Discrete Logarithms and Galois Invariant Smoothness Basis (with J.-M. Couveignes)

R. Lercier

DGA/CELAR & University of Rennes — France
Reynald.Lercier (at) m4x.org

CADO workshop on integer factorization

INRIA Nancy Grand-Est — LORIA

October 7-9, 2008

Motivation

- Computing discrete logarithms in $\mathbb{F}_q$, $q = p^d$, with the function field sieve (FFS) relies mostly on the ability of finding relations between elements of a smoothness basis.
- In some very particularly cases (Kummer and Artin-Schreier theories), the factor basis can be constructed in such a way that it is left invariant by automorphisms of $\mathbb{F}_q$.
- In this talk, we are going to explain how this nice property can be generalized to a broad class of finite fields.

J.-M. Couveignes and R. Lercier. Galois invariant smoothness basis. Series on Number Theory and Its Applications, 5:154-179, World Scientific, May 2008

Outline

Outline

Index calculus algorithms

A family of algorithms to solve:

- integer factorization problems,
- discrete logarithm problems in finite fields.

Two important sub-cases:

- Number Field Sieve (factoring and DL in large char.),
- Function Field Sieve (DL in small char.).

Index calculus methods

Step 1

One chooses $V = \{\gamma_1, \ldots, \gamma_{\#V}\} \subset < g >$, the "smoothness basis", and one looks for relations of the type $\prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon} = 1$.

Step 2

As soon as possible, one computes $\log_g \gamma$, solutions of a linear system.

Step 3

To compute $\log_g y$, for any y , one tries random integers ν until $g^{\nu} y = \prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon}$.

How to choose V ? How to find relations ?

Index calculus methods

Step 1

One chooses $V = \{\gamma_1, \ldots, \gamma_{\#V}\} \subset < g >$, the "smoothness basis", and one looks for relations of the type $\prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon} = 1$.

Step 2

As soon as possible, one computes $\log_g \gamma$, solutions of a linear system.

Step 3

To compute $\log_g y$, for any y , one tries random integers ν until $g^{\nu} y = \prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon}$.

How to choose V ? How to find relations ?

Index calculus methods

Step 1

One chooses $V = \{\gamma_1, \ldots, \gamma_{\#V}\} \subset < g >$, the "smoothness basis", and one looks for relations of the type $\prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon} = 1$.

Step 2

As soon as possible, one computes $\log_g \gamma$, solutions of a linear system.

Step 3

To compute $\log_g y$, for any y , one tries random integers ν until $g^{\nu} y = \prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon}$.

How to choose V ? How to find relations ?

Index calculus methods

Step 1

One chooses $V = \{\gamma_1, \ldots, \gamma_{\#V}\} \subset < g >$, the "smoothness basis", and one looks for relations of the type $\prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon} = 1$.

Step 2

As soon as possible, one computes $\log_g \gamma$, solutions of a linear system.

Step 3

To compute $\log_g y$, for any y , one tries random integers ν until $g^{\nu} y = \prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon}$.

How to choose V ? How to find relations ?

Index calculus methods

Step 1

One chooses $V = \{\gamma_1, \ldots, \gamma_{\#V}\} \subset < g >$, the "smoothness basis", and one looks for relations of the type $\prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon} = 1$.

Step 2

As soon as possible, one computes $\log_g \gamma$, solutions of a linear system.

Step 3

To compute $\log_g y$, for any y , one tries random integers ν until $g^{\nu} y = \prod_{(\epsilon,\gamma)\in\mathbb{Z}\times V} \gamma^{\epsilon}$.

How to choose V ? How to find relations ?

