Elliptic Periods for Finite Fields
&
Applications to the AKS primality test

(with J.-M. Couveignes, T. Ezome)

R. Lercier

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

AGCT-12

April 2009

Motivation

Given a finite field $\mathbb{F}_q$, and an integer d, how can we construct $\mathbb{F}_{q^d}$ s.t. the addition, the multiplication and computing q^{th} power is fast,

at most $\tilde{O}(d \log q)$elementary operations

Alternatively, is this possible for degree d extensions of $\mathbb{Z}/N\mathbb{Z}$, N not necessarily a prime ?

A first remark: Since $\mathbb{F}_{q^d}$ is a $\mathbb{F}_q$-vector space of dim. d,

- it is "natural" to represent elements as vectors over $\mathbb{F}_q$,
$$\vec{\alpha} = (\alpha_i)_{i \in \mathbb{Z}/d\mathbb{Z}},$$
- and addition is obviously fast.

But how about about multiplications and Frobenius maps ?

The textbook answer: Power Basis

$P(X)$, an irreducible polynomial of degree d over $\mathbb{F}_q$,
x, a root of $P(X)$, then $\vec{\alpha}$ is defined in the basis $(1, x, \ldots, x^{d-1})$.

- Multiplication is OK, it is

$$\left(\sum_{i=0}^{d-1} \alpha_i X^i\right) \cdot \left(\sum_{i=0}^{d-1} \beta_i X^i\right) \bmod P(X),$$

  and there exists fast (FFT-like) algorithms for it.

- But nothing better than exponentiation algorithms for the Frobenius, this yields a (too large)

$$\tilde{O}(d \log^2 q) \text{ complexity.}$$

Normal Basis

Basis of the form $(x, x^q, \ldots, x^{q^{d-1}})$.

- Frobenius is now obvious : a cyclic shift of the coordinates.
- But Multiplication is most of the time cumbersome !

More precisely, let $(\gamma_i) = \vec{\alpha} \,.\, \vec{\beta}$,

- each γ_i is a bilinear form in $\vec{\alpha}$ and $\vec{\beta}$, these forms are cyclic shifts of each other,
- their number of terms is called the complexity $\mathcal{C}$ of the normal basis.

This complexity $\mathcal{C}$ is at least $2d - 1$ [Mullin at al. 1989].

Gauss periods

Unless the degree d takes very special (and sparse) values, normal basis with bounded $\mathcal{C}$ are not known to exist.

A construction due to [Gao-Lenstra 1992] needs

- r-th roots of unity where $r = kd + 1$ is prime,
- q generates the unique quotient of order d of $(\mathbb{Z}/r\mathbb{Z})^*$.

Then $\mathcal{C}$ is bounded by $(d-1)k + d$

[Gao, von zur Gathen, Panario, 2000] show that fast FFT multiplication method can be adapted to this case, with complexity $\tilde{O}(kd \log q)$.

But in general $k \geqslant O(d^3 \log^2(dq))$ [Adleman-Lenstra 1986], this is too large.

Our Result

We make use of torsion points on elliptic curves instead of roots of unity.

Theorem

To every couple (q, d) with q a prime power and $d \geqslant 2$ an integer s.t. $d_q \leqslant \sqrt{q}$, one can associate a normal basis $\Theta(q, d)$ of the degree d extension of $\mathbb{F}_q$ such that the following holds:

- *There exists an algorithm that multiplies two elements given in $\Theta(q, d)$ at the expense of $\tilde{O}(d \log q)$ elementary operations.*

This can be easily extend to a result without any restriction on q and d.

Remark: Here d_q is such that

- $v_\ell(d_q) = v_\ell(d)$ if ℓ is prime to $q-1$, $v_\ell(d_q) = 0$ if $v_\ell(d) = 0$,
- $v_\ell(d_q) = \max(2v_\ell(q-1)+1, 2v_\ell(d))$ if ℓ divides both $q-1$ and d.

