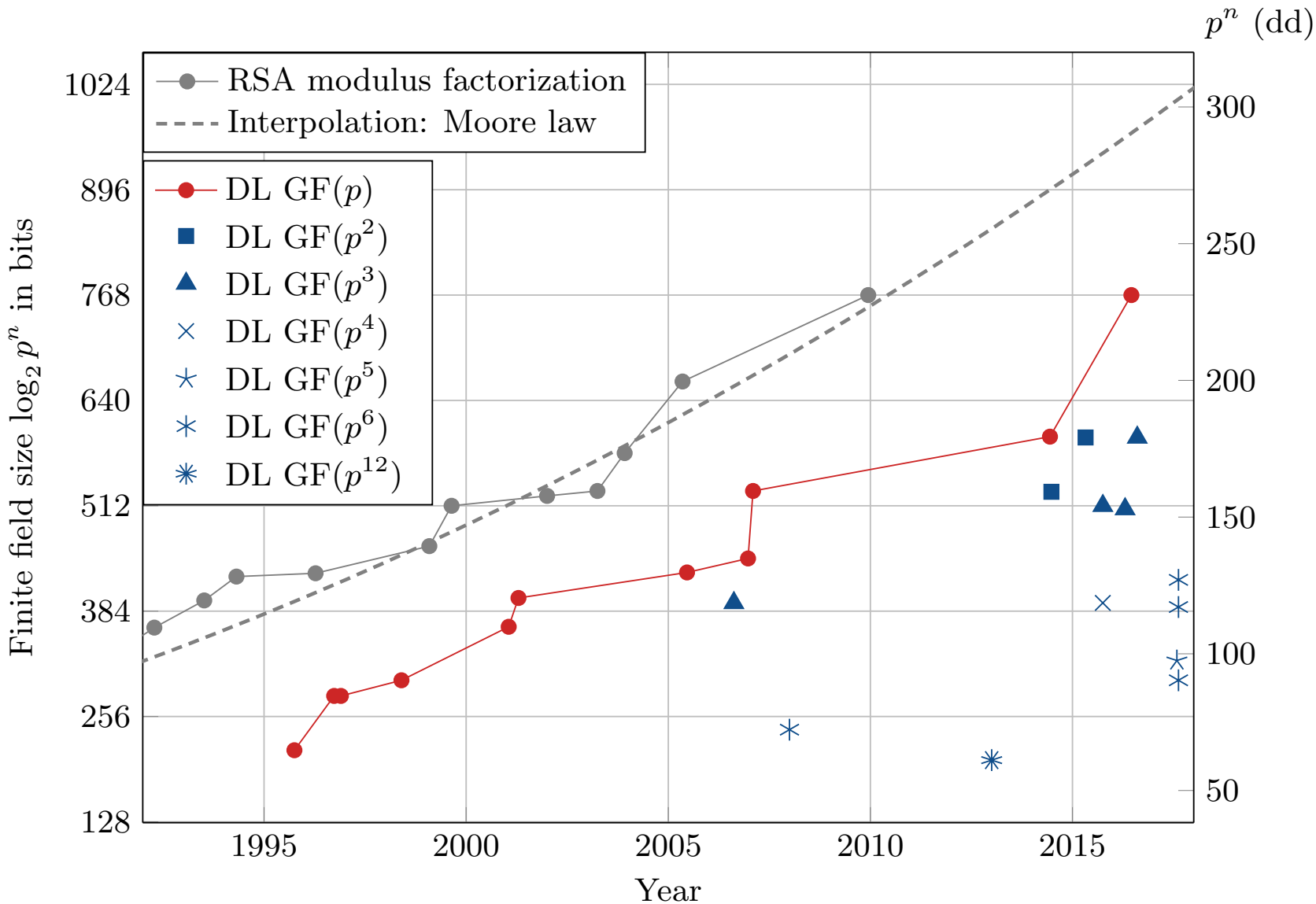
Number Field Sieve (NFS). Algorithme pour

- factoriser de très grands nombres (plus de 100 chiffres)
- calculer des logarithmes discrets dans des corps finis $\mathbb{F}_p$, $\mathbb{F}_{p^n}$

Quelques dates :

- 1922 : Calculs d'indices (Kraitchik), tables
- 70's : Redécouverte en cryptographie (Adleman, Western–Miller)
- 1984 : Function Field Sieve pour $\mathbb{F}_{2^n}$ (Coppersmith)
- 1986 : Quadratic Sieve (Coppersmith–Odlysko–Schroeppel)
- 1993 : Number Field Sieve (Gordon)
- 2006 : $\mathbb{F}_{p^n}$ (Joux–Lercier–Smart–Vercauteren)

Records de calculs [10]



Calcul d'indices dans $\mathbb{F}_p$

base de facteurs $= \{p \text{ premier } \leqslant B\}$, B borne de friabilité

Collecte de relations

Tant que #relations $<$ #base de facteurs

$t_i \leftarrow \{1, \ldots, r-1\}$

$m \leftarrow g^{t_i} \bmod p$; relever m dans $\{1, \ldots, p-1\}$

factoriser m (sur les entiers)

si $m = \prod_{p_i \leqslant B} p_i^{e_i}$ alors

Ajouter la relation $[e_1 \ldots e_i \ldots e_I \ -t_i] = M_i$

Algèbre linéaire

Résoudre $M \cdot \vec{x} = 0$ sur $\mathbb{Z}/(p-1)\mathbb{Z}$, on a alors $x_i = \log p_i$

Descente

$e = 0$; Faire

$e = e + 1$; $m = h \cdot g^e$

jusqu'à ce que $m = \prod_{p_i \leqslant B} p_i^{e_i'}$

$\log_g h = \sum e_i' \log p_i - e$

Calcul d'indices, exemple [10]

$p = 1019$, $g = 2$, $p - 1 = 2 \times 509$

$$\begin{array}{lcl} 2^{909} & = & 2 \cdot 3^2 \cdot 5 \\ 2^{10} & = & 5 \\ 2^{848} & = & 3^3 \cdot 5 \\ 2^{960} & = & 2^2 \cdot 3 \end{array} \quad \rightarrow \quad \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 1 \\ 0 & 3 & 1 \\ 2 & 1 & 0 \end{bmatrix} \cdot \vec{x} = \begin{bmatrix} 909 \\ 10 \\ 848 \\ 960 \end{bmatrix} \bmod 1018$$

Résolution mod 2, mod 509, restes chinois :
$\log_2 2 = 1$, $\log_2 3 = 958$, $\log_2 5 = 10$.

Cible $h = 314$
$g^{372} h = 2^4 \cdot 5^2 \bmod p$
$\log_2 h = 4 + 2 \cdot 10 - 372 \bmod 1018 = 670$

Calcul d'indices

Inconvénient : c'est **très lent**. Pourquoi ?

Calcul d'indices

Inconvénient : c'est **très lent**. Pourquoi ?
Factoriser m est très lent car $m \approx p$.

Calcul d'indices

Inconvénient : c'est **très lent**. Pourquoi ?
Factoriser m est très lent car $m \approx p$.
Solution : obtenir des relations de friabilité autrement.

Calcul d'indices : complexité

Notation :

$$L_N(\alpha, c) = \exp\Big((c + o(1))(\ln N)^{\alpha}(\ln \ln N)^{1-\alpha}\Big)$$

Le temps de calcul heuristique est asymptotiquement

$$L_p(1/2, 2) = e^{(2+o(1))\sqrt{\ln p \ln \ln p}} \text{ avec } \#\mathcal{B} \approx B = L_p(1/2, 1/2) \ .$$

- Temps prépondérant : collecte de relations en $L_p(1/2, 2)$.
- Algèbre linéaire en $L_p(1/2, 3/2)$.
- Descente en $L_p(1/2, 3/2)$.

Améliorations :

Théorème (Pomerance 1987)

le temps de calcul heuristique est asymptotiquement

$$L_p(1/2, \sqrt{2}) \textit{ avec } \#\mathcal{B} \approx B = L_p(1/2, \sqrt{2}/2) \ .$$

Temps équilibré entre collecte de relations et algèbre linéaire.