A school case

A DL problem in the cyclic subgroup $< 1193 > \subset \mathbb{F}_p$, $p = 10007$.
Let $V = \{2, 3, 5, 7, 11, 13, 17\}$, then

$$1193^{15} \bmod p = 2 \cdot 3 \cdot 7 \cdot 11\,, \quad 1193^{36} \bmod p = 7^2 \cdot 11^2\,,$$
$$1193^{41} \bmod p = 17^3\,, \quad 1193^{47} \bmod p = 2 \cdot 11 \cdot 13 \cdot 17\,,$$
$$1193^{73} \bmod p = 3 \cdot 5 \cdot 11 \cdot 13\,, \quad 1193^{74} \bmod p = 2^5 \cdot 3^2 \cdot 5^2\,,$$
$$1193^{78} \bmod p = 2^6 \cdot 3 \cdot 7^2\,, \quad 1193^{80} \bmod p = 2^3 \cdot 5^2\,.$$

It remains to combine these equations,

$$2 = 1193^{4764}\,,\ 3 = 1193^{236}\,,\ 5 = 1193^{7903}\,,\ 7 = 1193^{638}\,,$$
$$11 = 1193^{4383}\,,\ 13 = 1193^{2560}\,,\ 17 = 1193^{3349}\,.$$

Let now, for instance, $y = 8964$, then

$$(y \cdot 1193^{12}) \bmod p = 2^2 \cdot 3^3 \cdot 5 \cdot 17\,, \text{ and thus } y = 1193^{1464}\,.$$

Known complexity results

Complexity usually expressed as

$$L_q(\lambda, c) = \exp((c + o(1))(\log q)^{\lambda}(\log\log q)^{1-\lambda}) \quad .$$

Two extreme cases:

- $\mathbb{F}_q$, with fixed (small) d. NFS [Gor93, Sch93, JL03] yields

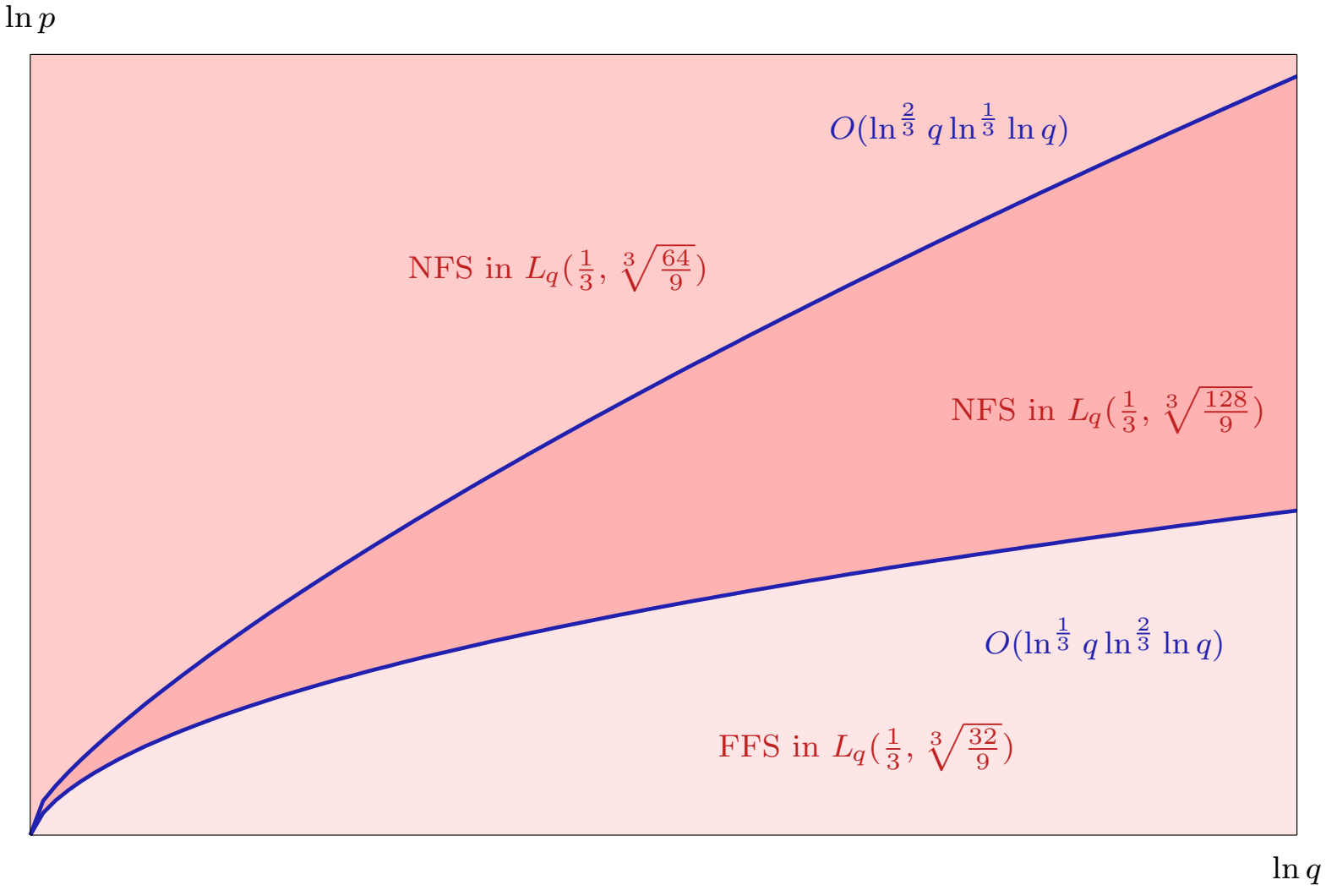
$$L_q(\frac{1}{3}, \left(\frac{64}{9}\right)^{\frac{1}{3}}) \quad .$$