Some notations

- Let $E/\mathbb{F}_q$ be an elliptic curve given by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\,.$$

- If A is a point in $E(\mathbb{F}_q)$, we denote by $\tau_A : E \longrightarrow E$ the translation by A. We set $x_A = x \circ \tau_{-A}$ and $y_A = y \circ \tau_{-A}$.
- If A, B and C are three pairwise distinct points in $E(\mathbb{F}_q)$, we define

$$\Gamma(A, B, C) = \frac{y(C - A) - y(A - B)}{x(C - A) - x(A - B)}\,.$$

- We define a function $u_{A,B} \in \mathbb{F}_q(E)$ by $u_{A,B}(C) = \Gamma(A, B, C)$.

It has degree two with two simple poles, at A and B.

Ingedient 1: Some simple elliptic functions

We can prove the following identities (with Taylor expansions at poles).

$$\begin{aligned}
\Gamma(A,B,C) &= \Gamma(B,C,A) = -\Gamma(B,A,C) - a_1 \\
&= -\Gamma(-A,-B,-C) - a_1\,, \\
u_{A,B} + u_{B,C} + u_{C,A} &= \Gamma(A,B,C) - a_1\,,
\end{aligned}$$

$$\begin{aligned}
u_{A,B}u_{A,C} &= x_A + \Gamma(A,B,C)u_{A,C} + \Gamma(A,C,B)u_{A,B} \\
&\quad + a_2 + x_A(B) + x_A(C)\,, \\
u_{A,B}^2 &= x_A + x_B - a_1 u_{A,B} + x_A(B) + a_2\,.
\end{aligned}$$

Ingredient 2: Residue fields of divisors on elliptic curves

Let E be an elliptic curve defined over $\mathbb{F}_q$.

- Assume $E(\mathbb{F}_q)$ contains a cyclic subgroup $\mathcal{T}$ of order d.
- Let $I : E \to E'$ be the degree d cyclic isogeny with kernel $\mathcal{T}$, the quotient $E'(\mathbb{F}_q)/I(E(\mathbb{F}_q))$ is isomorphic to $\mathcal{T}$.
- Take A in $E'(\mathbb{F}_q)$ such that A mod $I(E(\mathbb{F}_q))$ generates this quotient.
- The fibre $\mathcal{P} = I^{-1}(A) = \sum_{T \in \mathcal{T}} [B + T]$ is an irreducible divisor.

  The d geometric points above A are defined on a degree d extension $\mathbb{F}_{q^d}$ of $\mathbb{F}_q$ (and permuted by Galois action).

$\mathbb{F}_{q^d}$ is the residue extension of $\mathbb{F}_q(E)$ at $\mathcal{P}$.

Elliptic Normal Basis

For $k \in \mathbb{Z}/d\mathbb{Z}$, we set

$$u_k = \mathfrak{a} u_{kT,(k+1)T} + \mathfrak{b}.$$

($\mathfrak{a}$ and $\mathfrak{b}$, constants chosen such that $\sum u_k = 1$).

Lemma (A normal basis)

The system $\Theta = (u_k(B))_{k \in \mathbb{Z}/d\mathbb{Z}}$ is a $\mathbb{F}_q$ normal basis of $\mathbb{F}_{q^d}$.

Proof

Let λ_k in $\mathbb{F}_q$ such that $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_k(B) = 0$.

Let us consider the function $f = \sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_k$.

- It cancels not only at B, but at $B+T$ with $T \in \mathcal{T}$ (because f is defined over $\mathbb{F}_q$).
- And f has d poles, the points in $\mathcal{T}$.
- Let us assume $f \neq 0$, then $(f) = (f)_0 - (f)_\infty$ with
$$(f)_0 = \sum_{T\in\mathcal{T}} [B+T] \text{ and } (f)_\infty = \sum_{T\in\mathcal{T}} [T].$$
- So, $\sum_{T\in\mathcal{T}} (B+T) - (T) = d\,B = 0_E$. This is impossible, $\Rightarrow f = 0$.
- Taylor expansions at poles show that all λ_k's are equal.
- Since $\sum u_k = 1$, all λ_k's are thus null.

