Elliptic Periods & Applications

R. Lercier

DGA & University of Rennes — France

email : reynald.lercier(at)m4x.org
www : http://perso.univ-rennes1.fr/reynald.lercier/

ECC 2011 — 15-th Workshop on Elliptic Curve Cryptography

Nancy, September 2011

Motivation

- Let R be a (commutative and unitary) ring, the algebra $S = R[x]/(x^d - \alpha)$ has shown to be (algorithmically) very useful:
  - Low complexity normal basis [GL92];
  - Primality proving [AKS04];
  - Discrete Logarithm computations in Finite Fields [JL06];
  - Fast polynomial factorization and composition [KU08].
- But, often, there is no primitive d-th root of unity in R (and embedding the ring R into an auxiliary extension R' yields important losses of efficiency).
- Idea: substitute to S one elliptic curve E defined on R, having a point $T \in E(R)$ of exact order d.

Joint works with J.-M. Couveignes, C. Dunand, T. Ezome.

Outline

Outline

Classical Method

A classical approach:

- Choosing a random polynomial of degree d.
- Testing for its irreducibility.

Complexity:

- The probability that a polynomial of degree d be irreducible is at least $1/(2d)$ [LN83, Ex. 3.26 and 3.27, page 142]
- Ben-Or's irreducibility test [BO81], this test has average complexity $(\log q)^{1+o(1)} \times d^{1+o(1)}$ elementary operations

A total of $(\log q)^{2+o(1)} \times d^{2+o(1)}$ elementary operations.

Another approach [CL09b]

Difficult to improve things as long as we use an irreducibility test.
We are thus driven to consider very particular polynomials.

Adleman and Lenstra [AL86] construct such irreducible polynomials (thanks to Gauss periods),

- with (now) complexity quasi-linear in d,
- but only when $d = \ell^\delta$ with ℓ a prime divisor of $p(q-1)$.

We mimic their construction using isogenies between elliptic curves,

- with still complexity quasi-linear in d,
- but $d = \ell^\delta$ is coprime to $p\,(q-1)$.

A total complexity of $d^{1+o(1)} \times (\log q)^{5+o(1)}$.

Artin-Schreier towers : $d = p^\delta$ [LdS08]

For every $k \in \mathbb{N}^*$, le $\mathcal{A}_k \subset \overline{\mathbb{F}}_p$ be the subset of a's in $\overline{\mathbb{F}}_p$ s.t.

1. a generates $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$, *i.e.* $\mathbb{F}_p(a) = \mathbb{F}_{p^k}$,
2. a has non-zero absolute trace, *i.e.* $\mathrm{Tr}\, a \neq 0$,
3. a^{-1} has non-zero absolute trace, *i.e.* $\mathrm{Tr}\, a^{-1} \neq 0$.

Especially, $\mathcal{A}_1 = \mathbb{F}_p^*$.

Let now I be the map

$$I : \begin{array}{rcl} \overline{\mathbb{F}}_p \setminus \mathbb{F}_p & \to & \overline{\mathbb{F}}_p \setminus \{0\} \\ X & \mapsto & (X^p - 1)/(X + X^2 + \cdots + X^{p-1}) \end{array}$$

We check that

- $I^{-1}(\mathcal{A}_k) \subset \mathcal{A}_{pk}$,
- $I^{-\delta}(1)$ is a degree p^δ irreducible divisor over $\mathbb{F}_p$.

Examples

If $p = 2$, $d = 2$:

- Compute $I(x) = \dfrac{x^2 + 1}{x}$;
- $f(x) = x^2 + 1 - x$.

If $p = 2$, $d = 4$:

- Compute $(I \circ I)(x) = \dfrac{x^4 + x^2 + 1}{x^3 + x}$;
- $f(x) = x^4 + x^2 + 1 - (x^3 + x)$.

Both are irreducible polynomials in $\mathbb{F}_2[x]$.

Radicial extensions : $d = \ell^\delta$ with $\ell | p - 1$

If $\ell = 2$, we ask that $4 | p - 1$.