- $\mathbb{F}_q$, with fixed (small) p. FFS [Cop84, Adl94, AH99, JL02] yields

$$L_q(\frac{1}{3}, \left(\frac{32}{9}\right)^{\frac{1}{3}}) \quad .$$

Known complexity results ([JL06, JLSV06])

When d and p both tend to ∞.



Outline

Basic setup

An algorithm, parameterized by a degree D (which increases with d).

Choose two univariate polynomials f_1 and f_2 over $\mathbb{F}_p$

with degrees d_1 and d_2 (as small as possible) such that

- $d_1 \approx D d_2$,
- $\mathrm{Resultant}(\beta - f_1(\alpha), \alpha - f_2(\beta))$ in α or β has an irreducible factor of degree n modulo p,

($d_1 d_2 \geq n$, that is $d_1 \approx \sqrt{Dn}$ and $d_2 \approx \sqrt{n/D}$).

This means that

- there exist $\alpha, \beta \in \mathbb{F}_q$ such that $\beta = f_1(\alpha)$ and $\alpha = f_2(\beta)$.

The sieving

- Take p^{2D+1} polynomials of the form

$$a(\alpha)\beta + b(\alpha)$$

where a and b are polynomials of degree D (a unitary).

- In this expression, replace β by $f_1(\alpha)$ and α by $f_2(\beta)$, this yields equations

$$h_1(\alpha) = h_2(\beta)$$

where h_1 (resp. h_2) has degree $d_1 + D \approx \sqrt{Dn}$ (resp. $d_2 D + 1 \approx \sqrt{Dn}$).

- In good cases, h_1 and h_2 split into irreducible factors of degree at most D.

Example: $\mathbb{F}_{65537^{25}}$

- Take $D = 1$, $f_1(\alpha) = \alpha^5 + \alpha + 3$ and $f_2(\beta) = -\beta^5 - \beta - 1$
- Consider $\beta + 2\alpha - 20496$
  - It can be written as:

$$\alpha^5 + 3\alpha - 20493 =$$
$$(\alpha + 2445) \cdot (\alpha + 9593) \cdot (\alpha + 31166) \cdot (\alpha + 39260) \cdot (\alpha + 48610)$$

  - Or as:

$$-2\beta^5 - \beta - 20498 =$$
$$-2(\beta + 1946) \cdot (\beta + 17129) \cdot (\beta + 18727) \cdot (\beta + 43449) \cdot (\beta + 49823)$$

The end of the computation

- Linear algebra
  - When enough relations collected, inversion of the system yields DLs of irreducible polynomials of degree at most D modulo $(q-1)/(p-1)$.
- Discrete logarithms of any y. Basically
  - Test random ν until a polynomial $g^{\nu} \cdot y$ is $\sqrt{d}$-smooth.
  - For each factor δ, of degree d_δ, test for $(d_\delta - 1)$-smoothness elements $a(\alpha)\beta + b(\alpha)$ chosen such that δ divides $h_1(\alpha)$.

