Field Extensions and Elliptic Curves

August 1, 2024

Distributed Lab

zkdl-camp.github.io

github.com/ZKDL-Camp

Plan

Field Extensions

$\mathbb{Q}$ vs $\mathbb{R}$

Question #1

What is the difference between rational numbers $\mathbb{Q}$ and real numbers $\mathbb{R}$?

Definition

Rational numbers $\mathbb{Q}$ are defined as the set $\{\frac{n}{m} : n \in \mathbb{Z}, m \in \mathbb{N}\}$.

Question #2

Why cannot we say $m \in \mathbb{Z}$, similarly to n?

Theorem

$\sqrt{2}$ is not a rational number. Neither is π and e. But they are reals.

Conclusion

$\mathbb{R}$ is sort of "an extended version of $\mathbb{Q}$".

What about $\mathbb{R}$?

Rethorical Question

Can we extend $\mathbb{R}$?

Yes — just use complex numbers $\mathbb{C}$!

Definition

Complex numbers $\mathbb{C}$ is defined as the set of $x + iy$ where $i^2 = -1$.

Definition

Complex numbers $\mathbb{C}$ are defined as the set of pairs $(x, y) \in \mathbb{R}^2$ where addition is defined as $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, and the multiplication is:

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1).$$

A bit about complex numbers

Theorem

$(\mathbb{C}, +, \times)$ *is a field.*

Example

Let us see how arithmetic is performed in $\mathbb{C}$.

- **Addition:** $(2+3i)+(4+5i) = 6+8i$.
- **Multiplication:** $(1+i)(2+i) = 2+3i+i^2 = 1+3i$.
- **Division:**

$$\frac{2+i}{1+i} = \frac{(2+i)(1-i)}{(1+i)(1-i)} = \frac{2-i-i^2}{1-i^2} = \frac{3-i}{2} = \frac{3}{2} - \frac{1}{2}i$$

Question

What is $(1+i)+(2+i)$? $i(1+i)$? $1/i$?

Field Extension

Conclusion + Question

$\mathbb{C}$ is sort of "an extended version of $\mathbb{R}$". Thus, we have

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}, \text{ where } \mathbb{Q}, \mathbb{R}, \mathbb{C} \text{ are fields}$$

So we have two questions in mind:

- Is there any mathematical term for this?
- Can we go further?

Definition

Let $\mathbb{F}$ be a field. A field $\mathbb{K}$ is called an **extension** of $\mathbb{F}$ if $\mathbb{F} \subset \mathbb{K}$ which we denote as $\mathbb{K}/\mathbb{F}$.

Example

$\mathbb{C}/\mathbb{R}$ is a field extension. So is $\mathbb{R}/\mathbb{Q}$.

$\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$

Example

Define $\mathbb{Q}(\sqrt{2}) := \{p + q\sqrt{2} : p, q \in \mathbb{Q}\}$. This is a field extension of $\mathbb{Q}$. Arithmetic over $\mathbb{Q}(\sqrt{2})$ looks like:

- **Addition:** $(1 + 2\sqrt{2}) + (3 + 4\sqrt{2}) = 4 + 6\sqrt{2}$.
- **Multiplication:** $(1 + 2\sqrt{2})(1 + \sqrt{2}) = 1 + 3\sqrt{2} + 2\sqrt{2}^2 = 5 + 3\sqrt{2}$.
- **Division:**

$$\frac{1 + 2\sqrt{2}}{1 + \sqrt{2}} = \frac{(1 + 2\sqrt{2})(\sqrt{2} - 1)}{(\sqrt{2} + 1)(\sqrt{2} - 1)}$$

Example

Similarly, $\mathbb{Q}(i) := \{p + qi : p, q \in \mathbb{Q}\}$ is a field extension of $\mathbb{Q}$.

$\mathbb{Q}(\sqrt{2}, i)$

Example

Define $\mathbb{Q}(\sqrt{2}, i) = \{\alpha + \beta\sqrt{2} : \alpha, \beta \in \mathbb{Q}(i)\}$. Typicall element of $\mathbb{Q}(\sqrt{2}, i)$ can be written as:

$$(a + bi) + (c + di)\sqrt{2} = a + c\sqrt{2} + b\sqrt{2}i + di\sqrt{2}$$

Notice

Each element of $\mathbb{Q}(\sqrt{2}, i)$ is a linear combination of $\{1, \sqrt{2}, i, \sqrt{2}i\}$. This is usually called a **basis**. Moreover, to denote the dimensionality of $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$, we write $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.