Calcul d'indices : complexité

Théorème (Canfield–Erdős–Pomerance 1983)

Soit $\psi(x, y)$ *le nombre de nombres entiers naturels* $\leqslant x$ *qui soient* y*-friables. Si* $x \geq 10$ *et* $y \geq \log x$*, alors*

$$\psi(x, y) = xu^{-u(1+o(1))} \text{ avec } u = \frac{\log x}{\log y} ,$$

et $x \to \infty$ *pour la limite dans* $o(1)$*.*

Calcul d'indices : complexité

Corollaire (Probabilité de B-friabilité)

Étant donné une borne de friabilité $B = L_N(\alpha_B, \beta)$, un entier tiré aléatoirement, de taille au plus $L_N(\alpha_S, \sigma)$ avec $\alpha_B < \alpha_S$ aura une probabilité d'être B-friable de

$$\Pr[\textit{est } B\textit{-friable}] = L_N\left(\alpha_S - \alpha_B, -(\alpha_S - \alpha_B)\frac{\sigma}{\beta}\right) .$$

Outil principal pour les calculs de complexité, avec les astuces

$$L_N(\alpha_1, c_1)L_N(\alpha_2, c_2) = L_N(\max(\alpha_1, \alpha_2), c_{\{i:\ \alpha_i \geqslant \alpha_j\}})$$

$$L_N(\alpha, c_1)L_N(\alpha, c_2) = L_N(\alpha, c_1 + c_2)$$

$$L_N(\alpha, c_1)^{c_2} = L_N(\alpha, c_1 c_2)$$

Coppersmith–Odlyzko–Schroeppel 1986 : entiers de Gauss

Idée : énumérer autrement pour obtenir des relations.
Réduire les tailles de nombres à factoriser.
Si $p = 1 \bmod 4$, $\exists\ A$ t.q. $A^2 = -1 \bmod p$.
Soit $U/V \equiv A \bmod p$ et $|U|, |V| < \sqrt{p}$ (ici, $p = U^2 + V^2$).

côté algébrique	côté linéaire
$f = x^2 + 1$	$g = Vx - U$
$f(U/V) = 0 \bmod p$	$g(U/V) = 0 \bmod p$
$a - bi \in \mathbb{Z}[i]$	$aV - bU \in \mathbb{Z}$
factoriser dans $\mathbb{Z}[i]$	factoriser dans $\mathbb{Z}$
$\rightarrow$ factoriser Norme$(a - bi)$ dans $\mathbb{Z}$	
entier $a^2 + b^2 \geqslant 2\max(a, b)$	entier $\geqslant 2\max(a, b)\sqrt{p}$

Énumérer suffisamment de paires (a, b)
avec $|a|, |b| \ll \sqrt{p}$

Coppersmith–Odlyzko–Schroeppel 1986 : entiers de Gauss

côté algébrique	côté linéaire
$a - bi = \prod_{\substack{\mathfrak{p}_i \in \mathbb{Z}[i] \\ \text{idéal premier} \\ \text{Norme}(\mathfrak{p}_i) \leqslant B}} \mathfrak{p}_i^{e_i}$	$aV - bU = \prod_{\substack{q_i \in \mathbb{Z} \\ \text{premier} \\ q_i \leqslant B}} q_i^{e_i'}$

$$\begin{aligned} \rho : \mathbb{Z}[i] &\to \mathbb{Z}/p\mathbb{Z} \\ i &\mapsto U/V \end{aligned}$$

$$\rho(a - bi) = V^{-1}(aV - bU)$$

Borne de friabilité B, borne sur $|a|, |b|$: $B = L_p(1/2, 1/2)$.
Collecte de relations et algèbre linéaire : $L_p(1/2, 1)$.
Descente : $L_p(1/2, 1/2)$.

Crible de corps de nombres (NFS)

Gordon 1993 $L_p(1/3, 9^{1/3} = 2.080)$,
Schirokauer 1993 $L_p(1/3, (64/9)^{1/3} = 1.923)$

Gain de $1/2$ à $1/3$: provient la sélection polynomiale
Méthode base-m, polynômes de degré d et 1 :
$m = \lfloor p^{1/d} \rceil$
Écrire p en base m : $p = f_0 + f_1 m + \ldots + f_{d-1} m^{d-1} + f_d m^d$
$f = f_0 + f_1 x + \ldots + f_d x^d$, $g = x - m$.
Coefficients de f, g en $p^{1/d}$

Formules asymptotiques
Adapter d à la taille de p : $d \approx \delta \left(\frac{\ln p}{\ln \ln p} \right)^{1/3}$, $\delta = 3^{1/3} = 1.44$.

État de l'art de calculs de logs discrets dans $\mathbb{F}_p$

- sélection polynomiale de Joux–Lercier (Math. Comp. 2003)
  (1re selec. polynomiale qui ne s'applique pas à la factorisation)
- 2017 : Kleinjung et. al., record de calcul de 768 bits
- $L_p(1/3, 1.923)$
- améliorations depuis 1993 : absorbées dans $o(1)$

Méthode de sélection polynomiale de Joux–Lercier

Choisir $\deg f = d$, le 2e polynôme sera de degré $d-1$

1. choisir f de degré d, à petits coefficients, irréductible sur $\mathbb{Q}$, et ayant une racine r_0 mod p
2. $-r_0 + x$ est un facteur de f mod p
3. Réduire sur $\mathbb{Z}$ le réseau (avec LLL)
   chaque ligne $1 \leqslant i < d$ correspond à $x^i(x - r_0)$

$$M = \begin{bmatrix} p & 0 & \cdots & 0 \\ -r_0 & 1 & 0 & \vdots \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & -r_0 & 1 \end{bmatrix} \begin{matrix} \} 1 \text{ ligne} \\ \\ \\ \} d-1 \text{ lignes} \end{matrix} \rightarrow \mathrm{LLL}(M) = \begin{bmatrix} g_0 & g_1 & \cdots & g_{d-1} \\ & & & \\ & & * & \\ & & & \end{bmatrix}$$

4. $g = g_0 + g_1 x + \cdots + g_{d-1}x^{d-1}$, $||g||_\infty = O(p^{1/d})$ et $g(r_0) = 0$ mod p

Dernier record de calcul : $\mathbb{F}_p$ de 768 bits

Kleinjung, Diem, A. Lenstra, Priplata, Stahlke, Eurocrypt'2017.
$p = \lfloor 2^{766} \times \pi \rfloor + 62762$ premier, 768 bits, 232 chiffres :

$$12193448583342869326963419091957961095266573861542513280292736561757668709803065055845773891258608267152015472257940729358832588680364332872179947215421991481828415058004331484108696835906593468476595191083938374145678927305791623 19$$

$(p-1)/2$ premier

$$f(x) = 140x^4 + 34x^3 + 86x^2 + 5x - 55$$

$$\begin{aligned} g(x) = {} & 37086340388641614115050552391952767723193261818410009592 4x^3 \\ & - 193798131283303877856561746982939554406525593801592030967 9x^2 \\ & - 217583293626947899787577441128333027617541095004734736415x \\ & + 277260730400349522890422618473498148528706115003337935150 \end{aligned}$$

Énumération ($\sim 10^{12}$) de tous les $f(x)$ t.q. $|f_i| \leqslant 165$
$|g_i| \approx p^{1/4}$

critère d'élimination ?

L'enjeu de la sélection polynomiale

- 10% du temps total d'un record de calcul
- Quel(s) critère(s) de qualité de polynômes définir ?

L'enjeu de la sélection polynomiale

- 10% du temps total d'un record de calcul
- Quel(s) critère(s) de qualité de polynômes définir ?

Normes plus souvent B-friables que des nombres entiers de même taille

L'enjeu de la sélection polynomiale

- 10% du temps total d'un record de calcul
- Quel(s) critère(s) de qualité de polynômes définir ?

Normes plus souvent B-friables que des nombres entiers de même taille
prise de décision très rapide

L'enjeu de la sélection polynomiale

Exemple : lequel choisir

$$
\begin{aligned}
&f \\
&x^2 + 1 \\
&x^2 + 2 \\
&x^2 + 3 \\
&x^2 + 7 \\
&x^2 + 11 \\
&x^2 + 19 \\
&x^2 + 43 \\
&x^2 + 67 \\
&x^2 + 163
\end{aligned}
$$

L'enjeu de la sélection polynomiale

Exemple : lequel choisir

f	$\log_2 \max_i \lvert f_i \rvert$
$x^2 + 1$	0.00
$x^2 + 2$	1.00
$x^2 + 3$	1.58
$x^2 + 7$	2.81
$x^2 + 11$	3.46
$x^2 + 19$	4.25
$x^2 + 43$	5.43
$x^2 + 67$	6.07
$x^2 + 163$	7.35

L'enjeu de la sélection polynomiale

Exemple : lequel choisir

f	$\log_2 \max_i \lvert f_i \rvert$	$\alpha(f, B = 1000)$
$x^2 + 1$	0.00	1.3659
$x^2 + 2$	1.00	1.0810
$x^2 + 3$	1.58	1.0238
$x^2 + 7$	2.81	1.1180
$x^2 + 11$	3.46	0.5328
$x^2 + 19$	4.25	0.5399
$x^2 + 43$	5.43	0.8046
$x^2 + 67$	6.07	1.2680
$x^2 + 163$	7.35	2.8914

Friabilité

Définition

$$\alpha(f, B) = \sum_{\ell \text{ premier},\ \ell \leqslant B} \ln \ell \Big(\mathbb{E}\big(\mathrm{val}_\ell(n),\ n \in \mathbb{Z}\big) - \mathbb{E}\big(\mathrm{val}_\ell(\mathrm{Res}_x(f(x), a + bx),\ (a, b) \in I \times J\big) \Big)$$

On veut f avec des racines mod bcp de petits nombres premiers

Si $B \to \infty$, α converge (Th. Barbulescu–Lachand 2017)

Friabilité

Définition

$$\alpha(f, B) = \sum_{\ell \text{ premier},\ \ell \leqslant B} \ln \ell \Big(\mathbb{E}(\mathrm{val}_\ell(n),\ n \in \mathbb{Z}) - \mathbb{E}(\mathrm{val}_\ell(\mathrm{Res}_x(f(x), a + bx),\ (a, b) \in I \times J) \Big)$$

On veut f avec des racines mod bcp de petits nombres premiers
Si $B \to \infty$, α converge (Th. Barbulescu–Lachand 2017)