Experiments

Fields	Size (digits)	When	Complexity (GIPS year)	Method	Who
$\mathbb{F}_{2^{401}}$	121	1992	0.2	COPPERSMITH	Gordon, McCurley
$\mathbb{F}_{2^{521}}$	157	2002	0.4	FFS	Joux, Lercier
$\mathbb{F}_{2^{607}}$	183	2002	20	COPPERSMITH	Thomé
$\mathbb{F}_{2^{607}}$ $\mathbb{F}_{2^{613}}$	183	2005	1.6	FFS	Joux, Lercier

Fields	Size (digits)	When	Complexity (GIPS year)	Method	Who
$\mathbb{F}_{370801^{18}}$	101	2005	0.4	TORI	Lercier, Vercauteren
$\mathbb{F}_{65537^{25}}$	121	2005	$\simeq 0$	FFS	Joux, Lercier
$\mathbb{F}_{370801^{30}}$	168	2005	0.1	FFS	Joux, Lercier
$\mathbb{F}_{p^3}$	120	2006	1.2	NFS	Joux, Lercier, Smart,Vercauteren

Outline

First cases

Our concern is to find models for finite fields for which the automorphisms respect the special form of certain elements.

Kummer theory.

- Take $p = 43$ and $d = 6$, so $q = 43^6$, and set $A(X) = X^6 - 3$ which is an irreducible polynomial. So $\mathbb{F}_q$ is seen as $\mathbb{F}_{43}[X]/(X^6 - 3)$.
- Setting $x = X \bmod A(X)$, one has $\phi(x) = x^{43} = (x^6)^7\, x = 3^7\, x$.

Artin-Schreier theory.

- Take $p = 7$ and $d = 7$, so $q = 7^7$ and set $A(X) = X^7 - X - 1$ which is an irreducible polynomial. So $\mathbb{F}_q$ is seen as $\mathbb{F}_7[X]/(A(X))$.
- Setting $x = X \bmod A(X)$, one has $\phi(x) = x + 1$.

General framework

Kummer and Artin-Schreier theories are two special cases of a general situation

- Let $\mathbf{G}$ a commutative algebraic group over $\mathbb{F}_p$ ($\oplus_{\mathbf{G}}$ stands for the addition law and $0_{\mathbf{G}}$ for the unit element).
- Let $T \subset \mathbf{G}(\mathbb{F}_p)$ be a non trivial finite group of $\mathbb{F}_p$-rational points in $\mathbf{G}$.
- Let $I : \mathbf{G} \to \mathbf{H}$ be the quotient isogeny of $\mathbf{G}$ by T, $d \geq 2$ be the degree of I.
- Assume there exists a $\mathbb{F}_p$-rational point a on $\mathbf{H}$ such that $I^{-1}(a)$ is irreducible over $\mathbb{F}_p$.
- Let $b \in \mathbf{G}(\bar{\mathbb{F}}_p)$ such that $I(b) = a$, we set $\mathbb{F}_q = \mathbb{F}_p(b)$.

General framework (end)

The geometric origin of this extension results in a nice description of $\mathbb{F}_p$-automorphisms of $\mathbb{F}_q$.

- Let $t \in T$, the point $t \oplus_{\mathbf{G}} b$ verifies

$$I(t \oplus_{\mathbf{G}} b) = I(t) \oplus_{\mathbf{H}} I(b) = 0_{\mathbf{H}} \oplus_{\mathbf{H}} a = a.$$

- So $t \oplus_{\mathbf{G}} b$ is Galois conjugated to b and all conjugates are obtained that way from all points t in T.
- So we have an isomorphism between T and $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, which associates to every $t \in T$ the residual automorphism

$$b \in I^{-1}(a) \mapsto b \oplus_{\mathbf{G}} t.$$

Assuming the geometric formulae for $P \mapsto P \oplus_{\mathbf{G}} t$ in $\mathbf{G}$ are simple enough, we obtain a nice description of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Kummer Theory case revisited