Real Polynomials modulo $x^2 + 1$

Definition... "Kinda"

Consider the set $\mathcal{P}$ — a set of polynomials $\mathbb{R}[x]$ modulo $p(x) := x^2 + 1$.

Example

For example, $1,\ 5 + x,\ 3x,\ 1 + 2x \in \mathcal{P}$.

But what about $x^2 + 2x + 4$? We can divide by $x^2 + 1$!

$$x^2 + 2x + 4 = (x^2 + 1) \cdot 1 + (2x + 3)$$

So in $\mathcal{P}$, we have $x^2 + 2x + 4 = 2x + 3$.

Real Polynomials modulo $x^2 + 1$

Arithmetic

Over this field, we can do arithmetic as usual.

- **Addition:** $(1 + x) + (2 + 3x) = 3 + 4x$.
- **Multiplication:** $(1 + x)(2 + x) = x^2 + 3x + 2 = 3x + 1$.
- **Inverse**:

$$\left(\frac{1+x}{2}\right)^{-1} = 1 - x$$

Indeed,

$$\frac{1+x}{2} \cdot (1 - x) = \frac{1}{2} \cdot (1 - x^2) = \frac{1}{2}\left(-(x^2 + 1) + 2\right) = 1 \text{ (in } \mathcal{P})$$

Hold on a minute...

Results

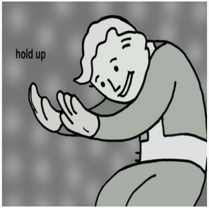
- $(1 + x) + (2 + 3x) = 3 + 4x$
- $(1 + x)(2 + x) = 1 + 3x$
- $\left(\frac{1+x}{2}\right)^{-1} = 1 - x$

Same, but over $\mathbb{C}$

Let us do the same, but instead of X, use i.

- $(1 + i) + (2 + 3i) = 3 + 4i.$
- $(1 + i)(2 + i) = 2 + 3i + i^2 = 1 + 3i.$
- $\frac{1}{\frac{1+i}{2}} = \frac{2}{1+i} = \frac{2(1-i)}{(1+i)(1-i)} = 1 - i.$

Hold on a minute...



So, basically, $\mathcal{P}$ and $\mathbb{C}$ have the same structure! Formally, they are isomorphic: $\mathcal{P} \cong \mathbb{C}$.

Question

Could we have used $x^2 + 3$ instead of $x^2 + 1$? What about $x^2 + x + 1$?

Yes, any **irreducible** 2nd-degree polynomial $p(x)$ over $\mathbb{R}$ can be used. Typically, this is denoted as $\boxed{\mathbb{R}[x]/(p(x))}$.

Isomorphisms

Reminder

For two groups $(\mathbb{G}, +)$ and $(\mathbb{H}, \times)$ we defined homomorphism to be a function $\phi : \mathbb{G} \to \mathbb{H}$ such that

$$\phi(a+b) = \phi(a) \times \phi(b)$$

However, we claim that $\mathbb{R}/(x^2+1) \cong \mathbb{C}$, which are fields!

Definition

A **field isomorphism** is a function $\phi : (\mathbb{F}, +, \times) \to (\mathbb{K}, \oplus, \otimes)$ such that

- $\phi(a+b) = \phi(a) \oplus \phi(b)$
- $\phi(a \times b) = \phi(a) \otimes \phi(b)$
- $\phi(1_{\mathbb{F}}) = 1_{\mathbb{K}}$

But for now, $\cong$ means "exhibit the same structure".