First, look for a generator a of the ℓ-Sylow subgroup of $\mathbb{F}_p^*$.

- Pick random α in $\mathbb{F}_p^*$ until $a = \alpha^{(p-1)/\ell^e} \neq 1$.
- The probability of success is about 1.

Then the polynomial $f(x) = x^d - a$ is irreducible in $\mathbb{F}_p[x]$.

Proof.

- The $\ell^{\delta+e}$-torsion $\mathbf{G}_m[\ell^{\delta+e}]$ of $\mathbf{G}_m$ is isomorphic to $(\mathbb{Z}/\ell^{\delta+e}\mathbb{Z}, +)$
- The Frobenius $\varphi_q : \mathbf{G}_m \to \mathbf{G}_m$ acts on it as mult. by q.
- The order of $q = 1 + \ell'\ell^e$ in $(\mathbb{Z}/\ell^{e+\delta}\mathbb{Z})^*$ is $\ell^\delta = d$.
- So the Frobenius Φ_q acts transitively on the roots of $f(x)$.

□

Example

We take $p = 5$, $\ell = 2$, $\delta = 3$ and $d = 8$.

- We check that 4 divides $p - 1$.
- In particular $e = 2$ and $\ell' = 1$.
- The class $a = 2 \bmod 5$ generates the 2-Sylow subgroup of $(\mathbb{Z}/5\mathbb{Z})^*$.

  ($2^4 = 1 \bmod 5$ and $2^2 = -1 \bmod 5$).
- We set $f(x) = x^8 - 2$.

Residue fields of divisors on elliptic curves

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

- Assume $E(\mathbb{F}_p)$ contains a cyclic subgroup $\mathcal{T}$ of order d.
- Let $I : E \to E'$ be the degree d cyclic isogeny with kernel $\mathcal{T}$
- Take a in $E'(\mathbb{F}_p)$ of order d.
- Consider the fibre $I^{-1}(a) = \sum_{T \in \mathcal{T}}[b + t]$.

$$\begin{array}{lcccl}
I^{-1}(a) = \sum_{T \in \mathcal{T}}[b + t] \subset & E(\mathbb{F}_{p^d}) & & & \\
 & \Big| \, d & \searrow^{I} & & \\
\mathcal{T} = \langle t \rangle \subset & E(\mathbb{F}_p) & \xrightarrow{I} & E'(\mathbb{F}_p) \ni a &
\end{array}$$

Irreducibility conditions

We factor $p+1-t = dd'$ where d' is coprime to d.

There exists two integers λ and μ such that

$$\begin{array}{rcl} X^2 - tX + q & = & (X-\lambda)(X-\mu) \bmod d^2\,, \\ \lambda = 1 \bmod d, & & \mu = q \bmod d\,. \end{array}$$

Remember $I(b) = a$, then b is a d^2-torsion point, and

$$\varphi(b) = \lambda b \text{ (where } \varphi \text{ is the Frobenius map)}\,.$$

- The order of $\lambda = 1 + d\lambda' \bmod d^2$ is equal to d.
- Thus the Galois orbit of b has cardinality d
- And the d geometric points $b+t$ above a are defined on a degree d extension $\mathbb{F}_{q^d}$ of $\mathbb{F}_p$ (and permuted by Galois action).

$\mathbb{F}_{q^d}$ is the residue extension of $\mathbb{F}_p(E)$ at $\mathcal{P} = \sum_{T\in\mathcal{T}}[b+T]$.

Example

We take $p = 7$, $q = 7$ and $d = 5$.

The elliptic curve $E/\mathbb{F}_7 \; : y^2 = x^3 + x + 4$ has got 10 $\mathbb{F}_7$-rational points.