Valuation moyenne en $\ell = 2$ pour un nombre entier n aléatoire :

- $1/2$ chance d'être pair, si pair : $\mathrm{val}_2\, n \geqslant 1$
- $1/4$ chance d'être multiple de 4, si oui :
  gain supplémentaire de 1 dans $\mathrm{val}_2\, n$
- $1/2^i$ chance d'être multiple de 2^i, si oui :
  gain supplémentaire de 1 dans $\mathrm{val}_2\, n$

Friabilité

Si $\mathrm{val}_\ell(n)$ est une variable aléatoire dans $\mathbb{N}$,

$$\mathbb{E}(\mathrm{val}_\ell(n),\ n \in \mathbb{Z}) = \sum_{i=1}^{\infty} i \Pr[\mathrm{val}_\ell(n) = i] = \sum_{i=1}^{\infty} \Pr[\mathrm{val}_\ell(n) \geqslant i]$$

Pour ℓ premier, on a

$$\mathbb{E}(\mathrm{val}_\ell(n),\ n \in \mathbb{Z}) =$$

$$\frac{1}{\ell} + \frac{1}{\ell^2} + \frac{1}{\ell^3} + \ldots + \frac{1}{\ell^k} + \ldots = \sum_{k=1}^{\infty} \frac{1}{\ell^k} = \lim_{k\to\infty} \frac{1 - 1/\ell^k}{1 - 1/\ell} - 1 = \frac{1}{\ell - 1}$$

et

$$\mathbb{E}(\mathrm{val}_\ell(n),\ n \in \mathbb{Z}) = \frac{1}{\ell - 1}\ .$$

Racines

$$\mathrm{val}_\ell(f) = \mathbb{E}\big(\mathrm{val}_\ell(\mathrm{Res}_x(f, a+bx),\ (a,b) \in I \times J\big)$$

- $(a,b) \in [0, \ell^k - 1]^2$ t.q. $\ell \nmid \mathrm{pgcd}(a,b)$, $\ell^{2k} - \ell^{2k-2}$ paires (a,b) valides (enlever $(i\ell, j\ell)$, $i,j \in [0, \ell^{k-1} - 1]$)

Racines

$$\mathrm{val}_\ell(f) = \mathbb{E}\big(\mathrm{val}_\ell(\mathrm{Res}_x(f, a+bx),\ (a,b) \in I \times J\big)$$

- $(a,b) \in [0, \ell^k - 1]^2$ t.q. $\ell \nmid \mathrm{pgcd}(a,b)$, $\ell^{2k} - \ell^{2k-2}$ paires (a,b) valides (enlever $(i\ell, j\ell)$, $i,j \in [0, \ell^{k-1} - 1]$)
- Pour quelles paires (a,b) : $a - bx$, $f(x)$ ont une racine commune mod ℓ^k ?

Racines

$$\mathrm{val}_\ell(f) = \mathbb{E}(\mathrm{val}_\ell(\mathrm{Res}_x(f, a+bx),\ (a,b) \in I \times J)$$

- $(a,b) \in [0, \ell^k - 1]^2$ t.q. $\ell \nmid \mathrm{pgcd}(a,b)$, $\ell^{2k} - \ell^{2k-2}$ paires (a,b) valides (enlever $(i\ell, j\ell)$, $i,j \in [0, \ell^{k-1} - 1]$)
- Pour quelles paires (a,b) : $a - bx$, $f(x)$ ont une racine commune mod ℓ^k ?
- Si $\ell \nmid b$, on a $\ell^k - \ell^{k-1}$ choix possibles pour b
  - si $f(x)$ n'a aucune racine mod ℓ^k, alors $\mathrm{val}_{\ell^k} = 0$
  - si $f(r_i) = 0 \bmod \ell^k$, $f'(r_i) \neq 0 \bmod \ell^k$, alors si $a - bx = \lambda(x - r_i) \bmod \ell$, $\mathrm{val}_{\ell^k} > 0$.
    Pour chaque b et chaque racine r_i, un seul $a = -br_i \bmod \ell$

Racines

$$\mathrm{val}_\ell(f) = \mathbb{E}(\mathrm{val}_\ell(\mathrm{Res}_x(f, a+bx),\ (a,b) \in I \times J)$$

- $(a,b) \in [0, \ell^k - 1]^2$ t.q. $\ell \nmid \mathrm{pgcd}(a,b)$, $\ell^{2k} - \ell^{2k-2}$ paires (a,b) valides (enlever $(i\ell, j\ell)$, $i,j \in [0, \ell^{k-1} - 1]$)
- Pour quelles paires (a,b) : $a - bx$, $f(x)$ ont une racine commune mod ℓ^k ?
- Si $\ell \nmid b$, on a $\ell^k - \ell^{k-1}$ choix possibles pour b
  - si $f(x)$ n'a aucune racine mod ℓ^k, alors $\mathrm{val}_{\ell^k} = 0$
  - si $f(r_i) = 0 \bmod \ell^k$, $f'(r_i) \neq 0 \bmod \ell^k$, alors si $a - bx = \lambda(x - r_i) \bmod \ell$, $\mathrm{val}_{\ell^k} > 0$.
    Pour chaque b et chaque racine r_i, un seul $a = -br_i \bmod \ell$

Soit n_{ℓ^k} le nombre de racines distinctes de $f(x) \bmod \ell^k$.
$(\ell^k - \ell^{k-1}) n_{\ell^k}$ paires (a,b) t.q. $\ell^k \mid \mathrm{Res}_x(f, a - bx)$

Racines

$$\mathrm{val}_\ell(f) = \mathbb{E}(\mathrm{val}_\ell(\mathrm{Res}_x(f, a+bx),\ (a,b) \in I \times J)$$

- $(a,b) \in [0, \ell^k - 1]^2$ t.q. $\ell \nmid \mathrm{pgcd}(a,b)$, $\ell^{2k} - \ell^{2k-2}$ paires (a,b) valides (enlever $(i\ell, j\ell)$, $i,j \in [0, \ell^{k-1} - 1]$)
- Pour quelles paires (a,b) : $a - bx$, $f(x)$ ont une racine commune mod ℓ^k ?
- Si $\ell \nmid b$, on a $\ell^k - \ell^{k-1}$ choix possibles pour b
  - si $f(x)$ n'a aucune racine mod ℓ^k, alors $\mathrm{val}_{\ell^k} = 0$
  - si $f(r_i) = 0 \bmod \ell^k$, $f'(r_i) \neq 0 \bmod \ell^k$, alors si $a - bx = \lambda(x - r_i) \bmod \ell$, $\mathrm{val}_{\ell^k} > 0$.
    Pour chaque b et chaque racine r_i, un seul $a = -br_i \bmod \ell$

  Soit n_{ℓ^k} le nombre de racines distinctes de $f(x) \bmod \ell^k$.
  $(\ell^k - \ell^{k-1}) n_{\ell^k}$ paires (a,b) t.q. $\ell^k \mid \mathrm{Res}_x(f, a - bx)$
- Si $\ell \mid b$, aucune paire possible, valuation 0.

Racines

$$val_\ell(f) = \sum_{k=1}^{\infty} \frac{(\ell^k - \ell^{k-1}) n_{\ell^k}}{\ell^{2k} - \ell^{2k-2}} = \sum_{k=1}^{\infty} \frac{\ell}{\ell+1} \frac{n_{\ell^k}}{\ell^k}$$

Si $n_{\ell^k} = n_\ell$ pour tout $k \geq 1$, $\mathrm{val}_\ell(f) = \ell n_\ell/(\ell^2 - 1)$.

Lemme (Hensel)

Soit $f(x)$ un polynôme de degré au moins 2 et r une racine simple modulo ℓ ($f'(r) \neq 0 \bmod \ell$). Alors pour tout $k > 1$, il existe une unique racine $r_k \in \mathbb{Z}/\ell^k\mathbb{Z}$ de $f(x)$ au dessus de r.

Si $\ell \nmid \mathrm{disc}(f)$,

$$\alpha_\ell(f) = \left(\frac{1}{\ell - 1} - \frac{n_\ell \ell}{\ell^2 - 1} \right) \log \ell$$

$n_\ell =$ nombre de racines distinctes de f mod ℓ

Si $\ell \mid \mathrm{disc}(f)$, ($\ell$ est un *bad prime*).

Lemme (Hensel)

Si r_k est une racine multiple de f mod ℓ^k, *c-à-d* $f(r_k) = 0 \bmod \ell$, $f'(r_k) = 0 \bmod \ell^k$

- *Si* $\ell^{k+1} \mid f(r_k)$, *alors* $\forall i \in [0, \ell - 1]$, $\ell^{k+1} \mid f(r_k + i\ell^k)$.
- *Si* $\ell^{k+1} \nmid f(r_k)$, *il n'y a pas de racine mod* ℓ^{k+1} *au dessus de* r_k.

Il existe un exposant e tel que $n_{\ell^k} = n_{\ell^e}$ pour tout $k \geqslant e$.

Si $\ell \mid \mathrm{disc}(f)$, ($\ell$ est un *bad prime*).