- $\mathbf{G}$ is the multiplicative group $\mathbf{G}_m$ over $\mathbb{F}_p$, seen as a sub-variety of the affine line $\mathbb{A}^1$ with z-coordinate:
  - The origin $0_{\mathbf{G}}$ has coordinate $z(0_{\mathbf{G}}) = 1$.
  - The group law is given by

$$z(P_1 \oplus_{\mathbf{G}_m} P_2) = z(P_1) \times z(P_2).$$

- The isogeny I is the multiplication by d, $[d] : \mathbf{G}_m \longrightarrow \mathbf{G}_m$:
  - given in terms of the z-coordinates by

$$z(I(P)) = z(P)^d.$$

  - z-coordinates of points in $\operatorname{Ker} I$ are the d-th roots of unity.
- $I^{-1}(P)$ is made of d geometric points having for z-coordinates the d-th roots of $z(P)$.
- Translation $P \mapsto P \oplus_{\mathbf{G}_m} t$ for $t \in \operatorname{Ker} I$, can be expressed as

$$z(P \oplus_{\mathbf{G}_m} t) = z(P) \times \zeta$$

where $\zeta = z(t)$ is a d-th root of unity.

Residue fields of divisors on elliptic curves

We now specialize to the case where **G** is an ordinary elliptic curve E, defined over $\mathbb{F}_p$.

- Assume $E(\mathbb{F}_p)$ contains a cyclic subgroup T of order d.
- Let $I : E \to F$ be the degree d cyclic isogeny with kernel T, the quotient $F(\mathbb{F}_p)/I(E(\mathbb{F}_p))$ is isomorphic to T.
- Take a in $F(\mathbb{F}_p)$ such that a mod $I(E(\mathbb{F}_p))$ generates this quotient.
- The fiber $\mathcal{P} = I^{-1}(a)$ is an irreducible divisor. The d geometric points above a are thus defined on a degree d extension $\mathbb{F}_q$ of $\mathbb{F}_p$ (and permuted by Galois action).

$\mathbb{F}_q$ is the residue extension of E at $\mathcal{P}$.

Residue fields of divisors on elliptic curves

We denote by

- $f \bmod \mathcal{P} \in \mathbb{F}_q$ the residue of a function f on E at $\mathcal{P}$;
- V_k, the set $\{f \bmod \mathcal{P} | \deg f \leq k\}$.

We have

$$V_0 = V_1 = \mathbb{F}_p \subset V_2 \subset \cdots \subset V_d = \mathbb{F}_q$$

and

$$V_k \times V_l \subset V_{k+l}.$$

- V_k is invariant under the action of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ (composition by a translation from T does not affect the degree of a function).
- One can choose a smoothness basis consisting of V_κ for a given κ.
- Factoring an element $z = f \bmod \mathcal{P}$ of $\mathbb{F}_q$ boils down to factoring the divisor of f as a sum of prime divisors of degree $\leq \kappa$.

$\mathbb{F}_{61^{19}}$ example

- $E/\mathbb{F}_{61} : Y^2 = X^3 + 20X + 21$, 76 points over $\mathbb{F}_{61}$.
- Let α be the degree 4 endomorphism defined by

$$\begin{aligned} \alpha : \quad E &\to E, \\ (x : y : 1) &\mapsto \left(\frac{49\,x^4+28\,x^3+55\,x^2+53\,x+27}{(x+25)(x+27)^2} : \right. \\ & \qquad \left. y\,\frac{38\,x^5+37\,x^4+30\,x^3+49\,x^2+9\,x+46}{(x+25)^2(x+27)^3} : 1\right). \end{aligned}$$

- Let β be the degree 3 endomorphism of E given by

$$\begin{aligned} \beta : \quad E &\to E, \\ (x : y : 1) &\mapsto \left(\frac{20\,x^3+36\,x^2+35\,x+40}{(x+7)^2} : y\,\frac{58\,x^3+59\,x^2+12\,x+21}{(x+7)^3} : 1\right). \end{aligned}$$

