The Multiple Number Field Sieve with Conjugation and Generalized Joux-Lercier Methods

Cécile Pierrot [1,2]

[1,] DGA and CNRS, France
[2] Laboratoire d'Informatique de Paris 6
UPMC, Sorbonne-Universités

May 27th, 2015

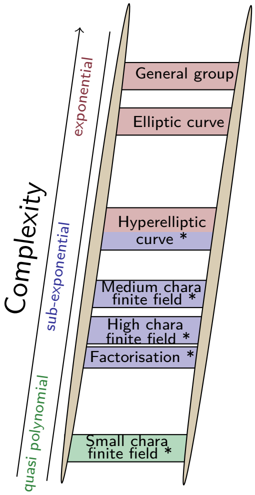
Eurocrypt Conference, Sofia, Bulgaria

The Discrete Logarithm Problem (DLP)

- Multiplicative group G generated by g: solving the discrete logarithm problem in G, is inverting the map $x \mapsto g^x$
- A hard problem in general, and used as such in cryptography.

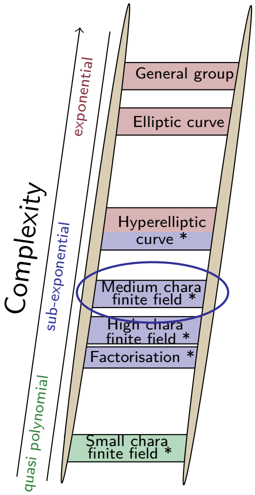
The Discrete Logarithm Problem (DLP)

- Multiplicative group G generated by g: solving the discrete logarithm problem in G, is inverting the map $x \mapsto g^x$
- A hard problem in general, and used as such in cryptography.
- Several groups in practice:



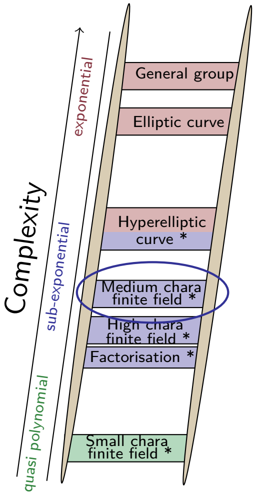
The Discrete Logarithm Problem (DLP)

- Multiplicative group G generated by g: solving the discrete logarithm problem in G, is inverting the map $x \mapsto g^x$
- A hard problem in general, and used as such in cryptography.
- Several groups in practice:



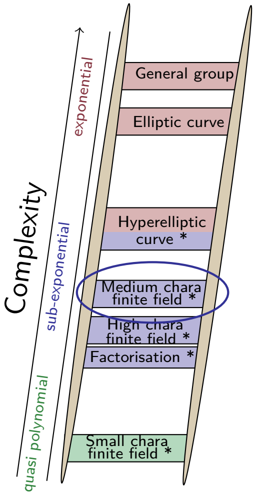
The Discrete Logarithm Problem (DLP)

- Multiplicative group G generated by g: solving the discrete logarithm problem in G, is inverting the map $x \mapsto g^x$
- A hard problem in general, and used as such in cryptography.
- Several groups in practice:
- Two families of algorithms :
  - Generic algorithms (Pollard's Rho, Pohlig-Hellman...)
  - Specific algorithms (Index Calculus *)



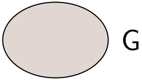
The Discrete Logarithm Problem (DLP)

- Multiplicative group G generated by g: solving the discrete logarithm problem in G, is inverting the map $x \mapsto g^x$
- A hard problem in general, and used as such in cryptography.
- Several groups in practice:
- Two families of algorithms :
  - Generic algorithms (Pollard's Rho, Pohlig-Hellman...)
  - Specific algorithms (Index Calculus *)



Index Calculus Algorithms

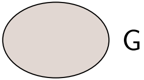
If you want to compute Discrete Logs in G:



1. Collection of Relations (or Sieving Phase)

Index Calculus Algorithms

If you want to compute Discrete Logs in G:

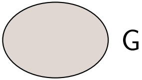


1. Collection of Relations (or Sieving Phase)
   $\rightarrow$ Create a lot of sparse multiplicative relations between some (small) specific elements = the factor base

$$\prod g_i^{e_i} = \prod g_i^{e_i'}$$

Index Calculus Algorithms

If you want to compute Discrete Logs in G:



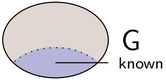
1. Collection of Relations (or Sieving Phase)
   $\rightarrow$ Create a lot of sparse multiplicative relations between some (small) specific elements = the factor base

$$\prod g_i^{e_i} = \prod g_i^{e_i'} \quad \Rightarrow \quad \sum (e_i - e_i') \log(g_i) = 0$$

   $\rightarrow$ So a lot of sparse linear equations

Index Calculus Algorithms

If you want to compute Discrete Logs in G:



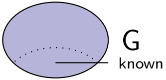
1. Collection of Relations (or Sieving Phase)
   $\rightarrow$ Create a lot of sparse multiplicative relations between some (small) specific elements = the factor base

$$\prod g_i^{e_i} = \prod g_i^{e_i'} \quad \Rightarrow \quad \sum (e_i - e_i') \log(g_i) = 0$$

   $\rightarrow$ So a lot of sparse linear equations
2. Linear Algebra
   $\rightarrow$ Recover the Discrete Logs of the factor base

Index Calculus Algorithms

If you want to compute Discrete Logs in G:



1. Collection of Relations (or Sieving Phase)
   $\rightarrow$ Create a lot of sparse multiplicative relations between some (small) specific elements = the factor base

$$\prod g_i^{e_i} = \prod g_i^{e_i'} \quad \Rightarrow \quad \sum (e_i - e_i') \log(g_i) = 0$$