Lemme (Hensel)

Si r_k est une racine multiple de f mod ℓ^k, *c-à-d* $f(r_k) = 0 \bmod \ell$, $f'(r_k) = 0 \bmod \ell^k$

- *Si* $\ell^{k+1} \mid f(r_k)$, *alors* $\forall i \in [0, \ell - 1]$, $\ell^{k+1} \mid f(r_k + i\ell^k)$.
- *Si* $\ell^{k+1} \nmid f(r_k)$, *il n'y a pas de racine mod* ℓ^{k+1} *au dessus de* r_k.

Il existe un exposant e tel que $n_{\ell^k} = n_{\ell^e}$ pour tout $k \geqslant e$.
Comment calculer e ?

Si $\ell \mid \mathrm{disc}(f)$, ($\ell$ est un *bad prime*).

Lemme (Hensel)

Si r_k est une racine multiple de f mod ℓ^k, *c-à-d* $f(r_k) = 0 \bmod \ell$, $f'(r_k) = 0 \bmod \ell^k$

- *Si* $\ell^{k+1} \mid f(r_k)$, *alors* $\forall i \in [0, \ell - 1]$, $\ell^{k+1} \mid f(r_k + i\ell^k)$.
- *Si* $\ell^{k+1} \nmid f(r_k)$, *il n'y a pas de racine mod* ℓ^{k+1} *au dessus de* r_k.

Il existe un exposant e tel que $n_{\ell^k} = n_{\ell^e}$ pour tout $k \geqslant e$.
Comment calculer e ?
bibliothèque de calcul `cado-nfs`, fichier `polyselect/auxiliary.c`, code C récursif

Calcul de $\mathrm{val}_\ell(f)$ pour les racines multiples

Rétro-ingénierie de `cado-nfs/polyselect/auxiliary.c`
Soit r_0 une racine multiple de f modulo ℓ.
Soit e tel que $\ell^{e-1} \mid \mathrm{cont}(f(r_0 + \ell x))$, et $\ell^e \nmid \mathrm{cont}(f(r_0 + \ell x))$.
La racine r_0 a ℓ^{e-1} racines relevées modulo ℓ^e :
$r_0 + i_1\ell + i_2\ell^2 + \ldots + i_{e-1}\ell^{e-1} \bmod \ell^e$
avec chaque $i_j \in [0, \ell - 1]$ donnant une racine de f valide mod ℓ^e.

Calcul de $\mathrm{val}_\ell(f)$ pour les racines multiples

Rétro-ingénierie de `cado-nfs/polyselect/auxiliary.c`
Soit r_0 une racine multiple de f modulo ℓ.
Soit e tel que $\ell^{e-1} \mid \mathrm{cont}(f(r_0 + \ell x))$, et $\ell^e \nmid \mathrm{cont}(f(r_0 + \ell x))$.
La racine r_0 a ℓ^{e-1} racines relevées modulo ℓ^e :
$r_0 + i_1\ell + i_2\ell^2 + \ldots + i_{e-1}\ell^{e-1} \bmod \ell^e$
avec chaque $i_j \in [0, \ell - 1]$ donnant une racine de f valide mod ℓ^e.

Si $f(r_0 + \ell x)/\ell^{e-1}$ a une racine simple i_e alors $n_{\ell^e} = \ell^{e-1}$, et

$$\mathrm{val}_\ell(f) = \frac{1}{\ell+1}\left(\underbrace{\frac{n_{\ell^e}}{\ell^{e-2}}\frac{1}{\ell-1}}_{\text{partie stabilisée}} + \sum_{k=1}^{e-1} \underbrace{\frac{n_{\ell^k}}{\ell^{k-1}}}_{n_{\ell^k} = \ell^{k-1}} \right)$$

$$= \frac{1}{\ell+1}\left(\frac{\ell^{e-1}}{\ell^{e-2}}\frac{1}{\ell-1} + (e-1)\right) = \frac{1}{\ell+1}\left(\frac{\ell}{\ell-1} + (e-1)\right)$$

Dernier record de calcul : $\mathbb{F}_p$ de 768 bits

Kleinjung, Diem, A. Lenstra, Priplata, Stahlke, Eurocrypt'2017.
$p = \lfloor 2^{766} \times \pi \rfloor + 62762$ premier, 768 bits, 232 chiffres,
$(p-1)/2$ premier

$$f(x) = 140x^4 + 34x^3 + 86x^2 + 5x - 55$$

$$\begin{aligned} g(x) = {} & 37086340388641614115050552391952767723193261818410009592 4x^3 \\ & - 19379813128330387785656174698293955440652559380159203096 79x^2 \\ & - 21758329362694789978757744112833302761754109500473473641 5x \\ & + 27726073040034952289042261847349814852870611500333793515 0 \end{aligned}$$

avec $\alpha(g, 1000) = -5.448$ (-7.860 bits), $\alpha(f, 1000) = -2.000$ (-2.885 bits).
Énumération ($\sim 10^{12}$) de tous les $f(x)$, $|f_i| \leqslant 165$
$\alpha(f, 1000)$ critère l'élimination

Log discret dans $\mathbb{F}_{p^n}$

Beaucoup moins étudié que le log discret dans $\mathbb{Z}/p\mathbb{Z}$ et la factorisation. Beaucoup moins d'utilisation en cryptographie, jusqu'en 2000.

- 2000 cryptosystèmes LUC et XTR : log discret dans le sous-groupe cyclotomique de $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^6}$
- Quelle difficulté pour calculer un log discret dans $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^6}$?
- 2005 Granger–Vercauteren $L_{p^n}(1/2)$
- 2006 Joux–Lercier–Smart–Vercauteren $L_{p^n}(1/3, 2.423)$ (NFS-HD pour High-Degree)
- Accouplements/couplages : $\mathbb{F}_{2^{4n}}$, $\mathbb{F}_{3^{6m}}$, $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^{12}}$

Tower-NFS

Pour calculer des logs discrets dans $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^4}$, ...
En cryptographie : corps d'arrivée d'accouplements (couplages) de Weil et Tate.
Soit $E/\mathbb{F}_p$ une courbe elliptique de trace t, d'ordre $p+1-t$ ayant un sous-groupe de $E(\mathbb{F}_p)$ d'ordre premier $r \mid p+1-t$
Le degré de plongement n est l'ordre de p dans $\mathbb{Z}/r\mathbb{Z}$,
ou encore $E[r] \subset E(\mathbb{F}_{p^n})$, et n est minimal.

$$e : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^n})[r]/(rE(\mathbb{F}_{p^n})) \to \mathbb{F}_{p^n}^*$$

Courbes Miyaji–Nakabayashi–Takano : $\mathbb{F}_{p^3}, \mathbb{F}_{p^4}, \mathbb{F}_{p^6}$
Courbes Barreto–Naehrig : $\mathbb{F}_{p^{12}}$
Courbes Barreto–Lynn–Scott : $\mathbb{F}_{p^{12}}, \mathbb{F}_{p^{24}}$

Complexités asymptotiques

$$L_{p^n}(1/3, c)$$

grande caractéristique $p = L_{p^n}(\alpha),\ \alpha > 2/3$:

$c = (64/9)^{1/3} \simeq 1.923$	NFS
p spécial :	
$c = (32/9)^{1/3} \simeq 1.526$	SNFS

caractéristique moyenne $p = L_{p^n}(\alpha),\ 1/3 < \alpha < 2/3$:

$c = (96/9)^{1/3} \simeq 2.201$	si n premier NFS-HD (Conjugaison)
$c = (48/9)^{1/3} \simeq 1.747$	si n composé, meilleur cas pour TNFS : paramètres parfaitement ajustés
p spécial :	
$c = (64/9)^{1/3} \simeq 1.923$	NFS-HD+Joux–Pierrot'13
$c = (32/9)^{1/3} \simeq 1.526$	n composé, meilleur cas pour STNFS

Diagramme commutatif de NFS, log discret dans $\mathbb{F}_{p^n}^*$

Soient f, g deux polynômes de $\mathbb{Z}[x]$ définissant deux corps de nombres
et t.q. f et g mod p ont un facteur irréductible $\varphi(z) \in \mathbb{F}_p[z]$ de degré n, on définit l'extension $\mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z))$
Diagramme :

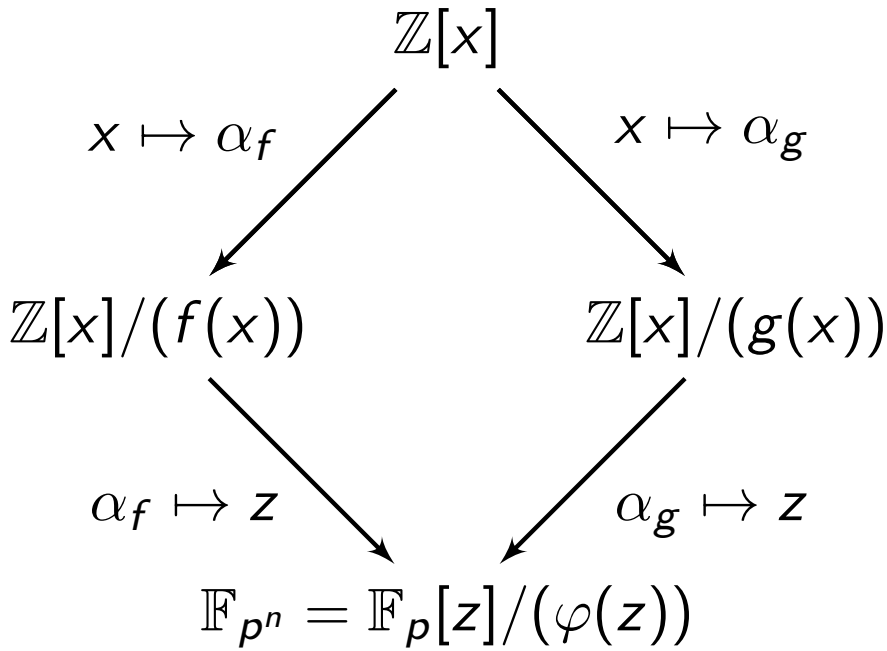


Diagramme commutatif de NFS, log discret dans $\mathbb{F}_{p^n}^*$

Soient f, g deux polynômes de $\mathbb{Z}[x]$ définissant deux corps de nombres
et t.q. f et g mod p ont un facteur irréductible $\varphi(z) \in \mathbb{F}_p[z]$ de degré n, on définit l'extension $\mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z))$
Diagramme : Grand p :

