Algorithmes arithmétiques pour la cryptologie — 17 octobre 2016, Paris

Le crible algébrique (NFS)

Razvan Barbulescu
CNRS et IMJ-PRG

Plan du cours

- Crible algébrique (NFS)
- Corps finis p^n avec $n > 1$

Sélection polynomiale

Exemple facile $p = 65537$

$f = x^2 + 1$ et $g = x - 256$ ont une racine commune modulo p car $p = 256^2 + 1$.

Cas général (méthode de la base m): ex $p = 314159$

- on choisit d en fonction des autres étapes de l'algorithme, en pratique $d \leq 6$, par exemple $d = 2$;
- on choisit un entier m proche de $p^{\frac{1}{d+1}}$, par exemple $m = 100 \approx 314159^{\frac{1}{3}}$;
- on écrit p en base m, par exemple $p = 31 \cdot 100^2 + 41 \cdot 100 + 59$, et on pose $f = 31x^2 + 41x + 59$ et $g = x - m = x - 100$.

En effet, f et g ont m comme racine commune modulo p.

Collecte de relations

Crible (identique dans le cas facile et le cas général)

Fixer deux paramètrs E et B. Énumérer toutes les paires (a, b) d'entiers de valeur absolue $\leq E$ pour un paramètre E, avec $a > 0$, et trouver celles où

- $\sum_{i=0}^{d} f_i a^i b^{d-i}$ est B-friable;
- $a - bm$ est B-friable;
- $\gcd(a, b) = 1$.

Exemple $p = 314159$

- $E = B = 50$;
- conditions: $\gcd(a, b) = 1$ et $31a^2 + 41ab + 59b^2$ et $a - 100b$ sont 50-friables;
- relations=$\{$(1, 0), (2, -9), (3, -4), (4, -11), (4, -1), (4, 3), (4, 31), (5, -4), (5, -1), (5, 2), (5, 16), (5, 27), (6, 1), (7, -38), (8, -25), (8, -1), (9, -2), (10, -3), (11, -32), (11, 3), (11, 10), (13, 1), (16, 5), (18, -11), (19, -14), (25, -19), (25, 24), (25, 49), (26, 17), (28, -41), (29, -43), (31, 4), (34, 3), (35, -26), (41, -8), (44, -29), (45, -31)$\}$.

Exemple $p = 65537$

- $E = 50$ et $B = 20$;
- conditions: $\gcd(a, b) = 1$ et $a^2 + b^2$ et $a - 256b$ sont 20-friables;
- relations=$\{$ (0, -1), (0, 1), (1, -2), (1, 0), (1, 1), (2, -3), (4, -1), (4, 1), (7, 24), (8, -1), (12, -5), (13, 1), (16, -13), (18, 1), (23, -7), (23, 11), (24, 7), (32, 43), (38, -1), (41, -23), (46, 3), (47, 1)$\}$.

Intermezzo mathématique

Factorisation dans un corps de nombres

Si $f \in \mathbb{Q}[x]$ on note α une racine complexe de f. Alors tout entier de de $\mathbb{Q}(\alpha)$ se factorise de manière unique en idéaux premiers (théorie algébrique des nombres).

exemple facile $f = x^2 + 1$: L'anneau des entiers est

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

Theorème: Les éléments premiers de $\mathbb{Z}[i]$ sont $1 + i$, les premiers de $\mathbb{Z}$ congriuents à 3 modulo 4 et les nombres $a \pm ib$ où $a, b \in \mathbb{Z}$ sont tels que $a^2 + b^2 = p$ premier congruent à 1 modulo 4.