Key Theorems

Theorem

*Let $\mathbb{F}$ be a field and $\mu(x)$ — irreducible polynomial over $\mathbb{F}$ (**reduction polynomial**). Consider a set of polynomials over $\mathbb{F}[x]$ modulo $\mu(x) \in \mathbb{F}[x]$, formally denoted as $\mathbb{F}[x]/(\mu(x))$. Then, $\mathbb{F}[x]/(\mu(x))$ is a field.*

Theorem

Let $\mathbb{F}$ be a field and $\mu \in \mathbb{F}[X]$ is an irreducible polynomial of degree n and let $\mathbb{K} := \mathbb{F}[X]/(\mu(X))$. Let $\theta \in \mathbb{K}$ be the root of μ over $\mathbb{K}$. Then,

$$\mathbb{K} = \{c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} : c_0, \dots, c_{n-1} \in \mathbb{F}\}$$

Coming back to previous examples

Example

Again, consider $\mathbb{Q}(\sqrt{2}) = \{q + p\sqrt{2} : p, q \in \mathbb{Q}\}$. Then,

$$\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$$

Example

Similarly, $\mathbb{Q}(i) \cong \mathbb{Q}[x]/(x^2 + 1)$.

Example

And $\mathbb{Q}(\sqrt{2}, i)$ is just a little bit more tricky. Notice that we can take

$$p(x) := (x^2 - 2)(x^2 + 1) = x^4 - x^2 - 2$$

So $\mathbb{Q}(\sqrt{2}, i) \cong \mathbb{Q}[x]/(x^4 - x^2 - 2)$.

Finite Field Extension

Definition

Recall that $\mathbb{F}_p$ (**prime field**) is a set $\{0, 1, \ldots, p-1\}$ with arithmetic modulo p.

In many cases, we need to extend $\mathbb{F}_p$ $2, 4, 8, 12, 24$ times. For this, we use the so-called **finite field extension**.

Definition

Suppose p is prime and $m \geq 2$. Let $\mu \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree m. Then, elements of $\mathbb{F}_{p^m}$ are polynomials in $\mathbb{F}_p^{(\leq m)}[X]$ modulo $\mu(x)$. In other words,

$$\mathbb{F}_{p^m} = \{c_0 + c_1 X + \cdots + c_{m-1} X^{m-1} : c_0, \ldots, c_{m-1} \in \mathbb{F}_p\},$$

where all operations are performed modulo $\mu(X)$.

Examples

It would be convenient to build $\mathbb{F}_{p^2}$ as $\mathbb{F}_p[i]/(i^2+1)$, but is it always possible? In other words, when $X^2 = -1$ has a solution in $\mathbb{F}_p$?

Theorem

Let p be an odd prime. Then X^2+1 is irreducible in $\mathbb{F}_p[X]$ if and only if $p \equiv 3 \pmod 4$.

Example

Pick $p = 19$. Then $\mathbb{F}_{361} := \mathbb{F}_{19}[i]/(i^2+1)$. So typical elements are: $1+3i,\ 10+15i,\ 18+18i,\ 5,\ 7i,\ \ldots$

- **Addition:** $(1+10i)+(18+15i) = 19+25i = 6i$.
- **Multiplication:** $(5+6i)(6+7i) = 30+71i+42i^2 = -12+71i = 7+14i$.

More Examples: Binary Extension Fields

Example

Consider the $\mathbb{F}_{2^4}$. Then, there are 16 elements in this set:

$$
\begin{aligned}
&0, 1, X, X+1,\\
&X^2, X^2+1, X^2+X, X^2+X+1,\\
&X^3, X^3+1, X^3+X, X^3+X+1,\\
&X^3+X^2, X^3+X^2+1, X^3+X^2+X, X^3+X^2+X+1.
\end{aligned}
$$

Set $\mu(X) := X^4 + X + 1$. Then, operations are performed in the following manner:

- **Addition:** $(X^3 + X^2 + 1) + (X^2 + X + 1) = X^3 + X$.
- **Multiplication:** $(X^3 + X^2 + 1) \cdot (X^2 + X + 1) = X^2 + 1$ since:
- **Inversion:** $(X^3 + X^2 + 1)^{-1} = X^2$ since $(X^3 + X^2 + 1) \cdot X^2 \bmod (X^4 + X + 1) = 1$.

More Examples: BN254

Example

Consider the **BN254 scalar field**, used in SNARKs:

$$p = \texttt{0x30644e72e131a029} \cdots \texttt{a8d3c208c16d87cfd47}$$

- Then, $\mathbb{F}_{p^2} := \mathbb{F}_p[u]/(u^2+1)$ since $p \equiv 3 \pmod 4$.
- Define $\xi := 9 + u \in \mathbb{F}_{p^2}$. Then, set $\mathbb{F}_{p^6} := \mathbb{F}_{p^2}[v]/(v^3 - \xi)$.
- Finally, set $\mathbb{F}_{p^{12}} := \mathbb{F}_{p^6}[w]/(w^2 - v)$.