   $\rightarrow$ So a lot of sparse linear equations
2. Linear Algebra
   $\rightarrow$ Recover the Discrete Logs of the factor base
3. Individual Logarithm Phase
   $\rightarrow$ Recover the Discrete Log of an arbitrary element

Sieving Phase and Commutative Diagram

- How to obtain relations?

$$
\begin{tikzcd}
 & E \arrow[dl, "u_1"'] \arrow[dr, "u_2"] & \\
E_1 \arrow[dr, "v_1"] & & E_2 \arrow[dl, "v_2"'] \\
 & G &
\end{tikzcd}
$$

Sieving Phase and Commutative Diagram

- How to obtain relations?

$$\begin{tikzcd}
& E \arrow[dl, "u_1"] \arrow[dr, "u_2"] & \\
E_1 \arrow[dr, "v_1"] & & E_2 \arrow[dl, "v_2"] \\
& G &
\end{tikzcd}$$

$\forall x \in E, v_1(u_1(x)) = v_2(u_2(x))$ thanks to commutativity.

Sieving Phase and Commutative Diagram

- How to obtain relations?

$$
\begin{tikzcd}
 & E \arrow[dl, "u_1"'] \arrow[dr, "u_2"] & \\
B_1 \subset E_1 \arrow[dr, "v_1"] & & E_2 \supset B_2 \arrow[dl, "v_2"'] \\
 & G &
\end{tikzcd}
$$

$\forall x \in E, v_1(u_1(x)) = v_2(u_2(x))$ thanks to commutativity.

- How to obtain "good" relations ?
  - Define B_1 and B_2 two small sets.
    Factor base $:= v_1(B_1) \bigcup v_2(B_2)$

Sieving Phase and Commutative Diagram

- How to obtain relations?

$$\begin{tikzcd}
 & & E \arrow[dl, "u_1"'] \arrow[dr, "u_2"] & & \\
B_1 \subset & E_1 \arrow[dr, "v_1"'] & & E_2 \arrow[dl, "v_2"] & \supset B_2 \\
 & & G & &
\end{tikzcd}$$

$$\forall x \in E, v_1(u_1(x)) = v_2(u_2(x)) \quad \text{thanks to commutativity.}$$

- How to obtain "good" relations ?
  - Define B_1 and B_2 two small sets.
    Factor base $:= v_1(B_1) \bigcup v_2(B_2)$
  - Keep only x such that $u_i = \prod_{b_i \in B_i} b_i$ and get:

$$v_1(u_1(x)) = v_2(u_2(x))$$

Sieving Phase and Commutative Diagram

- How to obtain relations?

$$\begin{tikzcd}
 & E \arrow[dl, "u_1"'] \arrow[dr, "u_2"] & \\
B_1 \subset E_1 \arrow[dr, "v_1"] & & E_2 \supset B_2 \arrow[dl, "v_2"] \\
 & G &
\end{tikzcd}$$

$\forall x \in E, v_1(u_1(x)) = v_2(u_2(x))$ thanks to commutativity.

- How to obtain "good" relations ?
  - Define B_1 and B_2 two small sets.
    Factor base $:= v_1(B_1) \bigcup v_2(B_2)$
  - Keep only x such that $u_i = \prod_{b_i \in B_i} b_i$ and get:

$$v_1\Big(\prod_{b_i \in B_2} b_i\Big) = v_2\Big(\prod_{b_i \in B_2} b_i\Big)$$

Sieving Phase and Commutative Diagram

- How to obtain relations?

$$\begin{tikzcd} & E \arrow[dl, "u_1"'] \arrow[dr, "u_2"] & \\ B_1 \subset E_1 \arrow[dr, "v_1"'] & & E_2 \supset B_2 \arrow[dl, "v_2"] \\ & G & \end{tikzcd}$$

$\forall x \in E, v_1(u_1(x)) = v_2(u_2(x))$ thanks to commutativity.

- How to obtain "good" relations ?
    - Define B_1 and B_2 two small sets.
      Factor base $:= v_1(B_1) \bigcup v_2(B_2)$
    - Keep only x such that $u_i = \prod_{b_i \in B_i} b_i$ and get:

$$\prod_{b_i \in B_2} v_1(b_i) = \prod_{b_i \in B_2} v_2(b_i)$$ thanks to linearity.

Number Field Sieve (NFS)

- Solves the DLP for medium and high characteristic fields $\mathbb{F}_{p^n}$.
- Belongs to the family of Index Calculus algorithms
  $\Rightarrow$ 3 phases.

Number Field Sieve (NFS)

- Solves the DLP for medium and high characteristic fields $\mathbb{F}_{p^n}$.
- Belongs to the family of Index Calculus algorithms
  $\Rightarrow$ 3 phases.
- Commutative Diagram ? With $m \in \mathbb{F}_{p^n}$ a root of f_1 and f_2 :

$$
\begin{tikzcd}
 & \mathbb{Z}[X] \arrow[dl, "X \mapsto \theta_1"'] \arrow[dr, "X \mapsto \theta_2"] & \\
\mathbb{Q}[X]/(f_1(X)) \cong \mathbb{Q}(\theta_1) \arrow[dr, "\theta_1 \mapsto m"] & & \mathbb{Q}(\theta_2) \cong \mathbb{Q}[X]/(f_2(X)) \arrow[dl, "\theta_2 \mapsto m"'] \\
 & \mathbb{F}_{p^n} &
\end{tikzcd}
$$

Number Field Sieve (NFS)

- Solves the DLP for medium and high characteristic fields $\mathbb{F}_{p^n}$.
- Belongs to the family of Index Calculus algorithms
  $\Rightarrow$ 3 phases.
- Commutative Diagram ? With $m \in \mathbb{F}_{p^n}$ a root of f_1 and f_2 :

$$\begin{tikzcd}
 & \mathbb{Z}[X] \arrow[dl, "X \mapsto \theta_1"'] \arrow[dr, "X \mapsto \theta_2"] & \\
\mathbb{Q}[X]/(f_1(X)) \cong \mathbb{Q}(\theta_1) \arrow[dr, "\theta_1 \mapsto m"] & & \mathbb{Q}(\theta_2) \cong \mathbb{Q}[X]/(f_2(X)) \arrow[dl, "\theta_2 \mapsto m"'] \\
 & \mathbb{F}_{p^n} &
\end{tikzcd}$$

Factor base ? $B_i :=$ prime ideals (of the ring of integers) with a norm smaller than a certain smoothness* bound.

