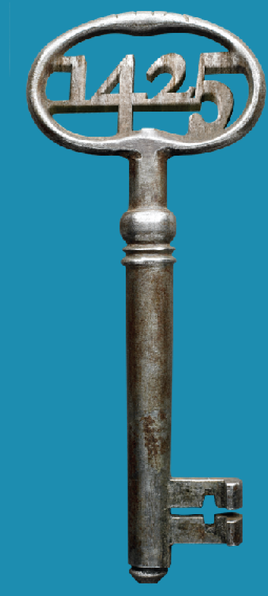
KU LEUVEN



Multiplication Polynomials for Elliptic Curves over Finite Local Rings

Riccardo Invernizzi Daniele Taufer
KU Leuven

Notation & standard results

We work on $R_k = \mathbb{F}_q[x]/(x^k) \cong \mathbb{F}_q[\varepsilon]$, where $q = p^e$ and p is a prime. R_k has one maximal principal ideal $\mathfrak{m} = (\varepsilon)$, with $\varepsilon^k = 0$.
An elliptic curve $E(R_k)$ is the set of points $P = (X : Y : Z) \in \mathbb{P}_2(R_k)$ satisfying

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3;$$

every point in E can be written as $P = (\alpha_x + \varepsilon\beta_x : \alpha_y + \varepsilon\beta_y : \alpha_z + \varepsilon\beta_z)$, and the standard projection

$$\pi : E(R_k) \to E(\mathbb{F}_q) \quad (\alpha_x + \varepsilon\beta_x : \alpha_y + \varepsilon\beta_y : \alpha_z + \varepsilon\beta_z) \mapsto (\alpha_x : \alpha_y : \alpha_z)$$

is a surjective group homomorphism.

Points over $\mathscr{O}$

$E^\infty := \pi^{-1}(0:1:0)$ is a p-subgroup of $E(R_k)$ with q^{k-1} elements. Every $P \in E^\infty$ can be written as $P = (X : 1 : Z)$.
Under broad assuptions it holds $E(R_k) \cong E(\mathbb{F}_q) \oplus E^\infty$.
Proposition: Let $P = (P_x : 1 : P_z) \in E^\infty$ be a point. There is a polynomial $\mathtt{f} \in R[x]$ such that $P_z = \mathtt{f}(P_x)$; moreover $x^3 | \mathtt{f}$.
Corollary: If P and Q are mulitple of a same point $(X : 1 : Z)$ and $R = P + Q$ then $R_x \in \langle X \rangle$.

Multiplication Polynomials

Given a curve E on R_k, for every $n \in \mathbb{N}$ there are uniquely defined coefficients $\psi_1(n), \dots, \psi_{k-1}(n) \in R_k$ such that for every point $P = (X : 1 : \mathtt{x})$ it holds

$$(nP)_x = \sum_{i=1}^{k-1} \psi_i(n) X^i.$$

The $i-th$ **multiplication polynomial** is ψ_i as a function $\mathbb{N} \to R_k$.
Remark: By definition, $\psi_i(1) = 0$ for all $i \geq 2$. $\psi_1(n) = n$ and $\psi_2(n) = \binom{n}{2} a_1$ can be shown easily.
Theorem: For every $1 \leq i \leq k-1$, the *i-th multiplication polynomial* ψ_i is a polynomial in $\mathbb{Q}[a_1, \dots, a_n][n]$ of degree i in n; moreover, $n | \psi_i(n)$.
Theorem: No primes greater than i appear in the factorization of the denominator of $\psi_i(n)$.
Corollary: Let p be a prime number. For every $l \geq 1$ and $1 \leq i < p$ it holds $\psi_i(p^l) \equiv 0 \bmod p^l$.

Group Structure

Corollary: Let $P = (X : 1 : \mathtt{f}(x)) \in E^\infty$ be a point, and p a prime number. Then

$$(pP)_x \equiv \psi_p(p) X^p \pmod{X}^{p+1}.$$

Proposition: Let E be an elliptic curve over R_k where $k \leq p$. Then we have the group isomorphism

$$E^\infty \cong (\mathbb{F}_p)^{e(k-1)}.$$

Definition: Let $r \in R_k \setminus \{0\}$. We define its *minimal degree* $\nu(r)$ as the maximal $i \geq 0$ such that $\varepsilon^i | r$. We also define $\nu(0) = \infty$. Finally, for every point $P \in E^\infty$, we define $\nu(P) = \nu(P_x)$.
If $\nu(P) \neq \nu(Q)$ then $\nu(P+Q) = \min\{\nu(P), \nu(Q)\}$. Moreover, if $p \nmid n$, then $\nu(nP) = \nu(P)$. Finally, if we assume $\psi_p(p) \in R_k^*$, then we have $\nu(p^iP) = p^i\nu(P)$.

Proposition: For every $1 \leq m \leq k-1$, if $P \in E^\infty$ has minimal degree $m = \nu(P)$, then its order is

$$ord(P) = p^{l_m}, \quad \text{where} \quad l_m = \left\lfloor \log_p \frac{k-1}{m} \right\rfloor + 1.$$

Theorem: Let E be an elliptic curve over R_k, such that $\psi_p(p) \in R_k^*$. Then

$$E^\infty \cong \prod_{\substack{1 \leq m \leq k-1 \\ (m,p)=1}} \left(\mathbb{Z}_{p^{l_m}}\right)^e.$$

The ECDLP

Given the coordinates of a point $P \in E$ and those of its multiple $Q = nP$, the **discrete logarithm problem** amounts to efficiently compute such $n \in \mathbb{Z}$.
From the results of the current paper, we efficiently recover the discrete logarithm of points in E^∞ over R_k. In fact, we can always write $n = b_0 + b_1p + \cdots + b_{k-1}p^{k-1}$.
Let $m_i = \nu(p^iP)$. Our results on multiplication polynomials imply

$$b_i = \left(\left(Q - \sum_{j=1}^{i-1} b_j p^j P \right)_x \bmod \varepsilon^{m_i+1} \right) \Big/ ((p^iP)_x \bmod \varepsilon^{m_i+1}).$$

We compute the $\log(n)$ digits b_i of n with two point multiplications ($\log(p)$ operations) at each step. Hence, the whole algorithm has a time complexity of $\log(p)\log(n)$. We **reduce the discrete logarithm problem over R_k to the corresponding problem over $\mathbb{F}_q$.**