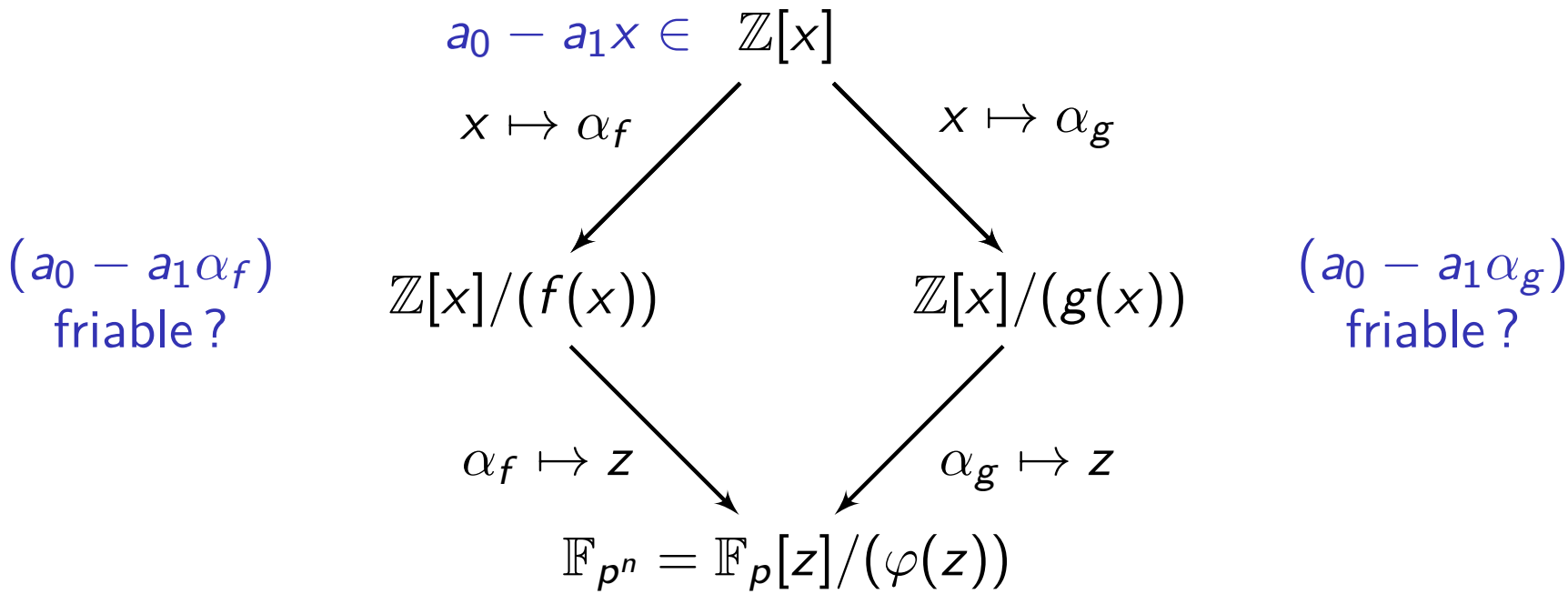
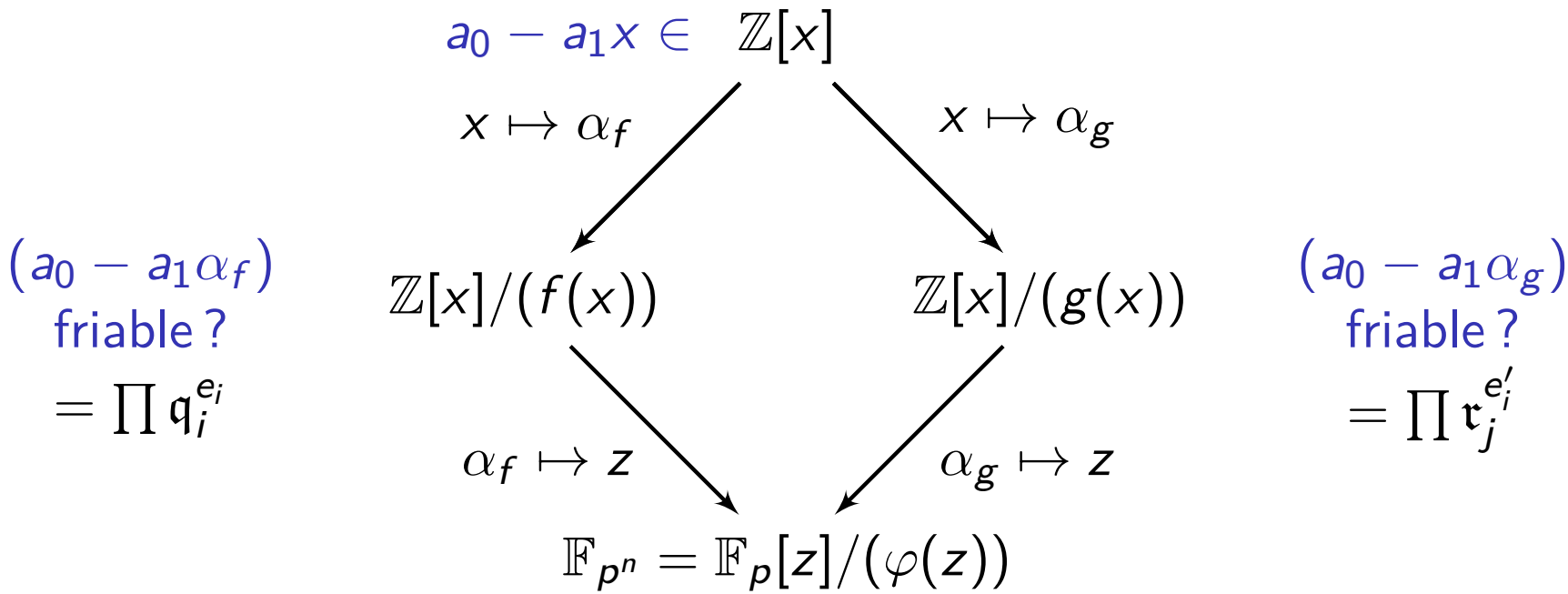


Diagramme commutatif de NFS, log discret dans $\mathbb{F}_{p^n}^*$

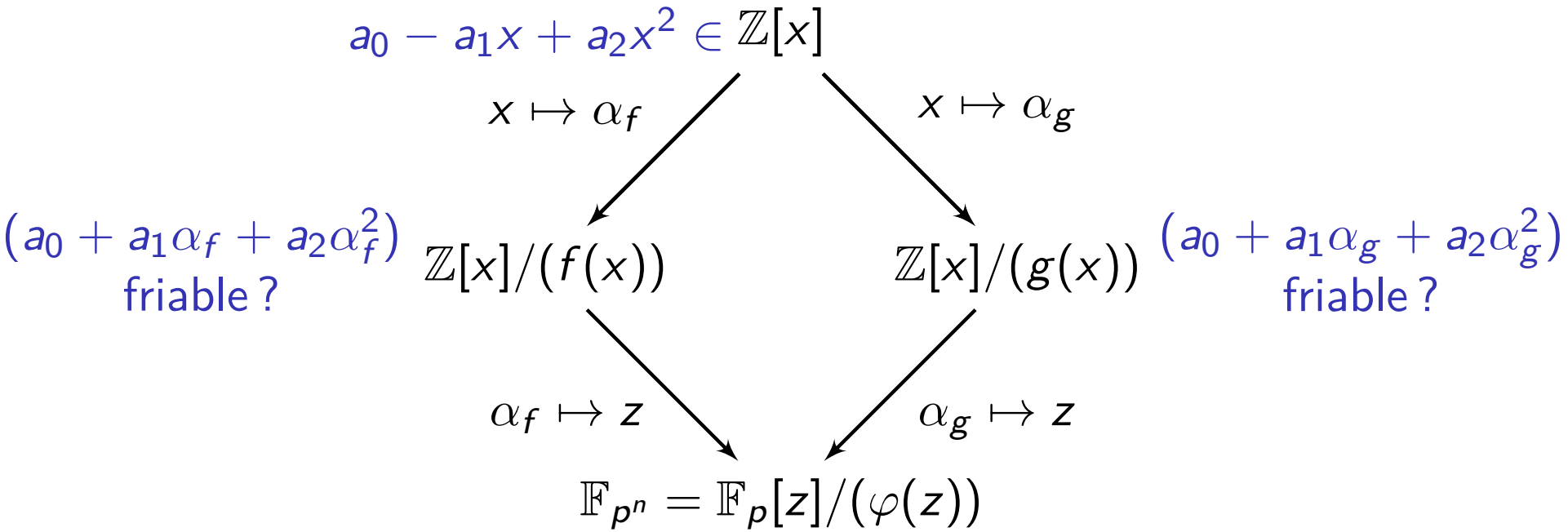
Soient f, g deux polynômes de $\mathbb{Z}[x]$ définissant deux corps de nombres
et t.q. f et g mod p ont un facteur irréductible $\varphi(z) \in \mathbb{F}_p[z]$ de degré n, on définit l'extension $\mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z))$
Diagramme : Grand p :



relation : "$\sum e_i$ vlog $\mathfrak{q}_i = \sum e'_j$ vlog $\mathfrak{r}_j$"