$\mathbb{F}_{61^{19}}$ example

The endomorphism $I = 1 - \beta\alpha$ has degree 19,

$$\begin{aligned}\operatorname{Ker} I = \{&(0:1:0),(11:\pm 13:1),(14:\pm 19:1),(21:\pm 8:1),(35:\pm 15:1),\\ &(40:\pm 10:1),(41:\pm 10:1),(45:\pm 27:1),(48:\pm 2:1),(51:\pm 23:1)\}.\end{aligned}$$

Note that $c = (57:11:1)$ is of order 38 and generates $E(\mathbb{F}_p)$ modulo the image of I.

$\mathcal{P} = I^{-1}(c)$ is a place of degree 19,

$$\begin{aligned}\mathcal{P} = (&{x_1}^{19}+60\,{x_1}^{18}+25\,{x_1}^{17}+21\,{x_1}^{16}+23\,{x_1}^{15}+22\,{x_1}^{14}+49\,{x_1}^{13}+38\,{x_1}^{12}+30\,{x_1}^{11}+57\,{x_1}^{10}+\\ &3\,{x_1}^{9}+15\,{x_1}^{8}+26\,{x_1}^{7}+17\,{x_1}^{6}+45\,{x_1}^{5}+30\,{x_1}^{4}+48\,{x_1}^{3}+55\,{x_1}^{2}+18\,x_1+35,\\ y_1+&12\,{x_1}^{18}+38\,{x_1}^{17}+5\,{x_1}^{16}+{x_1}^{15}+45\,{x_1}^{14}+42\,{x_1}^{13}+18\,{x_1}^{12}+34\,{x_1}^{11}+39\,{x_1}^{10}+\\ &59\,{x_1}^{9}+16\,{x_1}^{8}+18\,{x_1}^{7}+16\,{x_1}^{6}+36\,{x_1}^{5}+11\,{x_1}^{4}+9\,{x_1}^{3}+48\,{x_1}^{2}+59\,x_1+8),\end{aligned}$$

Galois action of $\mathrm{Gal}(\mathbb{F}_{61^{19}}/\mathbb{F}_{61})$ on any $f(P)$ mod $\mathcal{P}$ is obtained as

$$f(P+t) \bmod \mathcal{P} \text{ for some } t \in \operatorname{Ker} I$$

Sieving phase

- Let $\mathcal{S}$ be a smooth projective reduced, absolutely irreducible surface over $\mathbb{F}_p$. Let $\mathcal{A}$ and $\mathcal{B}$ be two absolutely irreducible curves on $\mathcal{S}$.
- Let $\mathcal{I}$ be an irreducible sub-variety of the intersection $\mathcal{A} \cap \mathcal{B}$. We assume that $\mathcal{A}$ and $\mathcal{B}$ meet transversely at $\mathcal{I}$ and we denote by d the degree of $\mathcal{I}$. The residue field of $\mathcal{I}$ is $\mathbb{F}_p(\mathcal{I}) = \mathbb{F}_q$ with $q = p^d$.
- We need a pencil of effective divisors on $\mathcal{S}$. We denote it by $(D_\lambda)_{\lambda \in \Lambda}$ where Λ is the parameter space.
- We look (at random) for divisors D_λ in the pencil, such that both intersection divisors $D \cap \mathcal{A}$ and $D \cap \mathcal{B}$ are disjoint to $\mathcal{I}$ and κ-smooth for some integer κ (they split as sums of effective $\mathbb{F}_q$-divisors of degree $\leq \kappa$).

Finite residue fields on elliptic squares

In the FFS, $\mathcal{S} = \mathbb{P}^1 \times \mathbb{P}^1$ and $\mathcal{A}$, $\mathcal{B}$ are the lines $\beta - f_1(\alpha)$, $\alpha - f_2(\beta)$.

Now, we are going to consider the product of 2 elliptic curves, $\mathcal{S} = E \times E$ ($E_1 = E_2 = E$).