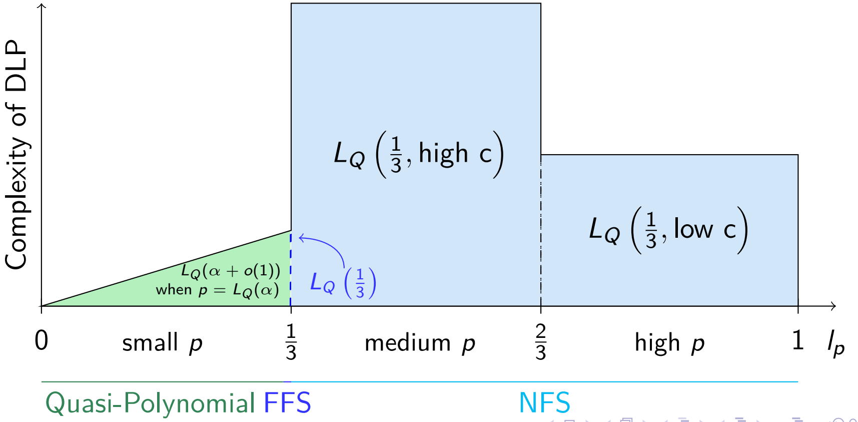
*An ideal $\mathfrak{I}$ is B-smooth if all its factors have norms lower than B.

Complexities

- Notation : $L_Q(\alpha, c) = \exp\left(c(\log Q)^{\alpha}(\log \log Q)^{1-\alpha}\right)$

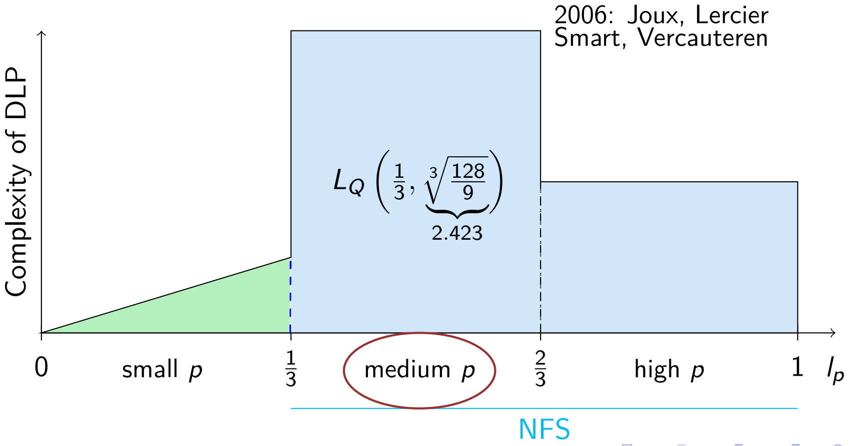
Complexities

- Notation : $L_Q(\alpha, c) = \exp\left(c(\log Q)^\alpha (\log\log Q)^{1-\alpha}\right)$
- In $\mathbb{F}_Q$ of characteristic $p = L_Q(l_p, c)$:



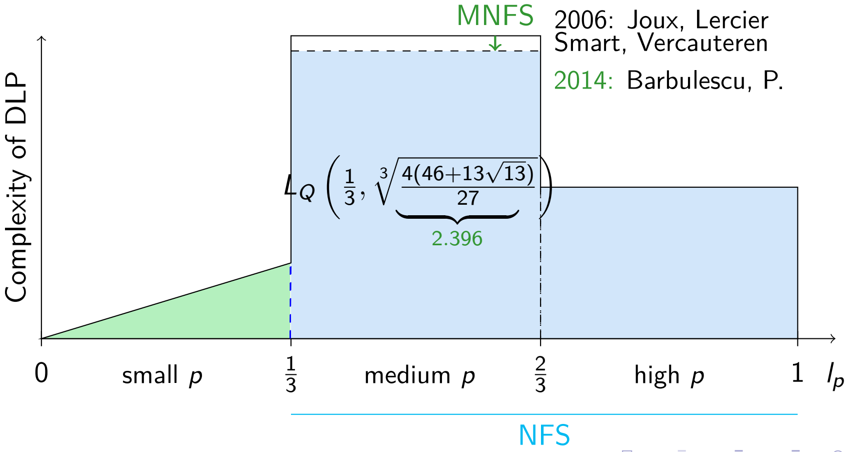
Complexities

- Notation : $L_Q(\alpha, c) = \exp\left(c(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}\right)$
- In $\mathbb{F}_Q$ of characteristic $p = L_Q(l_p, c)$:



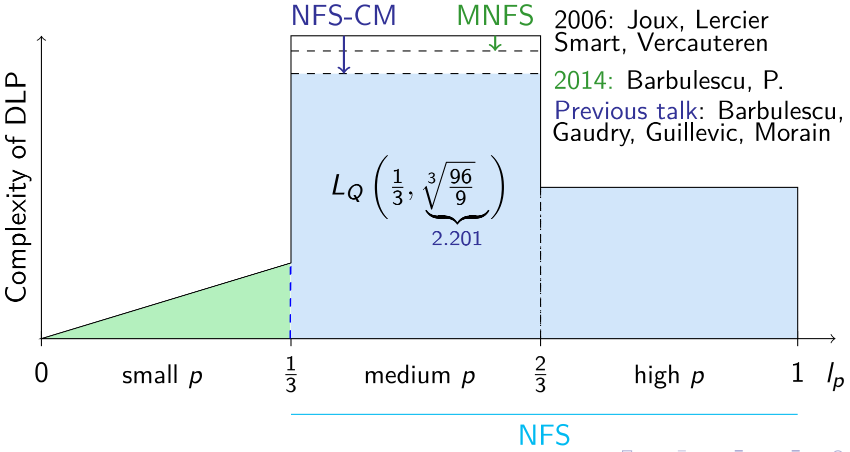
Complexities

- Notation : $L_Q(\alpha, c) = \exp\left(c(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}\right)$
- In $\mathbb{F}_Q$ of characteristic $p = L_Q(l_p, c)$:



Complexities

- Notation : $L_Q(\alpha, c) = \exp\left(c(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}\right)$
- In $\mathbb{F}_Q$ of characteristic $p = L_Q(l_p, c)$:



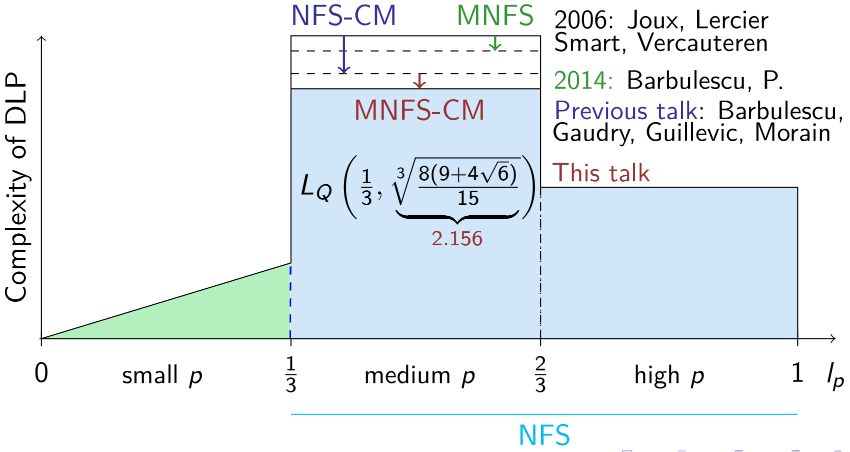
2006: Joux, Lercier
Smart, Vercauteren

2014: Barbulescu, P.

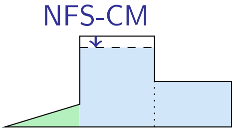
Previous talk: Barbulescu, Gaudry, Guillevic, Morain

Complexities

- Notation : $L_Q(\alpha, c) = \exp\left(c(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}\right)$
- In $\mathbb{F}_Q$ of characteristic $p = L_Q(l_p, c)$:



Polynomial Selection



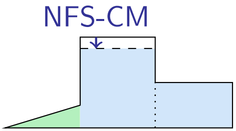
Preliminaries to the diagram:

Find two polynomials f_1 and f_2 with an irreducible factor $\mathcal{I}$ of degree n modulo p.

- Define $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(\mathcal{I})$.
- $\Rightarrow$ f_1 and f_2 have a common root $m \in \mathbb{F}_{p^n}$.

† $\mathrm{Norm}_{\mathbb{Q}[X]/(f)}(\varphi) = \mathrm{Res}(\varphi, f)$ if f is monic.

Polynomial Selection



Preliminaries to the diagram:

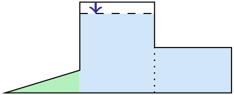
Find two polynomials f_1 and f_2 with
an irreducible factor $\mathcal{I}$ of degree n modulo p.

- Define $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(\mathcal{I})$.
- $\Rightarrow f_1$ and f_2 have a common root $m \in \mathbb{F}_{p^n}$.

Requirement: Good prob. to obtain a relation

† $\mathrm{Norm}_{\mathbb{Q}[X]/(f)}(\varphi) = \mathrm{Res}(\varphi, f)$ if f is monic.

Polynomial Selection



Preliminaries to the diagram:

Find two polynomials f_1 and f_2 with an irreducible factor $\mathcal{I}$ of degree n modulo p.

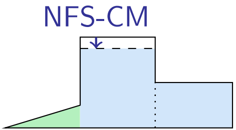
- Define $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(\mathcal{I})$.
- $\Rightarrow$ f_1 and f_2 have a common root $m \in \mathbb{F}_{p^n}$.

Requirement: Good prob. to obtain a relation

$\rightarrow$ Good prob. for a norm to be smooth

† $\mathrm{Norm}_{\mathbb{Q}[X]/(f)}(\varphi) = \mathrm{Res}(\varphi, f)$ if f is monic.

Polynomial Selection



Preliminaries to the diagram:

Find two polynomials f_1 and f_2 with an irreducible factor $\mathcal{I}$ of degree n modulo p.

- Define $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(\mathcal{I})$.
- $\Rightarrow$ f_1 and f_2 have a common root $m \in \mathbb{F}_{p^n}$.

Requirement: Good prob. to obtain a relation

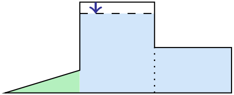
$\rightarrow$ Good prob. for a norm to be smooth

$\rightarrow$ Small norms† in the two number fields

† $\mathrm{Norm}_{\mathbb{Q}[X]/(f)}(\varphi) = \mathrm{Res}(\varphi, f)$ if f is monic.

Polynomial Selection

NFS-CM



Preliminaries to the diagram:

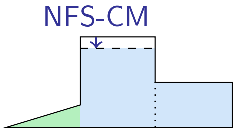
Find two polynomials f_1 and f_2 with
an irreducible factor $\mathcal{I}$ of degree n modulo p.