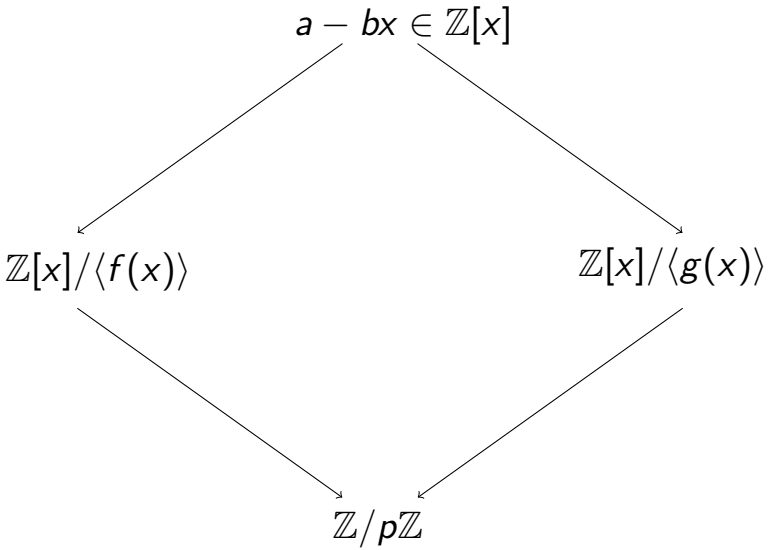
Norme d'un élément d'un corps de nombres

- cas général: on appelle norme de $a \in \mathbb{Q}(\alpha)$ le déterminant de l'application $x \mapsto ax$. Théorème: la norme de a est le produit des normes des iéaux premiers de sa factorisation (norm d'un idéal=indice dans l'anneau des entiers).
- cas de $f = x^2 + 1$: $N(a + ib) = a^2 + b^2 = |a + ib|^2$. Par exemple $8 + i = (-i)(2 + 3i)(2 + i)$ et alors $N(8 + i) = 8^2 + 1 = N(i)N(2 + 3i)N(2 + i) = 1 \cdot (2^2 + 3^2) \cdot (2^2 + 1^2)$.

Construction des équations (1/2)

NFS for DLP in $\mathbb{F}_p$

Soient $f, g \in \mathbb{Z}[x]$ deux polynômes irréductibles, qui ont une racine commune m modulo p.



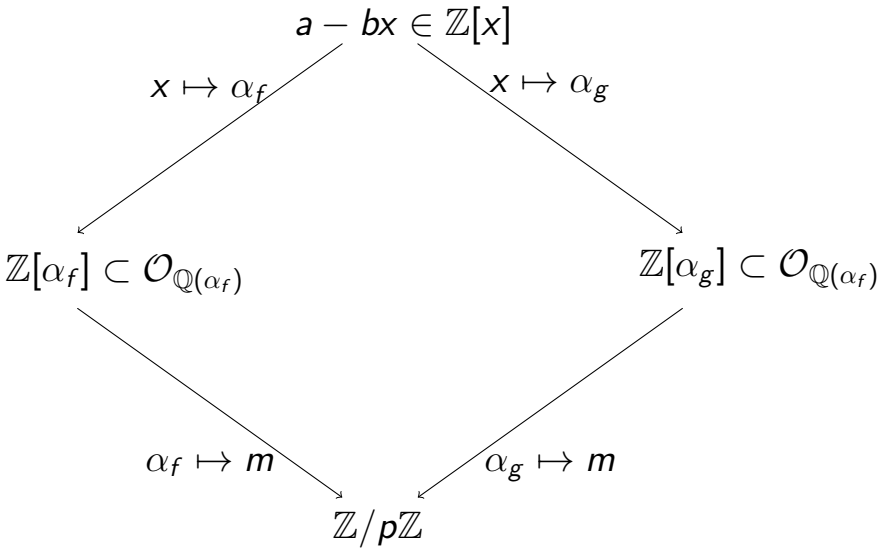
Calculs dans $\mathbb{Z}[\alpha_f]$?

- Les parties mathématiques sont négligeables en temps, mais causent de bugs.
- Implantations disponibles: PARI/GP, Magma, CADO.

Construction des équations (1/2)

NFS for DLP in $\mathbb{F}_p$

Soient $f, g \in \mathbb{Z}[x]$ deux polynômes irréducibles, qui ont une racine commune m modulo p.



Calculs dans $\mathbb{Z}[\alpha_f]$?