Equivalently, we can write:

$$\mathbb{F}_{p^{12}} := \mathbb{F}_p[w]/(w^{12} - 18w^6 + 82)$$

Algebraic Closure

Definition

Definition

A field $\mathbb{F}$ is called **algebraically closed** if every non-constant polynomial $p(x) \in \mathbb{F}[X]$ has a root in $\mathbb{F}$.

Example

$\mathbb{R}$ is not algebraically closed since $X^2 + 1$ has no roots in $\mathbb{R}$. However, $\mathbb{C}$ is algebraically closed, which follows from the fundamental theorem of algebra. Since $\mathbb{C}$ is a field extension of $\mathbb{R}$, it is also an algebraic closure of $\mathbb{R}$. This is commonly denoted as $\overline{\mathbb{R}} = \mathbb{C}$.

Definition

A field $\mathbb{K}$ is called an **algebraic closure** of $\mathbb{F}$ if $\mathbb{K}/\mathbb{F}$ is algebraically closed. This is denoted as $\overline{\mathbb{F}} = \mathbb{K}$.

Algebraic Closure for Finite Fields

Recall that we are cryptographers, not mathematicials. So we are interested in $\overline{\mathbb{F}}_p$. So I have two news to you:

- **Good news:** $\overline{\mathbb{F}}_p$ exists.
- **Bad news:** $\overline{\mathbb{F}}_p$ is infinite.

Theorem

No finite field $\mathbb{F}$ is algebraically closed.

Proof. Suppose $a_1, a_2, \ldots, a_n \in \mathbb{F}$ are all elements of $\mathbb{F}$. Consider

$$p(x) := \prod_{i=1}^{n}(x - a_i) + 1 = (x - a_1)(x - a_2)\cdots(x - a_n) + 1.$$

Clearly, $p(x)$ is a non-constant polynomial and has no roots in $\mathbb{F}$, since for any $a \in \mathbb{F}$, one has $p(a) = 1$. ■

So what?

But what form does the $\overline{\mathbb{F}}_p$ have? Well, it is a union of all $\mathbb{F}_{p^k}$ for $k \geq 1$. This is formally written as:

$$\boxed{\overline{\mathbb{F}}_p = \bigcup_{k \in \mathbb{N}} \mathbb{F}_{p^k}}$$

Remark

But this definition is super counter-intuitive! So here how we usually interpret it. Suppose I tell you that polynomial $q(x)$ has a root in $\overline{\mathbb{F}}_p$. What that means is that there exists some extension $\mathbb{F}_{p^m}$ such that for some $\alpha \in \mathbb{F}_{p^m}$, $q(\alpha) = 0$. We do not know how large this m is, but we know that it exists. For that reason, $\overline{\mathbb{F}}_p$ is defined as an infinite union of all possible field extensions.

Elliptic Curve

Definition

Definition

Suppose that $\mathbb{K}$ is a field. An **elliptic curve** E over $\mathbb{K}$ is defined as a set of points $(x, y) \in \mathbb{K}^2$:

$$y^2 = x^3 + ax + b,$$

called a **Short Weierstrass equation**, where $a, b \in \mathbb{K}$ and $4a^3 + 27b^2 \neq 0$. We denote $E/\mathbb{K}$ to denote the elliptic curve over field $\mathbb{K}$.

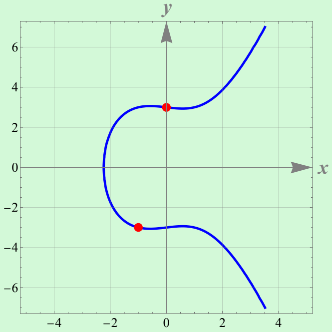
Definition

We say that $P = (x_P, y_P) \in \mathbb{A}^2(\mathbb{K})$ is the **affine representation** of the point on the elliptic curve $E/\mathbb{K}$ if it satisfies the equation $y_P^2 = x_P^3 + ax_P + b$.

Examples

Example

Consider $E/\mathbb{Q} : y^2 = x^3 - x + 9$. Valid affine points on $E/\mathbb{Q}$ are, for example, $P = (0, 3), Q = (-1, -3) \in \mathbb{A}^2(\mathbb{Q})$.