The point $t = (6, 4)$ has order $\ell = 5$ and

$$\langle t \rangle = \{O_E,\ (6,4),\ (4,4),\ (4,3),\ (6,3)\}\ .$$

The quotient by $\langle t \rangle$ isogenous curve E', given by Vélu's formulae, is

$$E' \; : y'^2 = x'^3 + 3\,x' + 4.$$

where, x' in terms of x alone,

$$x' = x + \frac{x+2}{(x+1)^2} + \frac{1}{(x+3)^2} = \frac{x^5 + x^4 + 2\,x^3 + 5\,x^2 + 4\,x + 5}{(x+3)^2\,(x+1)^2}\ .$$

We choose $a = (1, 1)$ in $E'(\mathbb{F}_7)$ and finally obtain,

$$\begin{aligned} f_a(x) &= x^5 + x^4 + 2\,x^3 + 5\,x^2 + 4\,x + 5 - 1\ \ (x+3)^2\,(x+1)^2 \\ &= x^5 + x^3 + 4\,x^2 + x + 3\,. \end{aligned}$$

Irreducible polynomials of degree $d = \ell^\delta$

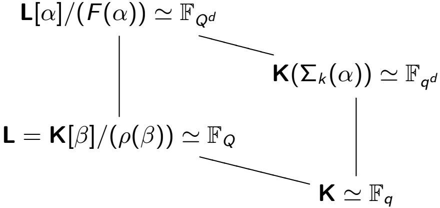
Algorithm for $4\ell \leqslant q^{\frac{1}{4}}$ and any δ :

- Pick a random elliptic curve E over $\mathbf{K}$ and compute its cardinality using Schoof's algorithm ($(\log q)^{5+o(1)}$ elem. ops).
- Repeat until the cardinality of E is divisible by ℓ (by a result of Howe, the average number of trials is $O(\ell)$).
- Compute a chain of δ quotient isogenies of degree ℓ from E with Vélu's formulas ($d^{1+o(1)} \times \ell^{1+o(1)} \times (\log q)^{2+o(1)}$ elem. ops).
- Compose these isogenies with Kedlaya-Umans' algorithm ($d^{1+o(1)} \times (\log q)^{1+o(1)}$ elem. ops).

A total of $\ell \times (\log q)^{5+o(1)} + d^{1+o(1)} \times (\log q)^{2+o(1)}$ elem. ops.

Base change

Now, assume $4\ell > q^{\frac{1}{4}}$, we have to base change to aux. extensions.



1. Find a degree $r \simeq (\log \ell)$ irreducible polynomial $\rho(\beta) \in \mathbf{K}[\beta]$ (negligible cost);
2. Obtain an irreducible polynomial $F(x)$ of degree d in $\tilde{\mathbf{L}}[x]$, in time $(\log q)^{5+o(1)} d^{1+o(1)}$ elem. ops;
3. There exists a symmetric function Σ_k such that the polynomial

$$f(x) = \prod_{0 \leqslant l < d} (x - \Phi_q^l(\Sigma_k(\alpha))) \in \mathbf{K}[x] \text{ is irreducible of degree } d.$$

Some technicalities

Three questions to be considered.

1. How to compute $\Sigma_k(\alpha)$ and its conjugates ?
   - $\alpha = x(b)$ where b is a geometric point of order $\ell^{e+\delta}$ in $E(\mathbf{L})$, so

     $$\exists\lambda \text{ s.t. } \varphi_E(b) = \lambda b \qquad (\varphi_E \text{ is the degree } Q \text{ Frobenius of } E/\mathbf{L})$$

2. How to find the good integer k ?
   - Compute the conjugates of α and form the pol. with these roots.
   - $\Sigma_k(\alpha)$ generates the degree d extension of $\mathbf{K}$ iff $\Phi_q^{\ell^{\delta-1}}(\Sigma_k(\alpha)) \neq \Sigma_k(\alpha)$, that is $\Sigma_k(\Phi_q^{\ell^{\delta-1}}(\alpha)) \neq \Sigma_k(\alpha)$.

3. How to compute $f(x) \in \mathbf{K}[x]$?
   - Compute the minimal pol.of $\Sigma_k(\alpha)$, with Kedlaya-Umans algorithm.