- Define $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(\mathcal{I})$.
- $\Rightarrow$ f_1 and f_2 have a common root $m \in \mathbb{F}_{p^n}$.

Requirement: Good prob. to obtain a relation
$\rightarrow$ Good prob. for a norm to be smooth
$\rightarrow$ Small norms† in the two number fields
$\rightarrow$ f_1 and f_2 with not too high degrees and not too large coefficients.

$^\dagger\mathrm{Norm}_{\mathbb{Q}[X]/(f)}(\varphi) = \mathrm{Res}(\varphi, f)$ if f is monic.

Polynomial Selection



Preliminaries to the diagram:

Find two polynomials f_1 and f_2 with an irreducible factor $\mathcal{I}$ of degree n modulo p. } Polynomial selection

- Define $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(\mathcal{I})$.
- $\Rightarrow$ f_1 and f_2 have a common root $m \in \mathbb{F}_{p^n}$.

Requirement: Good prob. to obtain a relation

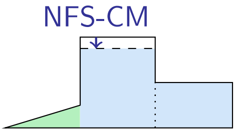
$\rightarrow$ Good prob. for a norm to be smooth

$\rightarrow$ Small norms† in the two number fields

$\rightarrow$ f_1 and f_2 with not too high degrees and not too large coefficients.

† $\mathrm{Norm}_{\mathbb{Q}[X]/(f)}(\varphi) = \mathrm{Res}(\varphi, f)$ if f is monic.

Polynomial Selection



Preliminaries to the diagram:

Find two polynomials f_1 and f_2 with an irreducible factor $\mathcal{I}$ of degree n modulo p. } Polynomial selection

- Define $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(\mathcal{I})$.
- $\Rightarrow$ f_1 and f_2 have a common root $m \in \mathbb{F}_{p^n}$.

Requirement: Good prob. to obtain a relation

$\rightarrow$ Good prob. for a norm to be smooth

$\rightarrow$ Small norms† in the two number fields

$\rightarrow$ f_1 and f_2 with not too high degrees and not too large coefficients.

New polynomial selection proposed by Barbulescu, Gaudry, Guillevic and Morain: the Conjugation Method.

† $\mathrm{Norm}_{\mathbb{Q}[X]/(f)}(\varphi) = \mathrm{Res}(\varphi, f)$ if f is monic.

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 - u g_a g_b + v {g_b}^2$. Remark that

$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 - u g_a g_b + v {g_b}^2$. Remark that
$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$
- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 - u g_a g_b + v {g_b}^2$. Remark that
$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$
- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p

n

- **Set** $f_1 = {g_a}^2 - u g_a g_b + v {g_b}^2$. Remark that
$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$
- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

Degrees

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 - u g_a g_b + v {g_b}^2$. Remark that
$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$
- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

$< n$

n

Degrees

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 - u g_a g_b + v {g_b}^2$. Remark that

$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$

- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

$< n$

n

$2n$

n

Degrees

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$

$< n$

- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p

n

- **Set** $f_1 = {g_a}^2 - u g_a g_b + v {g_b}^2$. Remark that

$2n$

$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda')g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$

- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

n

Degrees

Coeffs.

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

$< n$

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p

n small

$2n$

- **Set** $f_1 = {g_a}^2 - u g_a g_b + v {g_b}^2$. Remark that
$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$
- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

n

Degrees

Coeffs.

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

$< n$

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p

small

n

$2n$

- **Set** $f_1 = {g_a}^2 - u g_a g_b + v {g_b}^2$. Remark that

$$
\begin{aligned}
f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\
&\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p
\end{aligned}
$$

- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

n

Degrees

Coeffs.

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 + u g_a g_b + v {g_b}^2$. Remark that

$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$

- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

$< n$

n

$2n$

n

small

$\sqrt{p}$

Degrees

Coeffs.

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 + u g_a g_b + v {g_b}^2$. Remark that

$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$

- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

$2n$ small

n $\sqrt{p}$

Degrees Coeffs.

The Conjugation Method

Aim: Find two polynomials f_1 and f_2 with an irreducible factor of degree n modulo p.

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p

small

2n

- **Set** $f_1 = {g_a}^2 + u g_a g_b + v {g_b}^2$. Remark that

$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda')g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$

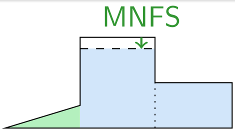
- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

n

$\sqrt{p}$

Degrees

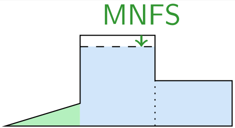
Coeffs.



The Multiple Number Field Sieve

Main idea: from 2 to V number fields.

- Idea from integer factorization [Coppersmith 93], prime fields [Matyukhin 03], high and medium characteristic [Barbulescu, P. 14].

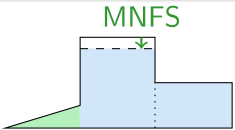


The Multiple Number Field Sieve

Main idea: from 2 to V number fields.

- Idea from integer factorization [Coppersmith 93], prime fields [Matyukhin 03], high and medium characteristic [Barbulescu, P. 14].
- With m a common root of the polynomials $f_1, \ldots, f_V$ in $\mathbb{F}_{p^n}$:

$$\begin{tikzcd}
 & & \mathbb{Z}[X] \arrow[dll] \arrow[dl] \arrow[d, "X \mapsto \theta_i"] \arrow[dr] \arrow[drr] & & \\
\mathbb{Q}(\theta_1) \arrow[drr] & \mathbb{Q}(\theta_2) \arrow[dr] & \mathbb{Q}(\theta_i) \arrow[d, "\theta_i \mapsto m"] & \mathbb{Q}(\theta_{V-1}) \arrow[dl] & \mathbb{Q}(\theta_V) \arrow[dll] \\
 & & \mathbb{F}_{p^n} & &
\end{tikzcd}$$



The Multiple Number Field Sieve

Main idea: from 2 to V number fields.