- Les parties mathématiques sont négligeables en temps, mais causent de bugs.
- Implantations disponibles: PARI/GP, Magma, CADO.

Construction des équations (2/2)

Exemple cas facile $p = 65537$ et $(a, b) = (8, -1)$

- 1ère demi-équation: $a - ib = 8 + i = (-i)(2 + 3i)(2 + i)$ d'où $8 + 256 \equiv (-256)(2 + 3 \cdot 256)(2 + 256) \pmod{65537}$.
- 2ème demi-équation: $a - mb = 8 - 256 \cdot (-1) = 264 = 2^3 \cdot 3 \cdot 11$ d'où $8 + 256 \equiv 2^3 \cdot 3 \cdot 11 \pmod{65537}$.
- équation: $(-256)(2 + 3 \cdot 256)(2 + 256) \equiv 2^3 \cdot 3 \cdot 11 \pmod{65537}$ d'où $\log(-256) + \log(2 + 3 \cdot 256) + \log(2 + 3 \cdot 256) \equiv 3 \log 2 + \log 3 + \log 11 \pmod{65537 - 1}$

Inconnues

- base de facteurs = les éléments premiers de $\mathbb{Z}[\alpha_f]$ de norme $\leq B$(ou des idéaux premiers de $\mathcal{O}_{\mathbb{Q}(\alpha)}$ dont la norme est puissance d'un premier $\leq B$) pour le côté de f et les nombres premiers rationnels de norme $\leq B$ pour le côté de g.
- inconnues: logarithmes discrets des images dans $\mathbb{Z}/p\mathbb{Z}$ des éléments de la base de facteurs.

Lemme

La norme de $a - b\alpha_f$, $\sum_{i=0}^{\deg f} f_i a^i b^{\deg f - i}$, est B-friable si et seulement si tous les facteurs de $a - b\alpha_f$ sont dans la base de facteurs.

Algèbre linéaire

Matrice M

- lignes = relations (a, b)
- colonnes = base de facteurs
- M(relation,premier π de $\mathcal{O}_{\mathbb{Q}(\alpha)}$)$=\pm \mathrm{val}_\pi(a - b\alpha)$ avec signe $+$ pour f et $-$ pour g.

Example $f = x^2 + 1$**,** $(a, b) = (8, -1)$**:** $M\left((a, b), (2 + i)\right) = 1$.

Wiedemann

- l'algèbre linéaire consiste à résoudre l'équation $Mx = 0$;
- coût: $B^{2+o(1)}$ car la base de facteurs a $(2 + o(1))B/\log B$ éléments;
- résultat: logarithmes discrets des éléments de la base de facteurs.

Changement de complexité

Idée

Au lieu de demander la friabilité d'un nombre grand on demande la friabilité de 2 nombres très petits: les normes $\sum_{i=0}^{d} f_i a^i b^{d-i}$ et $a - bm$.

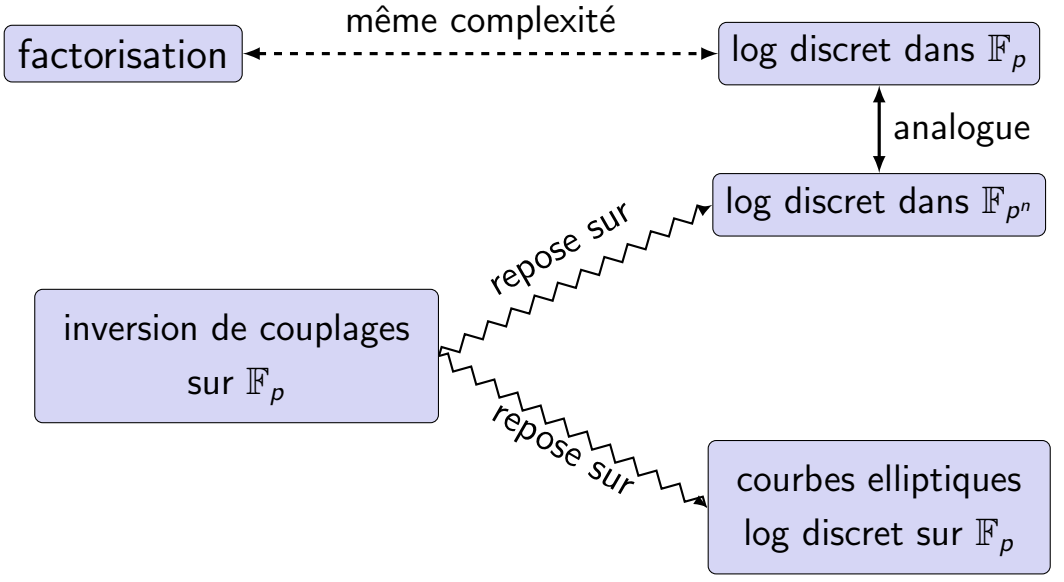
Pourquoi $L_p(1/3)$?