Prerequisities

There exists an algorithm with quasi-linear complexity to multiply two elements given in an elliptic normal basis.

It consists in evaluations and interpolations at d points $R + kT$, where

$$R \in E(\mathbb{F}_q) - E[d]\,.$$

Notations.

- $\vec{\alpha} \star_j \vec{\beta} = \sum_i \alpha_i \beta_{j-i}$, the j^{th} coord. of the convolution product $\vec{\alpha} \star \vec{\beta}$.
- $\sigma(\vec{\alpha}) = (\alpha_{i-1})_i$, the cyclic shift of $\vec{\alpha}$.
- $\vec{\alpha} \diamond \vec{\beta} = (\alpha_i \beta_i)_i$, the component-wise product.

A fast multiplication algorithm

$$\begin{aligned}\overrightarrow{\iota} &= (\iota_i)_{0\leqslant i\leqslant d-1} \text{ s.t. } x(B) = \textstyle\sum_{0\leqslant k\leqslant d-1} \iota_k\theta_k.\\ \vec{x}_R &= (x(R+kT))_{0\leqslant k\leqslant d-1}.\\ \vec{u}_R &= (u_0(R+kT))_{0\leqslant k\leqslant d-1}.\end{aligned}$$

Lemma

The multiplication tensor for normal elliptic basis of type Θ is

$$(\mathfrak{a}^2\overrightarrow{\iota}) \star \Big((\vec{\alpha}-\sigma(\vec{\alpha}))\diamond(\vec{\beta}-\sigma(\vec{\beta}))\Big) +$$
$$\overrightarrow{u_R}^{(-1)} \star \Big((\vec{u}_R\star\vec{\alpha})\diamond(\vec{u}_R\star\vec{\beta}) - (\mathfrak{a}^2\vec{x}_R)\star\Big((\vec{\alpha}-\sigma(\vec{\alpha}))\diamond(\vec{\beta}-\sigma(\vec{\beta}))\Big)\Big)$$

But how to obtain $\overrightarrow{\iota}$?

To compute $\overrightarrow{\iota}$, *i.e.* $x(B)$ in the basis Θ, we make use of the field trace as a non-degenerate quadratic form.

For f a function on E, we denote

$$\mathrm{Tr}(f) = \sum_{k \in \mathbb{Z}/d\mathbb{Z}} f \circ \tau_{kT}$$

(it can be seen as a function on E').

Our goal is to compute $\mathrm{Tr}(u_k u_l)$ and $\mathrm{Tr}(u_k x)$ as linear combinations of 1, x' and y' where $(x', y') = I(x, y)$.

Then $\overrightarrow{\iota} = \overrightarrow{e}^{(-1)} \star \overrightarrow{\hat{\iota}}$ where $\vec{e} = Tr(u_k u_l)(A)$ and $\overrightarrow{\hat{\iota}} = \mathrm{Tr}(u_k x)(A)$.

Other relations among functions

Let $x_k = x_{kT}$, $y_k = y_{kT}$.

Following Vélu, we have ($d \geqslant 3$, odd),

$$x' = x + \sum_{1 \leqslant k \leqslant d-1} [x_k - x(kT)] \text{ and } y' = y + \sum_{1 \leqslant k \leqslant d-1} [y_k - y(kT)] .$$

Further, we can prove

$$\begin{aligned} x_C u_{A,B} &= \Gamma(A,B,C)x_C + x_B(C)u_{C,B} - x_A(C)u_{C,A} + y_A(C) - y_B(C) , \\ x_A u_{A,B} &= y_A + x_B(A)u_{A,B} - y_B(A) , \\ x_B u_{A,B} &= -y_B - a_1 x_B - a_3 + x_B(A)u_{A,B} - y_B(A) . \end{aligned}$$

