KU LEUVEN

Multiplication polynomials for elliptic curves over finite local rings

Riccardo Invernizzi

Joint work with Daniele Taufer

ISSAC 2023

Tromsø, July 27th

0 Outline

KU LEUVEN

1 Outline

1 Elliptic curves

Definition

An elliptic curve E is the set of points $(X : Y : Z) \in \mathbb{P}^2(\mathbb{K})$ satisfying a Weierstrass equation, i.e.

$$y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3$$

for some field $\mathbb{K}$ ($\mathbb{F}_p$) such that $\Delta_E \neq 0$.

1 Elliptic curves

Definition

An elliptic curve E is the set of points $(X : Y : Z) \in \mathbb{P}^2(\mathbb{K})$ satisfying a Weierstrass equation, i.e.

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

for some field $\mathbb{K}$ ($\mathbb{F}_p$) such that $\Delta_E \neq 0$.

Remark

If $\mathrm{char}(\mathbb{K}) \notin \{2, 3\}$ we can work with the short Weierstrass equation

$$y^2z = x^3 + Axz^2 + Bz^3,$$

without loss of generality.

1 The group structure

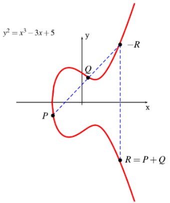
- An elliptic curve is equipped with an abelian group structure;

1 The group structure

- An elliptic curve is equipped with an abelian group structure;
- $\mathcal{O} = (0 : 1 : 0)$ is the zero;

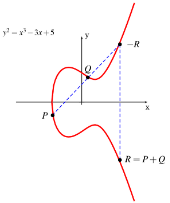
1 The group structure

- An elliptic curve is equipped with an abelian group structure;
- $\mathcal{O} = (0 : 1 : 0)$ is the zero;
- the sum is usually defined via the *chord-tangent* method.



1 The group structure

- An elliptic curve is equipped with an abelian group structure;
- $\mathcal{O} = (0 : 1 : 0)$ is the zero;
- the sum is usually defined via the *chord-tangent* method.



Theorem

Let p be a prime number, and E an elliptic curve defined over $\mathbb{F}_p$. There are positive integers $n, k \in \mathbb{Z}_{\geq 1}$ such that $n | (p-1)$ and

$$E(\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nk\mathbb{Z}.$$

1 The ECDLP

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

1 The ECDLP

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

- Given $P \in E$ and $n \in \mathbb{N}$, computing $Q = nP$ is easy ($\log(n)$ steps using *double & add*);

1 The ECDLP

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

- Given $P \in E$ and $n \in \mathbb{N}$, computing $Q = nP$ is easy ($\log(n)$ steps using *double & add*);
- given P and Q, recovering n is hard;

1 The ECDLP

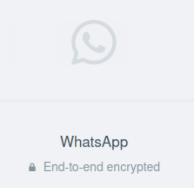
Let E be an elliptic curve over $\mathbb{F}_p$.

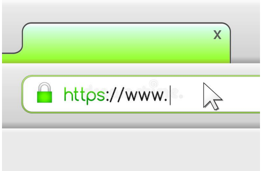
- Given $P \in E$ and $n \in \mathbb{N}$, computing $Q = nP$ is easy ($\log(n)$ steps using *double & add*);
- given P and Q, recovering n is hard;
- this is known as the **Discrete Logarithm Problem** (or **ECDLP**);

1 The ECDLP

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

- Given $P \in E$ and $n \in \mathbb{N}$, computing $Q = nP$ is easy ($\log(n)$ steps using *double & add*);
- given P and Q, recovering n is hard;
- this is known as the **Discrete Logarithm Problem** (or **ECDLP**);
- many modern cryptosystems (including *WhatsApp* and *TLS*) are based on ECDLP.





2 Outline

2 Finite local rings

- We focus on **finite local** rings;

2 Finite local rings

- We focus on **finite local** rings;
- in this presentation, we consider $R_k := \mathbb{F}_p[x]/x^k \cong \mathbb{F}_p[\epsilon]$;

2 Finite local rings

- We focus on **finite local** rings;
- in this presentation, we consider $R_k := \mathbb{F}_p[x]/x^k \cong \mathbb{F}_p[\epsilon]$;
- the definition of elliptic curve and the addition laws can be extended to finite local rings;

2 Finite local rings

- We focus on **finite local** rings;
- in this presentation, we consider $R_k := \mathbb{F}_p[x]/x^k \cong \mathbb{F}_p[\epsilon]$;
- the definition of elliptic curve and the addition laws can be extended to finite local rings;
- for a projective point $P = (X : Y : Z) \in E(R_k)$, we define its standard form as