- Les normes ont taille $\sum_{i=0}^{d} f_i a^i b^{d-i} \approx E^d p^{\frac{1}{d}}$ et $g \approx E p^{\frac{1}{d}}$.
- En prenant $E \approx 2^{\sqrt[3]{\log p}}$ et $d = \sqrt[3]{\log p}$ les deux normes ont taille $2^{(\sqrt[3]{\log p})^2}$.
- Le théorème de Canfield-Erdös-Pomerance dit que pour $B \approx 2^{\sqrt[3]{\log p}}$ la probabilité qu'une des deux normes soit B-friable est $1/2^{\sqrt[3]{\log p}}$.
- Le coût du crible est $E^{2+o(1)} = L(1/3)$, ça donne autant d'équation que d'inconnues. Le coût de l'algèbre linéaire est $B^{2+o(1)}$

Plan du cours

- Crible algébrique (NFS)
- Corps finis p^n avec $n > 1$

Les relations du log discret et couplages



F_Q est un corps à Q éléments, Q puissance de premier.

Chronologie

Calcul d'indice

- $\mathbb{F}_p$, '79, Adleman
- $\mathbb{F}_{2^n}$, '80, Hellman Reyneri, utiliser des polynômes à la place des nombres
- $\mathbb{F}_{p^n}$, '94, Adleman DeMarrais, $\mathbb{F}_{p^n} = \mathbb{Z}[\iota]/p\mathbb{Z}[\iota]$.

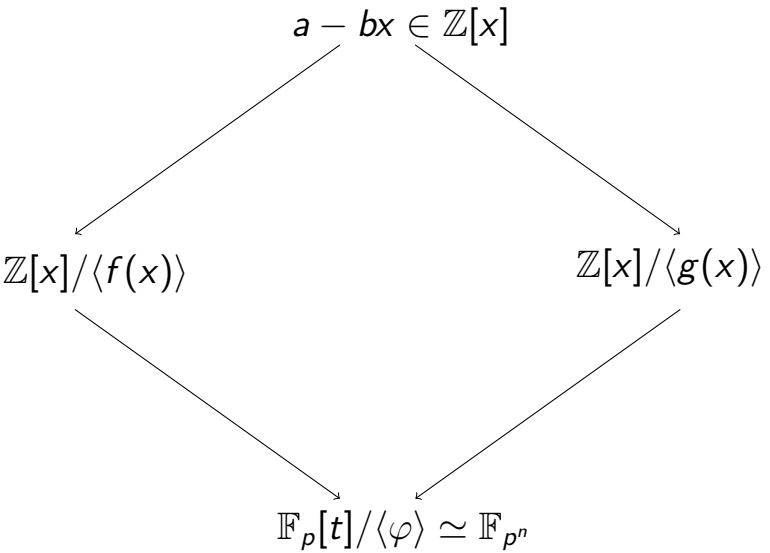
NFS et FFS

- $\mathbb{F}_p$, '93, Gordon / Schirokauer
- $\mathbb{F}_{2^n}$, '94, Adleman, utiliser des polynômes à la place des nombres
- $\mathbb{F}_{p^n}$,
  - '00, Schirokauer, $\mathbb{F}_{p^n} = \mathbb{Z}[\iota]/p\mathbb{Z}[\iota]$ (TNFS).
  - '06, Joux Lercier Smart Vercauteren, modifier la sélection polynomiale (JLSV)
  - '16, Kim et Barbulescu, combiner TNFS et JLSV: exTNFS