Trace computations

One may compute $\mathfrak{c}_k = \mathrm{Tr}(u_{O,kT})$ from

$$\begin{aligned}\mathrm{Tr}(u_{O,T}) &= \sum_{1\leqslant l\leqslant d-2} \Gamma(0, lT, (l+1)T) - a_1\,,\\ \mathrm{Tr}(u_{O,(k+l)T}) &= \mathrm{Tr}(u_{O,kT}) + \mathrm{Tr}(u_{O,lT}) - d\Gamma(0, kT, (k+l)T)\,.\end{aligned}$$

(k, l and $k+l$ are non-zero in $\mathbb{Z}/d\mathbb{Z}$)

Formulas for $\mathrm{Tr}(u_k u_l)$ and $\mathrm{Tr}(u_k x)$ follows,

$$\mathrm{Tr}(u_{0,T}^2) = 2x' + d(x(T) + a_2) - a_1\mathfrak{c}_1 + 2\sum_{1\leqslant l\leqslant d-1} x(lT)\,,$$

$$\mathrm{Tr}(xu_{0,T}) = y' + x(T)\mathfrak{c}_1 + d(y(T) + a_1 x(T) + a_3) + \sum_{1\leqslant l\leqslant d-1} y(lT)\,,$$

etc.

AKS primality test

Theorem

N is prime if and only if $(X+1)^N = X^N + 1 \bmod N$ in $\mathbb{Z}[X]$

Elegant. . . but it involves storing N coefficients !

AKS algorithm (mainly) performs this test

- modulo $X^r - 1$ for r s.t. $o_r(N) > \log^2 N$,
- not only for $X+1$, but for

$$X + a, \ a = 1, \ldots, \lfloor \sqrt{\varphi(r)} \log N \rfloor$$

.

That is,

$$(X+a)^N \equiv X^N + a \bmod (N, X^r - 1).$$

AKS improvements (in a nutshell)

We have $r \leqslant \max\{3, \lceil \log^5 N \rceil\}$,

this yields a $\tilde{O}(\log^{21/2} N)$ complexity [see AKS paper].

Roughly, we might distinguish two lines of improvements.

- Lenstra-Pomerance: Replace $X^r - 1$ by "irreducible polynomials" of degree $\simeq \log^2 N$

$$\longrightarrow \tilde{O}(\log^6 N) \text{ complexity.}$$

- Berritzbeitia-Cheng: Make use of "degree friendly" $\mathbb{Z}/N\mathbb{Z}$ automorphism, $X^N \mapsto \zeta X$, when $r \mid N - 1$ to restrict AKS to the *only* test $(X+1)^N \equiv X^N + 1$.

$$\longrightarrow \tilde{O}(\log^4 N) \text{ complexity} \quad (\text{if } \exists r \simeq \log^2 N \text{ s.t. } r | N - 1)\,.$$

The later was improved by [Avanzi-Mihailescu] and (indep.) [Bernstein] to the case $r | N^k - 1$ for some k.

Our approach

Using normal elliptic basis extensions, we can take advantage of both situations.

- We can find an elliptic curve E over $\mathbb{Z}/N\mathbb{Z}$ with a $r \simeq \log^2 N$ torsion part and construct from it a degree r elliptic extension of $\mathbb{Z}/N\mathbb{Z}$.

  $\longrightarrow$ Lentra-Pomerance arguments should transpose to this case.

- Elliptic extensions come, by construction, with a "degree friendly" $\mathbb{Z}/N\mathbb{Z}$ automorphism, $B \mapsto B + T$ on E.

  $\longrightarrow$ Berritzbeitia-Cheng arguments should transpose too.

This yields a $\tilde{O}(\log^4 N)$ primality test, but no more deterministic (we have to find a curve E).

Work in progress...