- Let α and β be two endomorphisms of E and let a, $b \in E(\mathbb{F}_p)$.
- We take $\mathcal{A}$ to be the points (P, Q) s.t. $\alpha(P) - Q = a$.
- We take $\mathcal{B}$ to be the points (P, Q) s.t. $P - \beta(Q) = b$.

Assume $1 - \beta\alpha = \phi - 1$, we choose a and b such that the intersection between $\mathcal{A}$ and $\mathcal{B}$ contains an irreducible component $\mathcal{I}$ of degree d.

Intersection Theory

It remains to find divisors D on $\mathcal{S}$ with intersection degrees, with $\mathcal{A}$ and $\mathcal{B}$, as small as possible.
It depends on the class (d_1, d_2, ξ) in the Néron-Severi group of $\mathcal{S}$, that is

$$\mathbb{Z} \times \mathbb{Z} \times \mathrm{End}(E) \text{ (see Mumphord).}$$

The classes of $\mathcal{A}$ and $\mathcal{B}$ are equal to $(\alpha\bar{\alpha}, 1, \alpha)$ and $(1, \beta\bar{\beta}, \bar{\beta})$.

The intersection degree of D and $\mathcal{A}$ is then

$$D.\mathcal{A} = d_1 + d_2\alpha\bar{\alpha} - \xi\bar{\alpha} - \bar{\xi}\alpha$$

and similarly

$$D.\mathcal{B} = d_1\beta\bar{\beta} + d_2 - \xi\bar{\beta} - \bar{\xi}\beta.$$

In the case where α and β have norms of essentially the square root of the norm of $\phi - 2$, we obtain a similar behavior as the FFS with Galois invariant smoothness bases on both $\mathcal{A}$ and $\mathcal{B}$.

$\mathbb{F}_{61^{19}}$ example (cont.)

Let us come back to $E/\mathbb{F}_{61} : Y^2 = X^3 + 20X + 21$.

- An effective divisor in the class $(1, 0, 0)$ is $c \times E_2$ where c is a place of degree 1 on E_1 and it is not difficult to see that the intersection degrees of such a divisor with $\mathcal{A}$ and $\mathcal{B}$ are 1 and 3.
- Similarly functions ε in the class $(0, 1, 0)$ are derived from divisors $E_1 \times c$. The intersection degrees are now 4 and 1.
- More interesting, the class $(1, 1, 1)$ containing the divisors with equation $P = Q + c$, $(P, Q) \in E_1 \times E_2$, yields intersection degrees 3 and 4.
- Finally, the intersection degrees of functions ε in the class $(2, 2, 1)$ with $\mathcal{A}$ and $\mathcal{B}$ are 8 and 8. Some functions of this class are

$$\varepsilon : y_1\, x_2 + x_1\, y_2 + \lambda(y_1 + y_2) + \mu(x_1 - x_2), \text{ with } \lambda, \mu \in \mathbb{F}_p.$$

$\mathbb{F}_{61^{19}}$ example (cont.)

Class	div ε_1	div ε_2
$(1,0,0)$	$(x_1+43, y_1+33)-(x_1+13, y_1+59)$	$(x_2^2+x_2+52, y_2+10\,x_2+37)+(x_2+12, y_2+35)-(x_2+2, y_2+20)-(x_2^2+26\,x_2+39, y_2+5\,x_2+27)$
$(0,1,0)$	$(x_1^2+4\,x_1+12, y_1+55\,x_1+47)+(x_1^2+45\,x_1+31, y_1+19\,x_1+23)-(x_1+42, y_1+60)-(x_1+36, y_1+15)-(x_1^2+60\,x_1+25, y_1+36\,x_1+26)$	$(x_2+43, y_2+33)-(x_2+13, y_2+59)$
$(2,2,1)$	$(x_1+10, y_1+23)+(x_1+20, y_1+x_1+30)+(x_1+29, y_1+1)+(x_1+41, y_1+x_1+33)+(x_1^2+6\,x_1+17, y_1+25\,x_1+16)+(x_1^2+25\,x_1+12, y_1+25\,x_1+47)-(x_1+1, y_1)-(x_1+54, y_1+4)-(x_1^2+17\,x_1+19, y_1+41\,x_1+21)-(x_1^2+51\,x_1+53, y_1+44\,x_1+31)-(x_1^2+55\,x_1+38, y_1+38\,x_1+58)$	$(x_2+29, y_2+60)+(x_2+36, y_2+15)+(x_2^2+15\,x_2+58, y_2+41\,x_2+39)+(x_2^2+23\,x_2+2, y_2+33\,x_2+7)+(x_2^2+44\,x_2+33, y_2+35\,x_2+28)-(x_2+1, y_2)-(x_2+11, y_2+42)-(x_2+16, y_2+34)-(x_2+50, y_2+13)-(x_2^2+26\,x_2+12, y_2+49\,x_2+29)-(x_2^2+47\,x_2+5, y_2+7\,x+14)$