Diagramme commutatif de NFS, log discret dans $\mathbb{F}_{p^n}^*$

Soient f, g deux polynômes de $\mathbb{Z}[x]$ définissant deux corps de nombres
et t.q. f et g mod p ont un facteur irréductible $\varphi(z) \in \mathbb{F}_p[z]$ de degré n, on définit l'extension $\mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z))$
Diagramme : Moyen p : (Joux–Lercier–Smart–Vercauteren 06)



Paramètres de NFS

- base de facteurs de petite norme $=$
  $\{$idéaux premiers $\mathfrak{p}_i$, $|\text{Norme}(\mathfrak{p}_i)| \leq B\}$
  $\cup\{$idéaux premiers $\mathfrak{r}_j$, $|\text{Norme}(\mathfrak{r}_i)| \leq B\}$
- il faut autant de relations friables que d'idéaux premiers $\mathfrak{p}_i, \mathfrak{r}_j$ pour avoir une matrice carrée
- équilibrer les temps de collecte de relations (crible) et d'algèbre linéaire

Normes algébriques

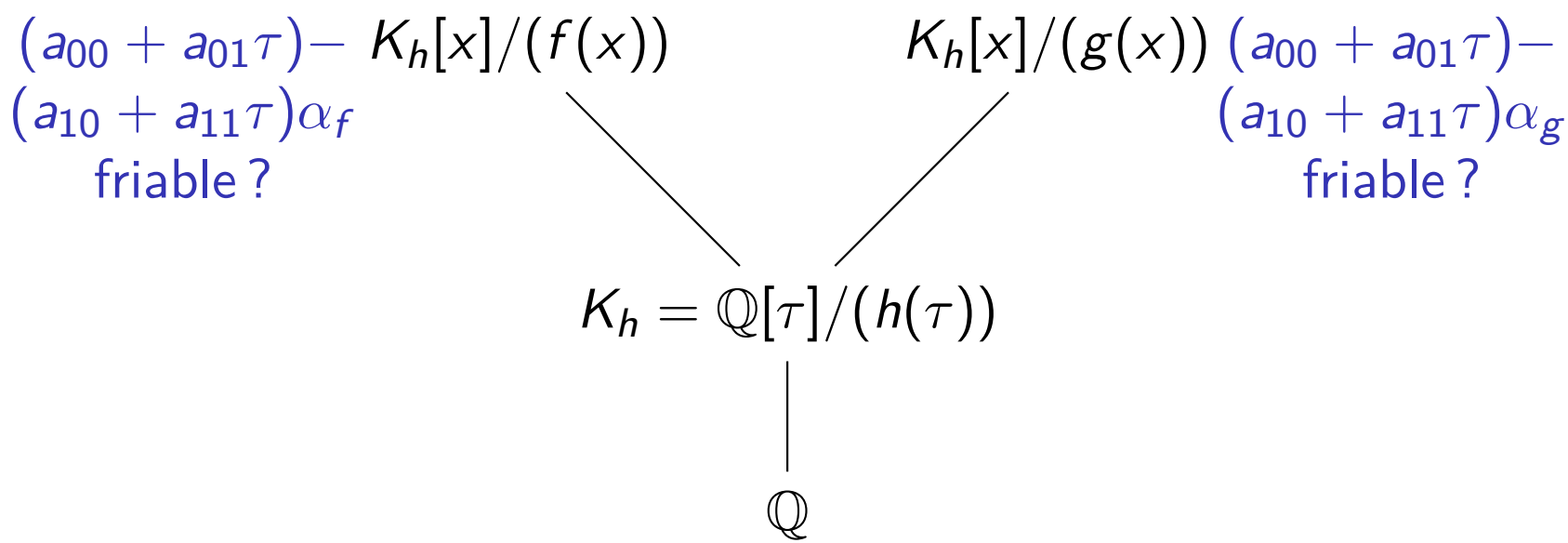
La complexité asymptotique est déterminée par la *taille des normes* des éléments $\sum_{0 \leq i < t} a_i \alpha^i$ dans la collecte de relations.
Il faut avoir les deux côtés *friables* pour en tirer une relation.

"Un idéal est B-friable" interprété en
"sa norme alg. est B-friable".

Borne de friabilité : $B = L_{p^n}[1/3, \beta]$
Taille des normes : $L_{p^n}[2/3, c_N]$
Complexité : minimiser c_N dans les formules.
Pour réduire la complexité de NFS, il faut réduire la taille des normes *asymptotiquement*.
$\rightarrow$ très difficile.

Extended Tower NFS (Kim Barbulescu 16)

- Tower NFS (TNFS) : Barbulescu–Gaudry–Kleinjung 2015
- Extended TNFS : Kim–Barbulescu, Kim–Jeong, Sarkar–Singh, 2016–2017
- Tour d'extension de corps de nombres
- $\deg(h)$ va remplacer t dans $a_0 + a_1\alpha + \ldots + a_{t-1}\alpha^{t-1}$ (de JLSV06)
- $a_0 - a_1\alpha$ devient $(a_{00} + a_{01}\tau) - (a_{10} + a_{11}\tau)\alpha$



Les limitations de la complexité asymptotique

$\mathrm{Norme}_{K_f}(a(\alpha)) = \mathrm{Res}(a(x), f(x))$ (pour f unitaire)

$$|\mathrm{Res}(a, f)| \leq (d_a + 1)^{d_f/2}(d_f + 1)^{d_a/2}\|a\|_\infty^{d_f}\|f\|_\infty^{d_a}$$

- utilise une borne sup sur les coefficients des polynômes, et une borne sur les normes algébriques
- Bornes pour résultants de Kalkbrener, Bistritz–Lifshitz pas assez fines pour des cas précis
- aucun record de calcul disponible pour calibrer les formules asymptotiques (deviner une partie de $o(1)$ sur un cas concret)

On voudrait trouver une estimation plus fine des tailles des normes, et concevoir une implémentation de TNFS

Simulation sans relations

Espace de relations :
$\mathcal{S} = \{\sum_{0 \le i < d_h} a_i y^i + (\sum_{0 \le i < d_h} b_i y^i)x,\ |a_i|, |b_i| < A\}$
Volume : $Vol = 2^{2d_h - 1} A^{2d_h}$
Norme algébrique :
$N = \text{Norme}_{K_f}(a(\alpha_h, \alpha_f)) = \text{Res}_y(\text{Res}_x(a(x, y), f(x)), h(y))$
(h, f unitaires)
N est B-friable ($N = \prod_{p_i < B} p_i^{e_i}$) avec probabilité