2 Finite local rings

- We focus on **finite local** rings;
- in this presentation, we consider $R_k := \mathbb{F}_p[x]/x^k \cong \mathbb{F}_p[\epsilon]$;
- the definition of elliptic curve and the addition laws can be extended to finite local rings;
- for a projective point $P = (X : Y : Z) \in E(R_k)$, we define its standard form as
  - $(X \cdot Z^{-1} : Y \cdot Z^{-1} : 1)$ if $Z \in R_k^*$,

2 Finite local rings

- We focus on **finite local** rings;
- in this presentation, we consider $R_k := \mathbb{F}_p[x]/x^k \cong \mathbb{F}_p[\epsilon]$;
- the definition of elliptic curve and the addition laws can be extended to finite local rings;
- for a projective point $P = (X : Y : Z) \in E(R_k)$, we define its standard form as
  - $(X \cdot Z^{-1} : Y \cdot Z^{-1} : 1)$ if $Z \in R_k^*$,
  - $(X \cdot Y^{-1} : 1 : Z \cdot Y^{-1})$ if $Z \notin R_k^*$, $Y \in R_k^*$;

2 Finite local rings

- We focus on **finite local** rings;
- in this presentation, we consider $R_k := \mathbb{F}_p[x]/x^k \cong \mathbb{F}_p[\epsilon]$;
- the definition of elliptic curve and the addition laws can be extended to finite local rings;
- for a projective point $P = (X : Y : Z) \in E(R_k)$, we define its standard form as
  - $(X \cdot Z^{-1} : Y \cdot Z^{-1} : 1)$ if $Z \in R_k^*$,
  - $(X \cdot Y^{-1} : 1 : Z \cdot Y^{-1})$ if $Z \notin R_k^*$, $Y \in R_k^*$;
- the third case (i.e. $X \in R_k^*$, $Y, Z \notin R_k^*$) cannot happen because of the Weierstrass equation.

2 Subgroup at infinity

- We also define a projection $\pi : R_k \xrightarrow{\bmod \epsilon} \mathbb{F}_p$ sending

$$\alpha + \epsilon\beta \mapsto \alpha;$$

2 Subgroup at infinity

- We also define a projection $\pi : R_k \xrightarrow{\text{mod } \epsilon} \mathbb{F}_p$ sending

$$\alpha + \epsilon\beta \mapsto \alpha;$$

- the induced map $\pi : E(R_k) \to E(\mathbb{F}_p)$ is a surjective group homomorphism;

2 Subgroup at infinity

- We also define a projection $\pi : R_k \xrightarrow{\bmod \epsilon} \mathbb{F}_p$ sending

$$\alpha + \epsilon\beta \mapsto \alpha;$$

- the induced map $\pi : E(R_k) \to E(\mathbb{F}_p)$ is a surjective group homomorphism;
- $E^\infty := \pi^{-1}(\mathcal{O})$ is a p-subgroup of $E(R_k)$;

2 Subgroup at infinity

- We also define a projection $\pi : R_k \xrightarrow{\text{mod } \epsilon} \mathbb{F}_p$ sending

$$\alpha + \epsilon\beta \mapsto \alpha;$$

- the induced map $\pi : E(R_k) \to E(\mathbb{F}_p)$ is a surjective group homomorphism;
- $E^\infty := \pi^{-1}(\mathcal{O})$ is a p-subgroup of $E(R_k)$;
- all points $P \in E^\infty$ are in the second standard form, i.e. $P = (X : 1 : Z)$, with $\epsilon | X, Z$;

2 Subgroup at infinity

- We also define a projection $\pi : R_k \xrightarrow{\text{mod } \epsilon} \mathbb{F}_p$ sending
$$\alpha + \epsilon\beta \mapsto \alpha;$$
- the induced map $\pi : E(R_k) \to E(\mathbb{F}_p)$ is a surjective group homomorphism;
- $E^\infty := \pi^{-1}(\mathcal{O})$ is a p-subgroup of $E(R_k)$;
- all points $P \in E^\infty$ are in the second standard form, i.e. $P = (X : 1 : Z)$, with $\epsilon | X, Z$;
- for *non-anomalous* curves (i.e. $\#E(\mathbb{F}_p) \neq p$) it holds
$$E(R_k) \cong E(\mathbb{F}_p) \oplus E^\infty;$$

2 Subgroup at infinity

- We also define a projection $\pi : R_k \xrightarrow{\text{mod } \epsilon} \mathbb{F}_p$ sending

$$\alpha + \epsilon\beta \mapsto \alpha;$$

- the induced map $\pi : E(R_k) \to E(\mathbb{F}_p)$ is a surjective group homomorphism;
- $E^\infty := \pi^{-1}(\mathcal{O})$ is a p-subgroup of $E(R_k)$;
- all points $P \in E^\infty$ are in the second standard form, i.e. $P = (X : 1 : Z)$, with $\epsilon | X, Z$;
- for *non-anomalous* curves (i.e. $\#E(\mathbb{F}_p) \neq p$) it holds

$$E(R_k) \cong E(\mathbb{F}_p) \oplus E^\infty;$$

- we restrict our attention to E^∞.