- Idea from integer factorization [Coppersmith 93], prime fields [Matyukhin 03], high and medium characteristic [Barbulescu, P. 14].
- With m a common root of the polynomials $f_1, \ldots, f_V$ in $\mathbb{F}_{p^n}$:

$$\begin{tikzcd}
 & & \mathbb{Z}[X] \arrow[dll] \arrow[dl] \arrow[d, "X \mapsto \theta_i"] \arrow[dr] \arrow[drr] & & \\
\mathbb{Q}(\theta_1) \arrow[drr] & \mathbb{Q}(\theta_2) \arrow[dr] & \mathbb{Q}(\theta_i) \arrow[d, "\theta_i \mapsto m"] & \mathbb{Q}(\theta_{V-1}) \arrow[dl] & \mathbb{Q}(\theta_V) \arrow[dll] \\
 & & \mathbb{F}_{p^n} & &
\end{tikzcd}$$

- Choice of polynomials f_1 and f_2 with a common root m in $\mathbb{F}_{p^n}$
  $\Rightarrow$ linear combination of f_1 and f_2
  $\Rightarrow$ for $i = 3, \ldots, V : f_i = \alpha_i f_1 + \beta_i f_2$ with $\alpha_i, \beta_i \approx \sqrt{V}$.

Dissymetric MNFS in one slide

Dissymmetric = when a polynomial is better than the other.

- E.g: f_1, f_2 have same size of coefficients but $\deg f_2 \geqslant \deg f_1$

Dissymetric MNFS in one slide

Dissymmetric = when a polynomial is better than the other.

- E.g: f_1, f_2 have same size of coefficients but $\deg f_2 \geqslant \deg f_1$
  $\Rightarrow$ Higher norms in $\mathbb{Q}(\theta_2), \ldots, \mathbb{Q}(\theta_V)$ than in $\mathbb{Q}(\theta_1)$.

Dissymetric MNFS in one slide

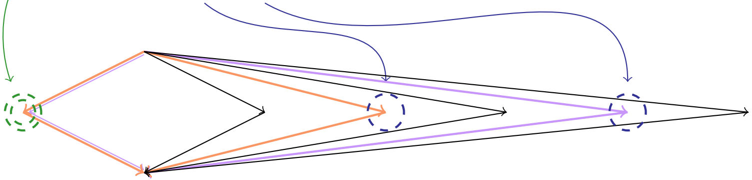
Dissymmetric = when a polynomial is better than the other.

- E.g: f_1, f_2 have same size of coefficients but $\deg f_2 \geqslant \deg f_1$ $\Rightarrow$ Higher norms in $\mathbb{Q}(\theta_2), \ldots, \mathbb{Q}(\theta_V)$ than in $\mathbb{Q}(\theta_1)$.
- Sieving: keep only polynomials that lead to a B-smooth norm in the first number field and a B'-smooth norm in (at least) one other number field.

Dissymetric MNFS in one slide

Dissymmetric = when a polynomial is better than the other.

- E.g: f_1, f_2 have same size of coefficients but $\deg f_2 \geqslant \deg f_1$ $\Rightarrow$ Higher norms in $\mathbb{Q}(\theta_2), \ldots, \mathbb{Q}(\theta_V)$ than in $\mathbb{Q}(\theta_1)$.
- Sieving: keep only polynomials that lead to a B-smooth norm in the first number field and a B'-smooth norm in (at least) one other number field.



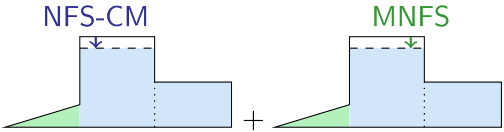
This Talk

Our aim is to combine:

This Talk

Our aim is to combine:

- the Conjugation Method
- with MNFS.

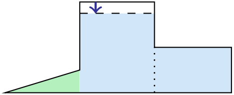


This Talk

Our aim is to combine:

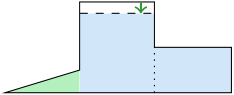
- the Conjugation Method
- with MNFS.

NFS-CM



+

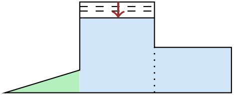
MNFS



$\Rightarrow$ Best algorithm to solve the DLP for medium characteristic finite fields $\mathbb{F}_{p^n}$.

=

MNFS-CM



Obstruction and Dreams

CM produces:

- f_1 with high degree, small coefficients
- f_2 with small degree, high coefficients

Obstruction and Dreams

CM produces:

- f_1 with high degree, small coefficients
- f_2 with small degree, high coefficients
- $\Rightarrow$ Linear combinations of f_1 and f_2 would have both inconveniences: high degrees and high coefficients.

Obstruction and Dreams

CM produces:

- f_1 with high degree, small coefficients
- f_2 with small degree, high coefficients
- $\Rightarrow$ Linear combinations of f_1 and f_2 would have both inconveniences: high degrees and high coefficients.

Our main idea:

- Linear combinations of f_1 and f_2

Obstruction and Dreams

CM produces:

- f_1 with high degree, small coefficients
- f_2 with small degree, high coefficients
- $\Rightarrow$ Linear combinations of f_1 and f_2 would have both inconveniences: high degrees and high coefficients.

Our main idea:

- Linear combinations of ~~f_1 and~~ f_2 and another polynomial f_3
- What was the f_3 of my dreams ?
  f_3 with small degree, high coefficients
  $+$ Shares the same common root m
  $+$ Independent from f_2 over $\mathbb{Q}$

Obstruction and Dreams

CM produces:

- f_1 with high degree, small coefficients
- f_2 with small degree, high coefficients
- $\Rightarrow$ Linear combinations of f_1 and f_2 would have both inconveniences: high degrees and high coefficients.