The idea of Joux Lercier Smart Vercauteren

Polynomial selection

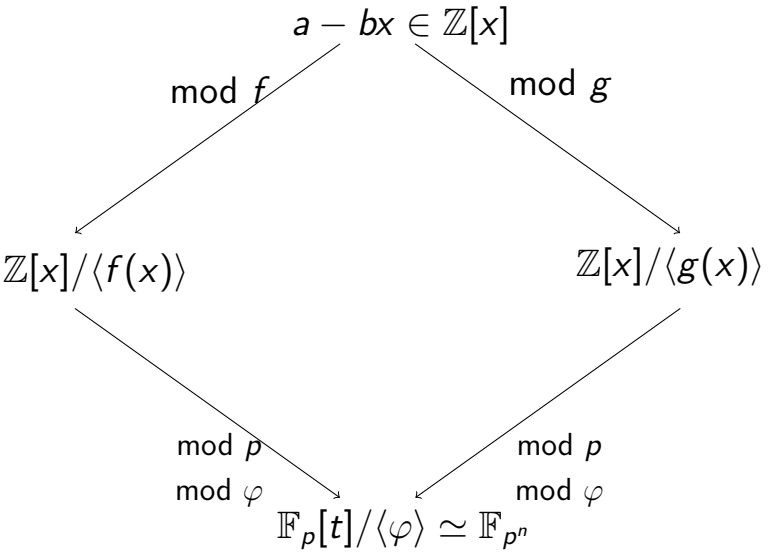
Select f and g which have a common ~~root~~ factor φ of degree n modulo p.



The idea of Joux Lercier Smart Vercauteren

Polynomial selection

Select f and g which have a common ~~root~~ factor φ of degree n modulo p.



JLSV en pratique

Modifications

Unique modification: sélection polynomial et les 2 côtés du crible sont non-liéaires.

- implémentation de Joux et Lercier était compatible depuis 2003;
- CADO-NFS accepte 2 polynômes non-linéaires depuis 2014.