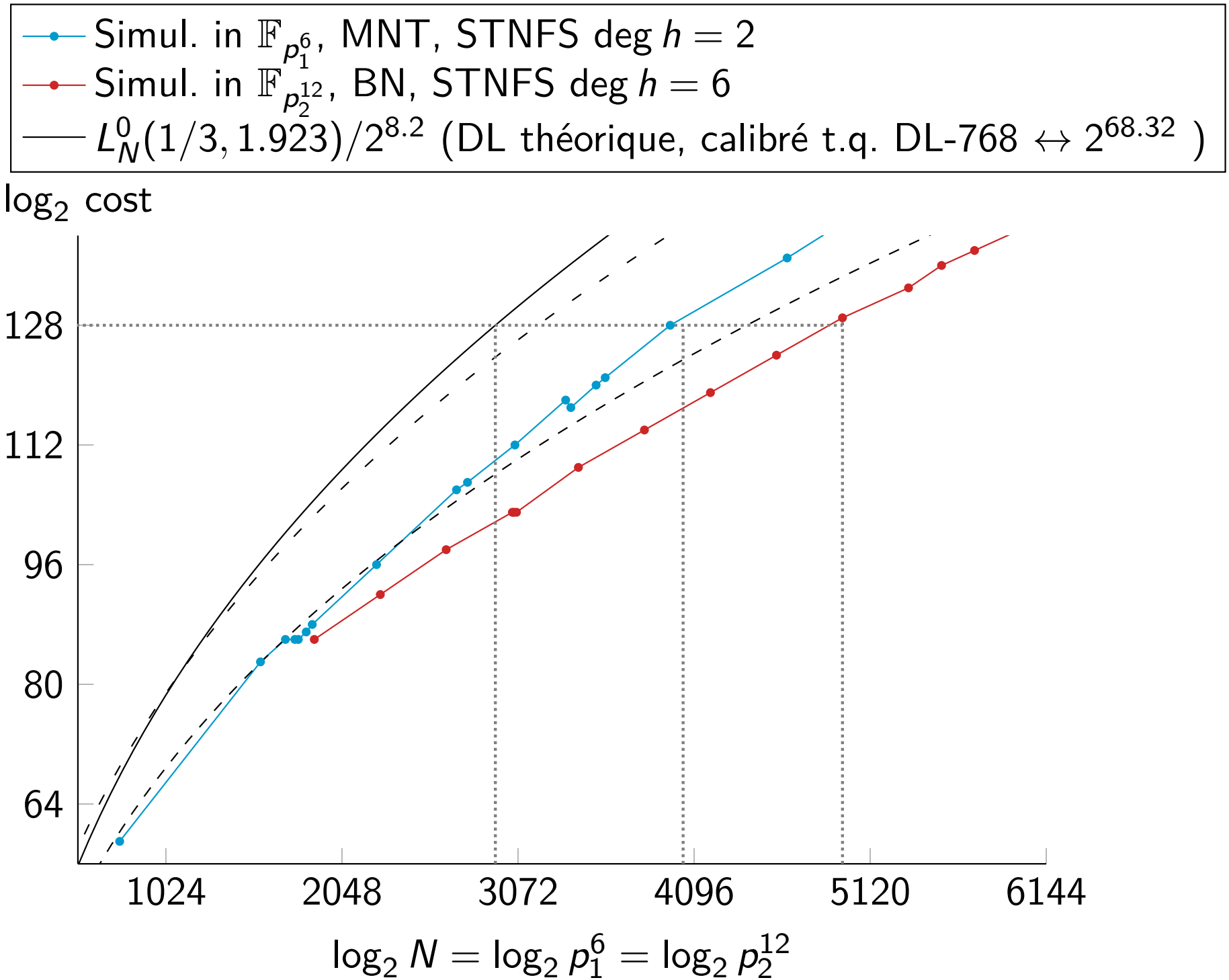
$$u = \frac{\log N + \alpha}{\log B},\ \text{Pr} = \rho(u) + (1 - \gamma)\frac{\rho(u-1)}{\log N}$$

avec $\gamma \approx 0.577$ la constante γ d'Euler,
ρ la fonction Dickman-ρ

Simulation sans relations

Implémentation de la technique Barbulescu–Duquesne
Variantes :

- calculer $\alpha(f), \alpha(g)$ (par rapport au sous-corps K_h)
- trouver h, f, g avec un bon α : $\alpha(f), \alpha(g) < 0$
- Simulation de Monte-Carlo avec 10^6 tirages aléatoires dans $\mathcal{S}$.
  Pour chaque tirage a :
  1. calculer la norme algébrique N_f, N_g (résultants)
  2. estimer la probabilité de friabilité avec Dickman-ρ
- Probabilité de friabilité moyenne sur l'échantillon ($\sim 10^6$)
  $\rightarrow$ Estimation du nombre total de relations possibles dans $\mathcal{S}$
- recherche par dichotomie de paramètres B (borne de friabilité), A (max des coefficients) pour atteindre un coût équilibré entre collecte de relations et algèbre linéaire


Simul. in $\mathbb{F}_{p_1^6}$, MNT, STNFS deg $h = 2$
Simul. in $\mathbb{F}_{p_2^{12}}$, BN, STNFS deg $h = 6$
$L_N^0(1/3, 1.923)/2^{8.2}$ (DL théorique, calibré t.q. DL-768 $\leftrightarrow 2^{68.32}$)
$\log_2$ cost
128
112
96
80
64
1024
2048
3072
4096
5120
6144
$\log_2 N = \log_2 p_1^6 = \log_2 p_2^{12}$

Tower-NFS : $\alpha(h, f, B)$

- remplacer ℓ petit nombre premier par $\mathfrak{l}$ idéal premier de $\mathcal{O}_h$ au dessus de ℓ
- remplacer n_ℓ le nombre de racines de f mod ℓ par $n_\mathfrak{l}$ le nombre de racines de f dans $\mathcal{O}_h/\mathfrak{l} = \mathbb{F}_{\ell^{\deg \mathfrak{l}}}$

$$\mathrm{val}_\mathfrak{l}(f) = \sum_{i=1}^{\infty} \Pr(\mathrm{val}_\mathfrak{l}(\mathrm{Res}(a(y) + b(y)x, f_y(x))) \geqslant i)$$

Problème d'implémentation lorsque $\mathfrak{l} \mid \mathrm{disc}(f)$, et $\mathfrak{l} \in \mathcal{O}_h$ n'est pas principal.

Exemple

Code Magma expérimental. Code SageMath en développement.
$h = y^2 + 5$, $f = x^4 - 3\tau x^3 - (6\tau + 1)x^2 - (\tau + 10)x - 10\tau$ avec τ une racine de h.
10^8 paires $(\mathbf{a}, \mathbf{b})$, avec $\mathbf{a} = a_0 + a_1 y$, $\mathbf{b} = b_0 + b_1 y$, $a_0, a_1, b_0 \in [-A, A]$ et $b_1 \in [0, A]$ entiers tirés aléatoirement, et $A = 10^6$.
Valuation en $\mathfrak{l}$ idéal premier au dessus de $\ell \in \mathbb{Z}$ premier $\leqslant B = 2000$.

$$\mathrm{val}_{\mathfrak{l}}(\mathrm{Res}((a_0 + a_1\tau) + (b_0 + b_1\tau)x, f(x))$$

Moyenne expérimentale :

$$1/10^8 \sum_{\mathbf{a},\mathbf{b}} \mathrm{val}_{\mathfrak{l}}(\mathrm{Res}(\mathbf{a} + \mathbf{b}x, f))$$

Exemple : “mauvais” idéaux

ℓ	$\mathfrak{l}$	$\mathrm{val}_{\mathfrak{l}}$ disc f	$\mathrm{val}_{\mathfrak{l}}(f)$	moyenne experim.	ratio $\mathrm{val}_{\mathfrak{l}}(f)/\mathrm{moy}$
bad primes					
2	$\langle 2, 1+\tau\rangle$	4	$4/3 = 1.33333333$	1.33327468	0.9999560
3	$\langle 3, 1+\tau\rangle$	2	$0 = 0$	0	–
3	$\langle 3, 5+\tau\rangle$	1	$1/4 = 0.25$	0.25001848	1.0000739
5	$\langle 5, \tau\rangle$	2	$5/6 = 0.83333333$	0.83321058	0.9998526
29	$\langle 29, 13+\tau\rangle$	1	$1/30 = 0.03333333$	0.03333272	0.9999816
263	$\langle 263, 28+\tau\rangle$	1	$197/17292 = 0.01139255$	0.01138250	0.9991177
487	$\langle 487, 344+\tau\rangle$	1	$1/488 = 0.00204918$	0.00205413	1.0024154

Exemple : “bons” idéaux

ℓ	$\mathfrak{l}$	$\mathrm{val}_{\mathfrak{l}}(f)$	moyenne experim.	ratio $\mathrm{val}_{\mathfrak{l}}(f)/\mathrm{moy}$
good primes				
7	$\langle 7, 3+\tau\rangle$	$7/24 = 0.29166666$	0.29167549	1.0000302
7	$\langle 7, 4+\tau\rangle$	$7/48 = 0.14583333$	0.14581621	0.9998825
19	19 (inert in K_h)	$361/130320 = 0.00277010$	0.00277376	1.0013196
23	$\langle 23, 8+\tau\rangle$	$23/528 = 0.04356060$	0.04354519	0.9996461
29	$\langle 29, 16+\tau\rangle$	$29/420 = 0.06904761$	0.06907099	1.0003384
41	$\langle 41, 6+\tau\rangle$	$41/420 = 0.09761904$	0.09762156	1.0000257
41	$\langle 41, -6+\tau\rangle$	$41/420 = 0.09761904$	0.09762177	1.0000278
43	$\langle 43, 34+\tau\rangle$	$43/1848 = 0.02326839$	0.02326401	0.9998114
47	$\langle 47, 29+\tau\rangle$	$47/1104 = 0.04257246$	0.04259221	1.0004638
59	$\langle 59\rangle$	$3481/12117360 = 0.00028727$	0.00028519	0.9927463

Exemple : courbe Barreto-Naehrig 254 bits

$p = 36s^4 + 36s^3 + 24s^2 + 6s + 1$ avec $s = -(2^{62} + 2^{55} + 1)$

$f = 36x^8 - 36(4y - 1)x^6 + 12(18y^2 - 9y + 2)x^4 - 6(24y^3 - 18y^2 + 8y - 1)x^2 + 36y^4 - 36y^3 + 24y^2 - 6y + 1$