3 Outline

3 Point sum

Proposition

There exist a polynomial $\mathtt{f} \in R_k[x]$ such that $x^3 | \mathtt{f}$, and for every point $P = (X : 1 : Z) \in E^\infty$ it holds $Z = \mathtt{f}(X)$.

KU LEUVEN

3 Point sum

Proposition

There exist a polynomial $\mathtt{f} \in R_k[x]$ such that $x^3|\mathtt{f}$, and for every point $P = (X : 1 : Z) \in E^\infty$ it holds $Z = \mathtt{f}(X)$.

Corollary

Given $P = (P_x : 1 : P_z)$, $Q = (Q_x : 1 : Q_z) \in E^\infty$ it holds

$$(P + Q)_x \in \langle P_x, Q_x \rangle.$$

In particular, $(nP)_x \in \langle P_x \rangle$.

3 Multiplication polynomials

As a consequence, for $P = (X : 1 : \mathtt{f}(X))$ we can write

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

3 Multiplication polynomials

As a consequence, for $P = (X : 1 : \mathtt{f}(X))$ we can write

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

Definition

The i**-th multiplication polynomial** is the unique function $\mathbb{N} \to R_k$ which sends n to $\psi_i(n)$.

3 Multiplication polynomials

As a consequence, for $P = (X : 1 : \mathtt{f}(X))$ we can write

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

Definition

The i-**th multiplication polynomial** is the unique function $\mathbb{N} \to R_k$ which sends n to $\psi_i(n)$.

Remark

ψ_i is well defined as a function; it is not clear yet that this should be a polynomial in n.

3 Multiplication polynomials

Remark

It can be shown directly that $\psi_1(n) = n$, $\psi_2(n) = \binom{n}{2} a_1 = \frac{n(n-1)}{2} a_1$.

3 Multiplication polynomials

Remark

It can be shown directly that $\psi_1(n) = n$, $\psi_2(n) = \binom{n}{2} a_1 = \frac{n(n-1)}{2} a_1$.

Theorem (I. and Taufer, 2023)

$\psi_i(n)$ is a degree-i polynomial in $\mathbb{Q}[a_1, \ldots, a_6][n]$ with no constant term. Moreover, no primes greater than i appears in the denominators of $\psi_i(n)$.

4 Outline

4 The jump

We fix p a prime number, $R_k = \mathbb{F}_p[\epsilon]$.

Corollary

For $i \leq p-1$,

$$\psi_i(p) \equiv 0 \bmod p.$$

4 The jump

We fix p a prime number, $R_k = \mathbb{F}_p[\epsilon]$.

Corollary

For $i \leq p - 1$,

$$\psi_i(p) \equiv 0 \bmod p.$$

Proposition

Let $E(R_k)$ be a curve, $P \in E$. It holds

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

4 Minimal degree

Definition

For a point $P = (X : 1 : Z) \in E^{\infty}$ we define $\nu(P)$ as the minimal i s.t. $\epsilon^i | X$.

4 Minimal degree

Definition

For a point $P = (X : 1 : Z) \in E^\infty$ we define $\nu(P)$ as the minimal i s.t. $\epsilon^i | X$.

Remark

For every $P \in E^\infty$ it holds $\nu(P) \geq 1$.

4 Minimal degree

Definition

For a point $P = (X : 1 : Z) \in E^\infty$ we define $\nu(P)$ as the minimal i s.t. $\epsilon^i | X$.

Remark

For every $P \in E^\infty$ it holds $\nu(P) \geq 1$.

Proposition

Let $P, Q \in E^\infty$. Then

- if $\nu(P) \neq \nu(Q)$, $\nu(P+Q) = \min(\nu(P), \nu(Q))$;

4 Minimal degree

Definition

For a point $P = (X : 1 : Z) \in E^\infty$ we define $\nu(P)$ as the minimal i s.t. $\epsilon^i | X$.

Remark

For every $P \in E^\infty$ it holds $\nu(P) \geq 1$.

Proposition

Let $P, Q \in E^\infty$. Then

- if $\nu(P) \neq \nu(Q)$, $\nu(P + Q) = \min(\nu(P), \nu(Q))$;
- if $p \nmid n$, $\nu(nP) = \nu(P)$;

4 Minimal degree

Definition

For a point $P = (X : 1 : Z) \in E^\infty$ we define $\nu(P)$ as the minimal i s.t. $\epsilon^i | X$.

Remark

For every $P \in E^\infty$ it holds $\nu(P) \geq 1$.