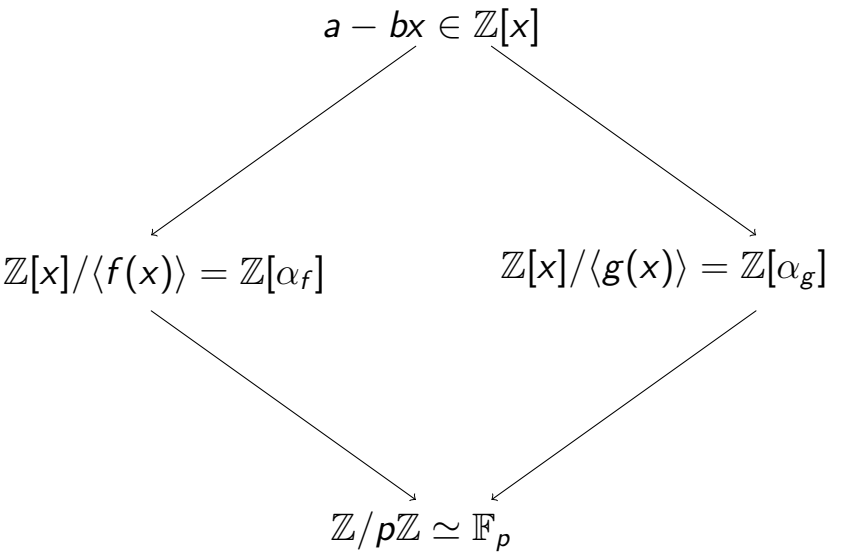
Records

- 2006, Joux Lercier Smart Vercauteren, $\mathbb{F}_{p^3}$, 120dd.
- 2014, Barbulescu Gaudry Guillevic Morain, $\mathbb{F}_{p^2}$, 180dd.
- 2015, Barbulescu Gaudry Guillevic Morain, $\mathbb{F}_{p^4}$, 120dd.
- 2015, Barbulescu Gaudry Guillevic Morain, $\mathbb{F}_{p^3}$ 156dd.
- 2016, Gaudry Grémy Videau, $\mathbb{F}_{p^6}$ 100dd.
- 2016, Gaudry Guillevic Morain, $\mathbb{F}_{p^3}$ 180dd.

Le diagramme TNFS

NFS pour DLP dans $\mathbb{F}_p$

Soient $f, g \in \mathbb{Z}[x]$ deux polynômes irréductibles ayant une racine commune m modulo p.

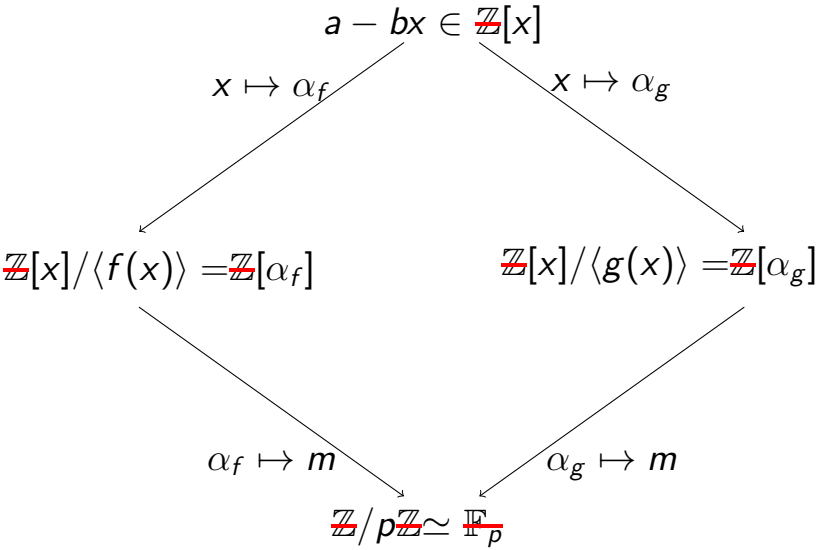


Le diagramme TNFS

NFS pour DLP dans $\mathbb{F}_p$

Soient $f, g \in \mathbb{Z}[x]$ deux polynômes irréductibles ayant une racine commune m modulo p.

Soit $h \in \mathbb{Z}[x]$ un polynôme unitaire de degré n qui est irréductible modulo p; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.