A total of $d^{1+o(1)} \times (\log q)^{2+o(1)}$ elem. ops

Compositum

The last problem to be considered is the following.

> *Given 2 irreducible polynomials $f_1(x)$ and $f_2(x)$ with coprime degrees d_1 and d_2, construct a deg. $d_1 d_2$ irreducible polynomial.*

This is a classical result.

- Let α_1 be a root of $f_1(x)$ and α_2 be a root of $f_2(x)$, then $\alpha_1 + \alpha_2$ generates an extension of degree $d_1 d_2$ of $\mathbb{F}_q$.
- The minimal polynomial of $\alpha_1 + \alpha_2$, called *composed sum* in a work of Bostan, Flajolet, Salvy and Schost, can be computed in quasi-linear time complexity in $d_1 d_2$.

A total of $(d_1 d_2)^{1+o(1)} \times (\log q)^{1+o(1)}$ elem. ops.

(Special) Irreducible polynomials over finite fields

Theorem

There exists an algorithm that on input a finite field $\mathbb{F}_q$, and a positive integer d, returns a degree d irreducible polynomial in $\mathbb{F}_q[X]$. The algorithm requires $d^{1+o(1)} \times (\log q)^{5+o(1)}$ elementary operations.

Remarks.

- We consider very particular polynomials (derived from points on elliptic curves).
- Some special cases $\ell = 2, 3$ have to be handled in specific ways.

(Random) Irreducible polynomials over finite fields

Given a *special* irreducible polynomial $f(x)$ of degree d, one can compute a *random* irreducible polynomial $g(x)$ of degree d with only $d^{1+o(1)} \times (\log q)^{1+o(1)}$ elementary operations.

- Choose a random element a in $\mathbf{L} = \mathbf{K}[x]/(f(x))$ (generates $\mathbf{L}$ with probability greater than $1 - \frac{q}{q-1}(q^{-\frac{d}{2}} - q^{-d}) > 1/2$);
- Compute the minimal polynomial of the element a (at the expense of $d^{1+o(1)}(\log q)^{1+o(1)}$ with Kedlaya-Umans' algorithm);

Outline

Normal basis

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 q^{th} power are fast operations,

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

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 ?

Ingredient 1: Residue fields of divisors on elliptic curves (again)

$$I^{-1}(a) = \sum_{T \in \mathcal{T}} [b + t] \subset \quad E(\mathbb{F}_{p^d})$$

$$E(\mathbb{F}_{p^d}) \xrightarrow{\;I\;} E'(\mathbb{F}_p), \qquad E(\mathbb{F}_{p^d}) \overset{d}{\text{—}} E(\mathbb{F}_p)$$

$$\mathcal{T} = \langle t \rangle \subset \quad E(\mathbb{F}_p) \xrightarrow{\;I\;} E'(\mathbb{F}_p) \ni a$$

Again, under some mild condition, $\phi(b) - b$ is a generator of $\mathcal{T}$ and 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 $\mathcal{P}$.

Ingredient 2 : simple functions

- 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, 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.

Elliptic Normal Basis

Coming back to the functions u_{AB}, we choose for A and B "consecutive points" in $\mathcal{T}$.

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

$$u_k = \mathfrak{a} u_{kt,(k+1)t} + \mathfrak{b}$$

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

and we evaluate the u_k's at b.

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 $\mathbb{F}_{q^d}$.

Θ is a basis

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.

Θ is normal

We have

$$\begin{aligned} \phi(u_k(b)) &= u_k(\phi(b)), \\ &= u_k(b+t). \end{aligned}$$

Remember that by def. $u_k = \mathfrak{a} u_{kt,(k+1)t} + \mathfrak{b}$, and thus

$$\begin{aligned} \phi(u_k(b)) &= \mathfrak{a} u_{kt,(k+1)t}(b+t) + \mathfrak{b}, \\ &= \mathfrak{a} u_{(k-1)t,kt}(b) + \mathfrak{b}. \\ &= u_{k-1}(b). \end{aligned}$$

Ingredient 2: Relations among elliptic functions

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

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

and

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

where

- $\tau_A : E \to E$ denotes the translation by A,
- and in $\mathbb{F}_q(E)$, $x_A = x \circ \tau_{-A}$ and $y_A = y \circ \tau_{-A}$.