Proposition

Let $P, Q \in E^\infty$. Then

- if $\nu(P) \neq \nu(Q)$, $\nu(P+Q) = \min(\nu(P), \nu(Q))$;
- if $p \nmid n$, $\nu(nP) = \nu(P)$;
- $\nu(pP) = p\nu(P)$ (assuming $\psi_p(p) \in R_k^*$).

KU LEUVEN

4 Group structure

Lemma

We obtain the following:

- $pP = \mathcal{O}$ if and only if $p\nu(P) \geq k$;

4 Group structure

Lemma

We obtain the following:

- $pP = \mathcal{O}$ if and only if $p\nu(P) \geq k$;
- $g_i := (\epsilon^i : 1 : \mathtt{f}(\epsilon^i))$ for $(i, p) = 1$ are $\mathbb{F}_p$-linearly independent.

4 Group structure

Lemma

We obtain the following:

- $pP = \mathcal{O}$ if and only if $p\nu(P) \geq k$;
- $g_i := (\epsilon^i : 1 : \mathtt{f}(\epsilon^i))$ for $(i,p) = 1$ are $\mathbb{F}_p$-linearly independent.

Theorem (I. and Taufer, 2023)

Let E be an elliptic curve over R_k s.t. $\#E(\mathbb{F}_p) \neq p$ and $\psi_p(p) \in R_k^*$. Then

$$E \cong E(\mathbb{F}_p) \times \prod_{\substack{1 \leq m \leq k-1 \\ (m,p)=1}} \mathbb{Z}/p^{l_m}\mathbb{Z}, \text{ where } \quad l_m = \left\lfloor \log_p \frac{k-1}{m} \right\rfloor + 1.$$

KU LEUVEN

4 The ECDLP

Let

$$P_x = a_1\epsilon + a_2\epsilon^2 + \cdots + a_{k-1}\epsilon^{k-1}$$

and

$$n = b_0 + b_1 p + b_2 p^2 + \cdots + b_d p^d.$$

Suppose we know P, $Q = nP$ and want to recover n. Then:

4 The ECDLP

Let

$$P_x = a_1\epsilon + a_2\epsilon^2 + \cdots + a_{k-1}\epsilon^{k-1}$$

and

$$n = b_0 + b_1 p + b_2 p^2 + \cdots + b_d p^d.$$

Suppose we know P, $Q = nP$ and want to recover n. Then:

$$Q_x \equiv a_1 b_0 \epsilon \bmod \epsilon^2$$

4 The ECDLP

Let

$$P_x = a_1\epsilon + a_2\epsilon^2 + \cdots + a_{k-1}\epsilon^{k-1}$$

and

$$n = b_0 + b_1 p + b_2 p^2 + \cdots + b_d p^d.$$

Suppose we know P, $Q = nP$ and want to recover n. Then:

$$Q_x \equiv a_1 b_0 \epsilon \bmod \epsilon^2 \Rightarrow b_0 = Q_x^{(1)} \cdot a_1^{-1}$$

4 The ECDLP

Let

$$P_x = a_1\epsilon + a_2\epsilon^2 + \cdots + a_{k-1}\epsilon^{k-1}$$

and

$$n = b_0 + b_1 p + b_2 p^2 + \cdots + b_d p^d.$$

Suppose we know P, $Q = nP$ and want to recover n. Then:

$$(Q - b_0 P)_x \equiv a_1' b_1 \epsilon^p \bmod \epsilon^{p+1}$$

4 The ECDLP

Let

$$P_x = a_1\epsilon + a_2\epsilon^2 + \cdots + a_{k-1}\epsilon^{k-1}$$

and

$$n = b_0 + b_1 p + b_2 p^2 + \cdots + b_d p^d.$$

Suppose we know P, $Q = nP$ and want to recover n. Then:

$$(Q - b_0 P)_x \equiv a_1' b_1 \epsilon^p \bmod \epsilon^{p+1} \Rightarrow b_1 = (Q - b_0 P)_x^{(p)} \cdot (a_1')^{-1}$$

4 The ECDLP

Let

$$P_x = a_1\epsilon + a_2\epsilon^2 + \cdots + a_{k-1}\epsilon^{k-1}$$

and

$$n = b_0 + b_1 p + b_2 p^2 + \cdots + b_d p^d.$$

Suppose we know P, $Q = nP$ and want to recover n. Then:

$$\ldots$$

4 The ECDLP

Theorem (I. and Taufer, 2023)

It holds

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

where $m_i = \nu(p^i P)$. Over E^∞, the discrete logarithm can hence be solved in time $\mathcal{O}(\log(p)\log(n))$. As a consequence, the discrete logarithm over $E(R_k)$ can be efficiently reduced to the corresponding logarithm over $E(\mathbb{F}_p)$.

Thank you for your attention.