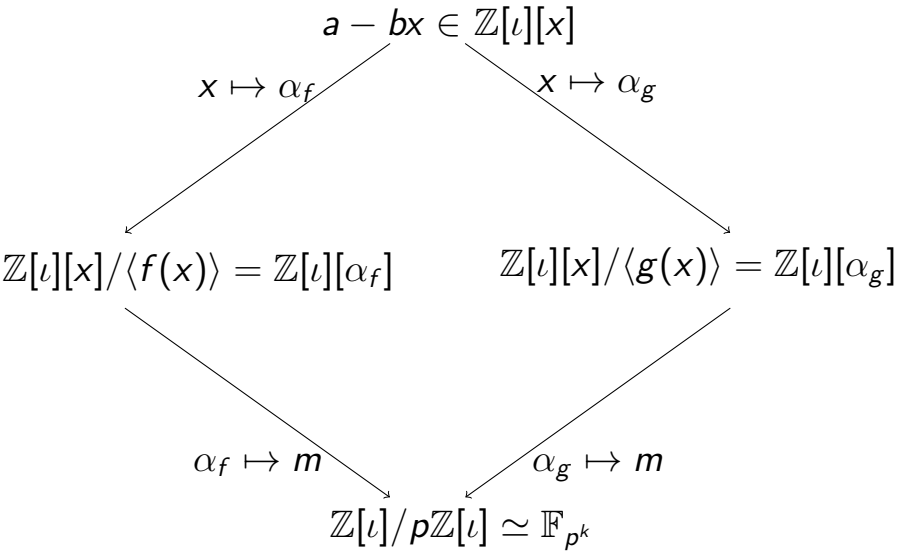


Le diagramme TNFS

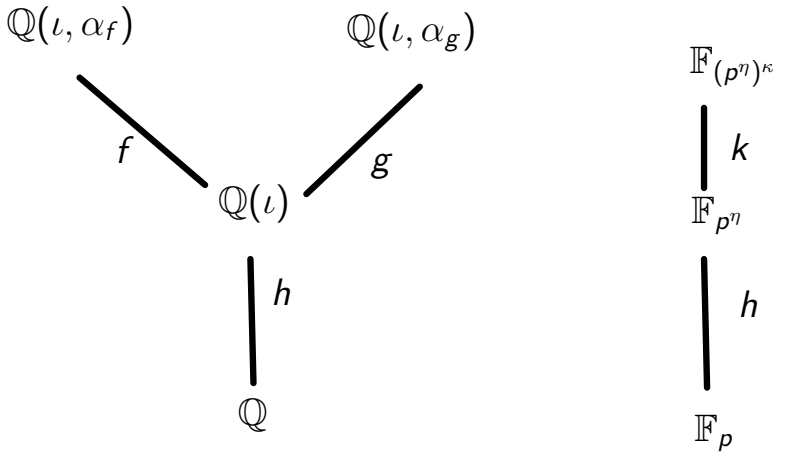
NFS pour DLP dans $\mathbb{F}_{p^k}$

Soient $f, g \in \mathbb{Z}[x]$ deux polynômes irréductibles ayant une racine commune m modulo p.

Soit $h \in \mathbb{Z}[x]$ un polynôme unitaire de degré n qui est irréductible modulo p; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.