A fast multiplication algorithm

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

This yields a multiplication tensor for Θ with quasi-linear complexity,

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

Notations :

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

The result [CL09a]

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.

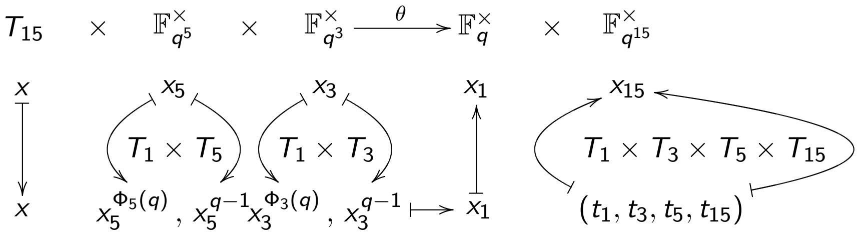
Application to Torus-based cryptography [DL09]

We have $q^n - 1 = \prod_{d \mid n} \Phi_d(q)$, and thus $\mathbb{F}_q^\times \simeq \prod_{d \mid n} T_d(\mathbb{F}_q)$.

$T_n(\mathbb{F}_q) \cong \{x \in \mathbb{F}_{q^n}^\times : x^{\Phi_n(q)} = 1\}$ is an alg. variety of dimension $\varphi(n)$.

Often, no known rational parameterization of $T_n(\mathbb{F}_q)$ with $\varphi(n)$-tuples.

Elliptic basis may yield efficient variants of a nice workaround due to van Dijk and Woodruff.



Conclusion

- We made use of torsion points on elliptic curves for finite field algorithms :
  - irreducible polynomials,
  - normal basis,
  - torus-based cryptography
  - discrete logarithms (in some very particular cases)
- It seems useful in other situations,
  - over the integers, with an elliptic AKS primality criterion,
  - over the p-adics, for counting points on curves.

Bibliography I

M. Agrawal, N. Kayal, and N. Saxena.
Primes is in p.
Annals of Mathematics, 160(2):781–793, 2004.

L.M. Adleman and H.W. Lenstra.
Finding irreducible polynomials over finite fields.
Proceedings of the 18th Annual ACM Symposium on the Theory of Computing, pages 350–355, 1986.

M. Ben-Or.
Probabilistic algorithms in finite fields.
22nd Annual Symposium on Foundations of Computer Science, 11:394–398, 1981.

J.-M. Couveignes and R. Lercier.
Elliptic periods for finite fields.
Finite Fields and their Applications, 15(1):1–22, January 2009.

J.-M. Couveignes and R. Lercier.
Fast construction of irreducible polynomials over finite fields.
Eprint arXiv:0905.1642v2, September 2009.
Submitted for publication.

C. Dunand and R. Lercier.
Normal Elliptic Bases and Torus-Based Cryptography.
Eprint arXiv:0909.0236v1, September 2009.
To appear in the proceedings of the *9-th international conference on finite fields and their applications* (Fq9).

S. Gao and H.W. Lenstra.
Optimal normal basis.
Designs, Codes and Cryptography, 2:315–323, 1992.

Bibliography II

A. Joux and R. Lercier.
The function field sieve in the medium prime case.
In *EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Comput. Sci.*, pages 254–270, 2006.

K.S. Kedlaya and C. Umans.
Modular composition in any characteristic.
Foundations of Computer Science, FOCS, 2008.

H. W. Lenstra and B. de Smit.
Standard models for finite fields: the definition.
`http://www.math.leidenuniv.nl/$\sim$desmit`, 2008.

R. Lidl and H. Niederreiter.
Finite Fields.
Addison-Wesley, 1983.