$\mathbb{F}_{61^{19}}$ example (end.)

With our smoothness choice, the factor basis is derived from places of degree one and two:

- but we can divide by 19 the size of the factor basis (at the expense in the linear algebra phase of entries equal to sums of powers of p).
- and we finally have 4 meaningful places of degree 1 and 94 meaningful places of degree 2 on each side, that is a total of 196 entries in our factor basis.

We were able to find, as expected, 195 independant relations in the sieving phase and we succesfully performed the linear algebra modulo the largest factor of $61^{19} - 1$, that is a 99-bit integer.

In such a field, the FFS would handle a factor basis of irreducible polynomials of degree 2 over $\mathbb{F}_{61}$, in two variables, that is about 3600 elements.

Outline

Conclusion

Galois invariant smoothness basis for FFS can be easily find for $\mathbb{F}_{p^d}$ when,

- d divides $p-1$ (Kummer case),
- $d = p$ (Artin Schreier case).

This may be extended to

- d divides $p+1$ (Algebraic Tori of dimension 1),
- d divides D s.t.

$$p+1-2\sqrt{p} < D < p+1+2\sqrt{p} \quad \text{(Elliptic Curves)}.$$

Bibliography I

L. Adleman and J. DeMarrais.

A subexponential algorithm for discrete logarithms over all finite fields.
volume 773 of *Lecture Notes in Computer Science*, pages 147–158. Springer, 1993.

L. M. Adleman.

The function field sieve.
In *Algorithmic Number Theory, Proceedings of the ANTS-I conference*, 1994.

L. M. Adleman and M. A. Huang.

Function field sieve method for discrete logarithms over finite fields.
In *Information and Computation*, volume 151, pages 5–16. Academic Press, 1999.

D. Coppersmith.

Fast evaluation of logarithms in fields of characteristic two.
IEEE Trans. Inform. Theory, 30(4):587–594, 1984.

D. Gordon.

Discrete logarithms in $GF(p)$ using the number field sieve.
SIAM J. Discrete Math, 6:124–138, 1993.

R. Granger and F. Vercauteren.

On the discrete logarithm problem on algebraic tori.
In *Advances in Cryptology – Crypto 2005*.

A. Joux and R. Lercier.

The function field sieve is quite special.
In *Algorithmic Number Theory, Proceedings of the ANTS-V conference*, 2002.

Bibliography II

A. Joux and R. Lercier.

Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the gaussian integer method.
Math. Comp., 72:953–967, 2003.

A. Joux and R. Lercier.

The Function Field Sieve in the Medium Prime case.
Eurocrypt 2006.

A. Joux, R. Lercier, N. Smart, and F. Vercauteren.

The Number Field Sieve in the Medium Prime case.
Crypto 2006.

M. Kraitchik.

Théorie des nombres, volume 1.
Gauthier-Villars, 1922.

O. Schirokauer.

Discrete logarithms and local units.
Phil. Trans. R. Soc. Lond. A 345, pages 409–423, 1993.

O. Schirokauer.

The Special Function Field Sieve.
SIAM J. Discrete Math. 16(1) pages 81-98, 2002.