Le TNFS étendu

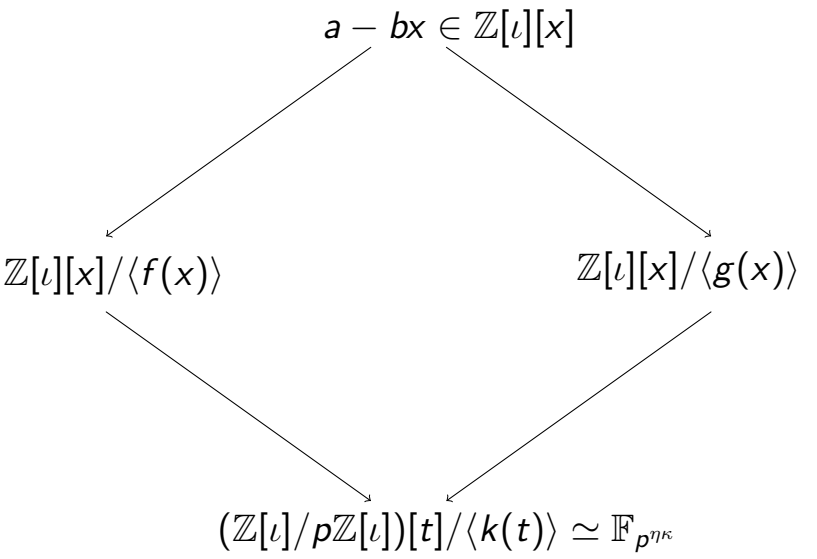


L'algorithme exTNFS

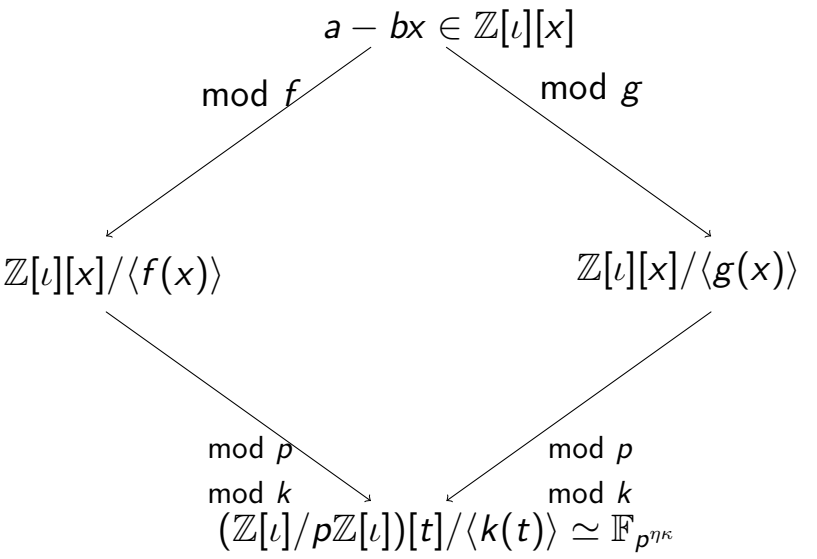
contraintes: $n = \eta\kappa$ avec $\gcd(\eta, \kappa) = 1$

1. choisir h comme dans TNFS pour $\mathbb{F}_{p^\eta}$;
2. choisir f et g comme pour $\mathbb{F}_{p^\kappa}$; poser $k = \gcd(f \bmod p, g \bmod p)$;
3. continuer comme dans TNFS.

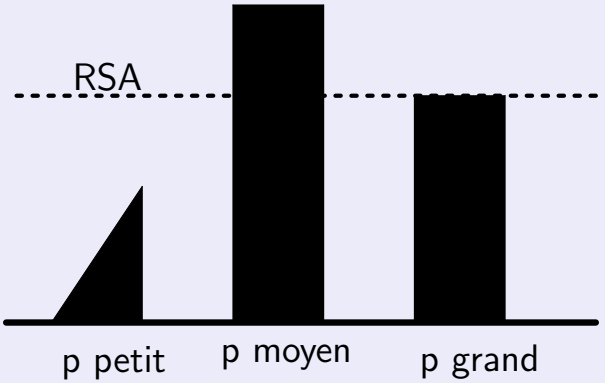
exTNFS diagram



exTNFS diagram

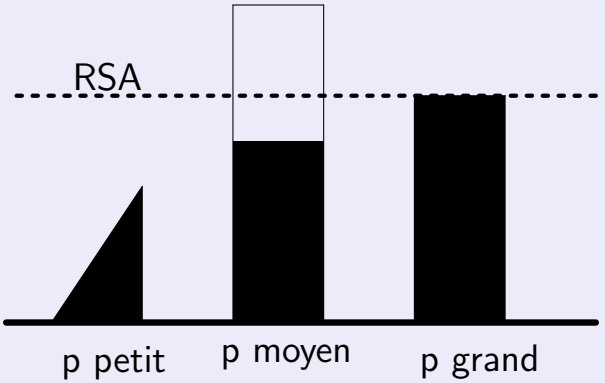


Conséquences d'exTNFS (1/2)



- le cas de p moyen était plus dur que la factorisation comme complexité asymptotique;

Conséquences d'exTNFS (1/2)



- le cas de p moyen était plus dur que la factorisation comme complexité asymptotique;
- à cause d'exTNFS la situation a changé
- en pratique $n = 2$ est déjà dans le cas moyen.

Conséquences d'exTNFS (2/2)

Quand p a une forme spéciale la complexité de NFS est $L_{p^n}(1/3, (c/9)^{\frac{1}{3}}$ avec c comme suit

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	$2/3 < \ell_p < 1$
SNFS-(JP 2013)	64	32
STNFS (BGK 2015)	none	32
SexTNFS (Kim-B. 2016)	32	32

Barreto-Naehrig (BN)

Les standards de l'ENISA cotenait des erreurs pour les couplages BN. La courbe estimée initialement à 128 bits de sécurité n'en a que ≤ 115 (Kim Barbulescu 2016).