Our main idea:

- Linear combinations of $\cancel{f_1}$ ~~and~~ f_2 and another polynomial f_3
- What was the f_3 of my dreams ?
  f_3 with small degree, high coefficients
  $+$ Shares the same common root m
  $+$ Independent from f_2 over $\mathbb{Q}$
- $\Rightarrow$ Linear combinations of f_2 and f_3 have small degrees and high coefficients.

Obstruction and Dreams

CM produces:

- f_1 with high degree, small coefficients
- f_2 with small degree, high coefficients
- $\Rightarrow$ Linear combinations of f_1 and f_2 would have both inconveniences: high degrees and high coefficients.

Our main idea:

- Linear combinations of ~~f_1 and~~ f_2 and another polynomial f_3
- What was the f_3 of my dreams ?

  f_3 with small degree, high coefficients
  $+$ Shares the same common root m
  $+$ Independent from f_2 over $\mathbb{Q}$

  How to catch it ?

- $\Rightarrow$ Linear combinations of f_2 and f_3 have small degrees and high coefficients.

Catching f_3 in the Conjugation Method

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p

small

2n

- **Set** $f_1 = {g_a}^2 + ug_ag_b + v{g_b}^2$. Remark that

$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda')g_ag_b + \lambda\lambda'{g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$

- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)

n

- **Set** $f_2 = bg_a + ag_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

$\sqrt{p}$

Degrees

Coeffs.

Catching f_3 in the Conjugation Method

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 + u g_a g_b + v {g_b}^2$. Remark that

$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$

- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.)
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

n $\sqrt{p}$

Degrees Coeffs.

Catching f_3 in the Conjugation Method

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 + ug_a g_b + v{g_b}^2$. Remark that
$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda')g_a g_b + \lambda\lambda'{g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$
- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.) **and** $\lambda = a'/b' \mod p$ with $a', b' \approx \sqrt{p}$
- **Set** $f_2 = bg_a + ag_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$.

n $\sqrt{p}$

Degrees Coeffs.

Catching f_3 in the Conjugation Method

- **Start** with g_a and $g_b \in \mathbb{Z}[X]$
- **Find** u and v small integers such that $X^2 + uX + v$ is:
  - irreducible over $\mathbb{Z}[X]$ but has roots λ and λ' modulo p
  - $g_a + \lambda g_b$ is irreducible modulo p
- **Set** $f_1 = {g_a}^2 + u g_a g_b + v {g_b}^2$. Remark that

$$\begin{aligned} f_1 &\equiv {g_a}^2 + (\lambda + \lambda') g_a g_b + \lambda\lambda' {g_b}^2 \mod p \\ &\equiv (g_a + \lambda g_b)(g_a + \lambda' g_b) \mod p \end{aligned}$$

- **Rewrite** $\lambda = a/b \mod p$ with $a, b \approx \sqrt{p}$ (continued frac.) **and** $\lambda = a'/b' \mod p$ with $a', b' \approx \sqrt{p}$
- **Set** $f_2 = b g_a + a g_b$. Remark that $f_2 \equiv g_a + \lambda g_b \mod p$. **and** $f_3 = b' g_a + a' g_b$

n $\qquad\qquad\qquad\qquad$ $\sqrt{p}$

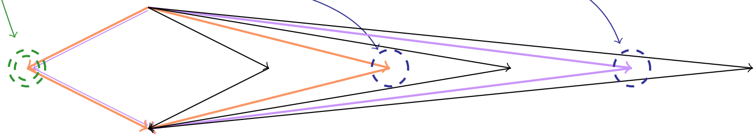
n $\qquad\qquad\qquad\qquad$ $\sqrt{p}$

Degrees $\qquad\qquad\qquad\qquad$ Coeffs.

And then ?

Construct a Multiple NFS thanks to:

- $\mathbb{Q}[X]/(f_1(X))$ on one side
- $\mathbb{Q}[X]/(f_i(X))$ on the other side, where the $V-1$ polynomials are defined as $f_i = \alpha_i f_2 + \beta_i f_3$ with $\alpha_i, \beta_i \approx \sqrt{V}$



Asymptotic Complexity Analysis

The idea is classical:

1. Choose parameters of size:
   - Sieving space : $L_Q(1/3)$
   - Smoothness bounds B and B': $L_Q(1/3)$
   - Number of number fields V: $L_Q(1/3)$

Asymptotic Complexity Analysis

The idea is classical:

1. Choose parameters of size:
   - Sieving space : $L_Q(1/3)$
   - Smoothness bounds B and B': $L_Q(1/3)$
   - Number of number fields V: $L_Q(1/3)$
2. Runtime of the sieving $\approx$ cost of the linear algebra.
3. Size of the factor base $\approx$ number of equations created (i.e. the probability to obtain a good relation multiplied by the sieving space).

Asymptotic Complexity Analysis

The idea is classical:

1. Choose parameters of size:
   - Sieving space : $L_Q(1/3)$
   - Smoothness bounds B and B': $L_Q(1/3)$
   - Number of number fields V: $L_Q(1/3)$
2. Runtime of the sieving $\approx$ cost of the linear algebra.
3. Size of the factor base $\approx$ number of equations created (i.e. the probability to obtain a good relation multiplied by the sieving space).
4. Optimize the total runtime under these constraints.

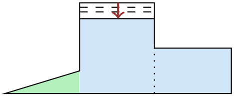
Asymptotic Complexity Analysis

The idea is classical:

1. Choose parameters of size:
   - Sieving space : $L_Q(1/3)$
   - Smoothness bounds B and B': $L_Q(1/3)$
   - Number of number fields V: $L_Q(1/3)$
2. Runtime of the sieving $\approx$ cost of the linear algebra.
3. Size of the factor base $\approx$ number of equations created (i.e. the probability to obtain a good relation multiplied by the sieving space).
4. Optimize the total runtime under these constraints.