$g = x^2 - y + 4647714815446351873$

$B = 2000$

h	$1/\zeta_{K_h}(2)$	$\alpha(h, f, B)$	$\alpha(h, g, B)$	$\alpha_f + \alpha_g$
$y^6 + y^5 - y^2 - y - 1$	0.953	2.917	1.650	4.568
$y^6 - y^4 + y^3 + y^2 - 1$	0.917	1.124	2.294	3.418
$y^6 + y^3 + y^2 - y - 1$	0.917	2.763	2.544	5.307
$y^6 + y^5 - y^3 + y - 1$	0.909	0.518	2.736	3.254
$y^6 + y^5 + y^4 + y^3 + y^2 + y - 1$	0.883	2.303	0.842	3.145
$y^6 + y^4 + y^3 + y - 1$	0.867	2.283	0.542	2.825
$y^6 + y^4 + y^2 + y + 1$	0.836	2.238	0.330	2.568
$y^6 + y^5 + y^2 - y + 1$	0.763	0.893	1.599	2.492
$y^6 + y^5 - y^4 + y^3 + y^2 + y - 1$	0.756	0.951	0.478	1.429
$y^6 + y^5 + y - 1$	0.736	2.167	1.179	3.346
$y^6 + y^5 + y^3 - y^2 + y - 1$	0.732	1.649	1.766	3.414
$y^6 + y^3 + y - 1$	0.728	0.697	2.089	2.786
$y^6 + y^3 - y + 1$	0.720	1.462	1.320	2.782
$y^6 + y^3 + y^2 + 1$	0.718	1.322	-0.027	1.296
$y^6 - y^4 + y^3 - y^2 - y - 1$	0.710	0.249	0.826	1.075
$y^6 + y^5 - y^3 + y^2 - y + 1$	0.697	2.148	1.468	3.616
$y^6 + y^4 + y + 1$	0.679	1.339	1.013	2.351

Exemple : courbe Barreto-Naehrig 254 bits

$f = 36x^8 + 36yx^6 + 24y^2x^4 + 6y^3x^2 + y^4$
$g = x^2 + 46477148154463518 73y$
$B = 2000$

h	$1/\zeta_{K_h}(2)$	$\alpha(h, f, B)$	$\alpha(h, g, B)$	$\alpha_f + \alpha_g$
$y^6 + y^5 - y^2 - y - 1$	0.953	2.042	2.479	4.521
$y^6 - y^4 + y^3 + y^2 - 1$	0.917	1.288	1.740	3.028
$y^6 + y^3 + y^2 - y - 1$	0.917	2.419	2.876	5.295
$y^6 + y^5 - y^3 + y - 1$	0.909	0.278	2.357	2.636
$y^6 + y^5 + y^4 + y^3 + y^2 + y - 1$	0.883	2.341	2.033	4.374
$y^6 + y^4 + y^3 + y - 1$	0.867	0.899	2.526	3.425
$y^6 + y^4 + y^2 + y + 1$	0.836	1.955	1.141	3.095
$y^6 + y^5 + y^2 - y + 1$	0.763	0.891	1.264	2.155
$y^6 + y^5 - y^4 + y^3 + y^2 + y - 1$	0.756	0.956	1.177	2.133
$y^6 + y^5 + y - 1$	0.736	1.925	2.108	4.032
$y^6 + y^5 + y^3 - y^2 + y - 1$	0.732	1.729	2.099	3.828
$y^6 + y^3 + y - 1$	0.728	-0.250	1.191	0.941
$y^6 + y^3 - y + 1$	0.720	1.605	1.348	2.952
$y^6 + y^3 + y^2 + 1$	0.718	1.151	1.294	2.445
$y^6 - y^4 + y^3 - y^2 - y - 1$	0.710	0.406	2.278	2.684
$y^6 + y^5 - y^3 + y^2 - y + 1$	0.697	1.572	0.818	2.390
$y^6 + y^4 + y + 1$	0.679	1.319	1.683	3.002

Points techniques pour les simulations

- Unités : induisent quelle proportion de relations identiques ?
- Comment se passer d'une simulation sur un échantillon de 10^6 pour chacun des polynômes candidats ?
- $\sum_{i=0}^{\deg h-1} a_i h^i + x \sum_{i=0}^{\deg h-1} b_i h^i$: a_i, b_i dans un cube de dimension $2 \deg h$, et avec une sphère ?

NFS

- Années 70-90 : USA, Canada, Pays-Bas (not. CWI, Elkenbracht-Huizing, H. Lenstra, Montgomery, Tijdeman `https://ir.cwi.nl/`)
- Années 2000 : séries de records de calculs français (Joux–Lercier)
- 2013–2016 : petite caractéristique (Irlande, Suisse, Mexique, France)
  Projet ANR-CATREL (crible algébrique) Nancy, Saclay-Polytechnique, Montpellier
- 2017 : record de calcul de log discret dans $\mathbb{F}_p$, 768 bits, Kleinjung et al. (Suisse, Allemagne)
- USA, Canada, Pays-Bas ont disparus... (ou presque `https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2018-August/000926.html`)

Bibliography I

L. Adleman.
A subexponential algorithm for the discrete logarithm problem with applications to cryptography.
In *20th FOCS*, pages 55–60. IEEE Computer Society Press, Oct. 1979.
https://doi.org/10.1109/SFCS.1979.2.

L. Adleman.
The function field sieve.
In L. M. Adleman and M.-D. Huang, editors, *Algorithmic Number Theory (ANTS-I)*, volume 877 of *LNCS*, pages 141–154. Springer, Heidelberg, 1994.

L. M. Adleman and M.-D. A. Huang.
Function field sieve method for discrete logarithms over finite fields.
Information and Computation, 151(1/2) :5–16, 1999.
https://dl.acm.org/citation.cfm?id=305383.305385,
https://doi.org/10.1006/inco.1998.2761.

R. Barbulescu, P. Gaudry, and T. Kleinjung.
The tower number field sieve.
In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 31–55. Springer, Heidelberg, Nov. / Dec. 2015.

Bibliography II


R. Barbulescu and A. Lachand.
Some mathematical remarks on the polynomial selection in NFS.
Math. Comp., 86(303) :397–418, 2017.
https://hal.inria.fr/hal-00954365,
https://doi.org/10.1090/mcom/3112.


E. R. Canfield, P. Erdős, and C. Pomerance.
On a problem of Oppenheim concerning "factorisatio numerorum".
Journal of Number Theory, 17(1) :1–28, 1983.
https://math.dartmouth.edu/~carlp/PDF/paper39.pdf.


D. Coppersmith.
Fast evaluation of logarithms in fields of characteristic two.
IEEE Transactions on Information Theory, 30(4) :587–594, 1984.
http://ieeexplore.ieee.org/document/1056941/,
https://doi.org/10.1109/TIT.1984.1056941.


D. Coppersmith, A. M. Odlyzko, and R. Schroeppel.
Discrete logarithms in $\mathrm{GF}(p)$.
Algorithmica, 1(1) :1–15, 1986.
https://dl.acm.org/citation.cfm?id=6835,
https://doi.org/10.1007/BF01840433.

Bibliography III

D. M. Gordon.
Discrete logarithms in $\mathrm{GF}(p)$ using the number field sieve.
SIAM Journal on Discrete Mathematics, 6(1) :124–138, 1993.
https://www.ccrwest.org/gordon/log.pdf.

A. Guillevic and F. Morain.
Pairings for Engineers, chapter 9 – Discrete Logarithms, pages 203–242.
CRC Press Taylor and Francis group, Spring 2016.
N. ElMrabet and M. Joye (eds),
https://www.crcpress.com/Guide-to-Pairing-Based-Cryptography/El-Mrabet-Joye/p/book/9781498729505,
https://hal.inria.fr/hal-01420485v2.

A. Joux, R. Lercier, N. Smart, and F. Vercauteren.
The number field sieve in the medium prime case.
In C. Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 326–344.
Springer, Heidelberg, Aug. 2006.

T. Kim and R. Barbulescu.
Extended tower number field sieve : A new complexity for the medium prime case.
In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 543–571. Springer, Heidelberg, Aug. 2016.

Bibliography IV


T. Kleinjung, C. Diem, A. K. Lenstra, C. Priplata, and C. Stahlke.
Computation of a 768-bit prime field discrete logarithm.
In J. Coron and J. B. Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 185–201. Springer, Heidelberg, Apr. / May 2017.


M. Kraitchik.
Théorie des Nombres.
Gauthier–Villars, 1922.


M. Kraitchik.
Recherches sur la Théorie des Nombres.
Gauthier–Villars, 1924.


H. Lenstra and C. Pomerance.
A rigorous time bound for factoring integers.
J. Amer. Math. Soc., 5(3) :483–516, 1992.


D. V. Matyukhin.
Effective version of the number field sieve for discrete logarithms in the field $\mathrm{GF}(p^k)$ (in Russian).
Trudy po Discretnoi Matematike, 9 :121–151, 2006.

Bibliography V

K. S. McCurley.
The discrete logarithm problem.
In C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, pages 49–74. AMS, 1990.
http://www.mccurley.org/papers/dlog.pdf.

C. Pomerance.
Fast, rigorous factorization and discrete logarithm algorithms.
In D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, editors, *Discrete algorithms and complexity*, pages 119–143, Orlando, Florida, 1987. Academic Press.
https://math.dartmouth.edu/~carlp/disclog.pdf.

O. Schirokauer.
Discrete logarithms and local units.
Philos. Trans. Roy. Soc. London Ser. A, 345(1676) :409–423, 1993.
http://rsta.royalsocietypublishing.org/content/345/1676/409, http://doi.org/10.1098/rsta.1993.0139.

A. E. Western and J. C. P. Miller.
Tables of Indices and Primitive Roots, volume 9 of *Royal Society Mathematical Tables*.
Cambridge University Press, 1968.