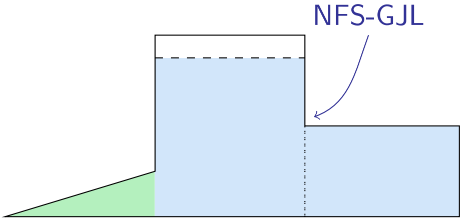
$$\Rightarrow L_Q\left(\frac{1}{3}, \sqrt[3]{\frac{8(9+4\sqrt{6})}{15}}\right)$$

MNFS-CM



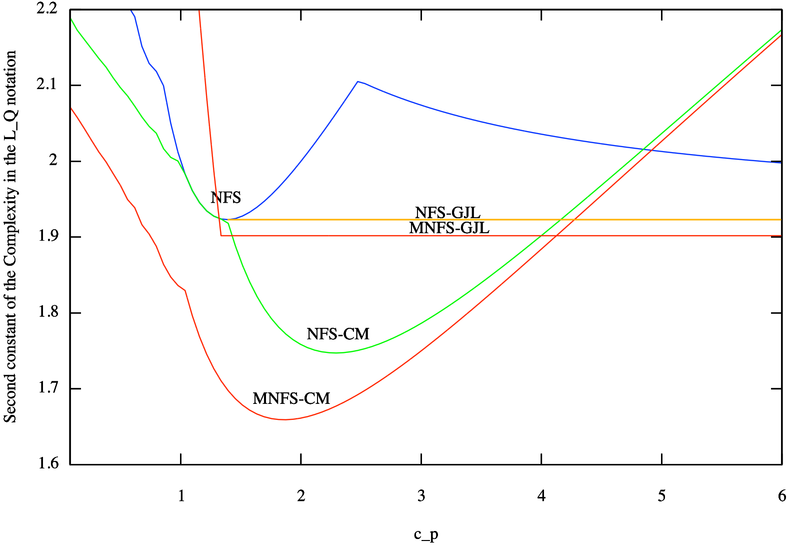
A similar approach permits to combine:

- the Generalized Joux-Lercier Method [BGGM 15]
- with MNFS.

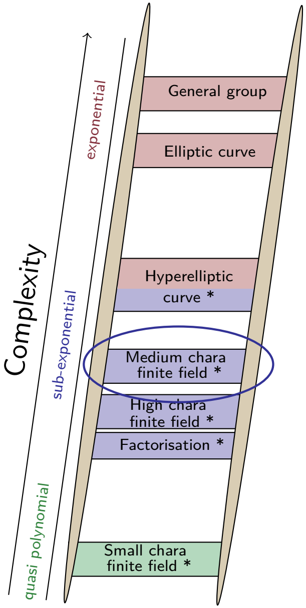


$$p = L_{p^n}(2/3, c_p)$$

Complexities at $p = L_{p^n}(2/3, c_p)$



Thank you for your attention !



Going further

Implementation ?

- For factoring (as a comparison): implemented in 1996 by Elkenbracht-Huizing, but not as efficient as the classical NFS for those parameters.
- For Discrete Logs: tested for small parameters but MNFS in a more realistic context is still to do.

Choice of Polynomials

Previously (NFS) :

- For medium p : f_1 irreducible of degree n over $\mathbb{F}_p$ and $f_2 = f_1 + p$
  Small degrees but high coeffs for f_2
- For high p : based on lattice reduction of $(f_1, Xf_1, \cdots, X^{d-n}f_1, p, Xp, \cdots, X^d p)$
  $\Rightarrow$ f_2 is a multiple of f_1 modulo p but with smaller coeffs
  f_1 with not too small coeffs (otherwise we get trivial multiples)

Some Obstructions Coming from Number Fields and its Solutions

How to go down ?

$$\begin{array}{ccc} \mathbb{Q}[\theta] & & \\ & \searrow & \\ & & \mathbb{F}_{p^n} \end{array}$$

- No unique factorization over elements $\Rightarrow$ we consider ideals in the ring of integers of $\mathbb{Q}[\theta]$.
- Ideals are not principal $\Rightarrow$ we (virtually) raise them to the power of the class number of $\mathbb{Q}[\theta]$.
- Generators are not unique $\Rightarrow$ Schirokauers maps.

Extension of NFS in the boundary case $p = L_{p^n}(1/3)$

- We want to upper-bound the resultant :
  $|\det \mathrm{Sylv}(h, f)| \leqslant \Theta \|f\|^{\deg h} \|h\|^{\deg f}$ with Θ = number of permutations with non zero contributions in the sum.
- Θ ? Let deg $(h) = n$ and deg $(f) = t$.
  Before : $\Theta \leqslant n^t t^n$. Kalkbrener gives : $\Theta \leqslant \binom{n+t}{n} \cdot \binom{n+t-1}{t}$.
  Because of the following inequalities:

$$\begin{aligned}
\binom{n+t}{n} \cdot \binom{n+t-1}{t} &= \frac{n}{n+t} \left(\frac{(n+t)!}{n!t!} \right)^2 \\
&\leq \frac{n}{n+t} \left(\frac{(n+1)\cdots(n+t)}{t!} \right)^2 \\
&\leq \frac{n}{n+t} \left(\prod_{i=1}^{t} \frac{(n+i)}{i} \right)^2 \\
&\leq \frac{n}{n+t} \prod_{i=1}^{t} \left(\frac{n}{i} + 1 \right)^2
\end{aligned}$$

we obtain that $\Theta \leqslant (n+1)^{2t}$.