More Examples

Some more examples[1]:

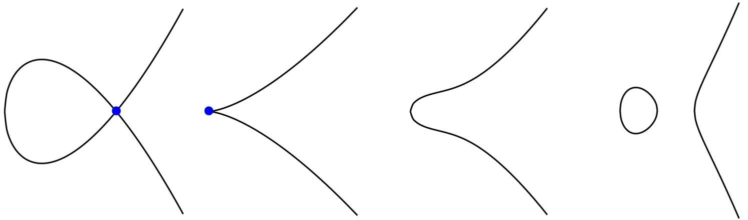


Figure 2.1: Singular curve $y^2 = x^3 - 3x + 2$ over $\mathbb{R}$.

Figure 2.2: Singular curve $y^2 = x^3$ over $\mathbb{R}$.

Figure 2.3: Smooth curve $y^2 = x^3 + x + 1$ over $\mathbb{R}$.

Figure 2.4: Smooth curve $y^2 = x^3 - x$ over $\mathbb{R}$.

[1] Figure taken from "Pairings for Beginners"

Real Elliptic Curves

But real elliptic curves are not that simple. Here how they look like[2]:

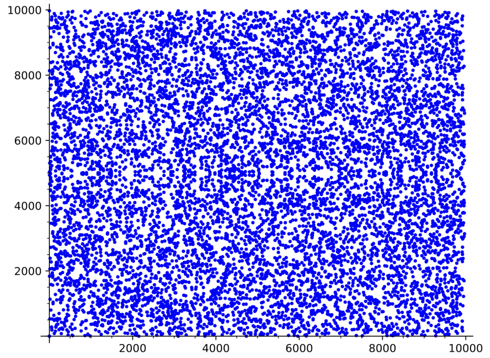


Figure: Curve $E/\mathbb{F}_{9973} : y^2 = x^3 - 2x + 1$ over the finite field

[2] Figure taken from "Moonmath"

Defining a Group Structure: A Few Words

Definition

The set of points on the curve, denoted as $E_{a,b}(\mathbb{K})$, is defined as:

$$E_{a,b}(\mathbb{K}) = \{(x, y) \in \mathbb{A}^2(\mathbb{K}) : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is the so-called **point at infinity**.

Remark #1

If $(x_P, y_P) \in E(\mathbb{K})$ then $(x_P, -y_P) \in E(\mathbb{K})$.

Remark #2

Typically, $\mathbb{K} = \overline{\mathbb{F}}_p$: we do not conretize over which finite field we define the elliptic curve.

Defining a Group Structure: Chord Method

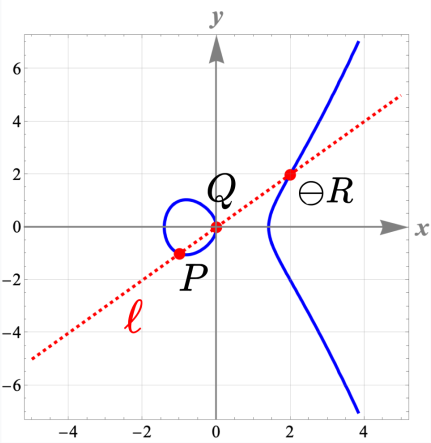


Figure: Chord method for adding two points

Defining a Group Structure: Tangent Method

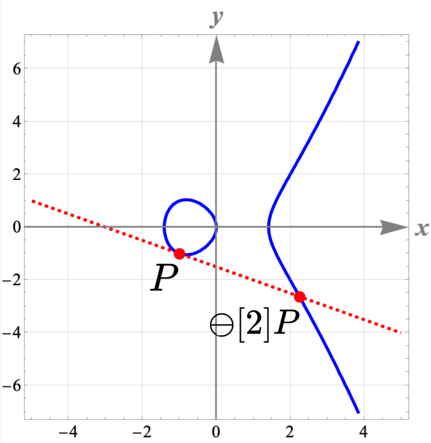


Figure: Tangent method for the point doubling

Idea of Derivation

Line equation through $P = (x_P, y_P), Q = (x_Q, y_Q)$:

$$\ell : y = \lambda(x - x_P) + y_P,\ \lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

So all we need is to solve the system of equations:

$$\begin{cases} y^2 = x^3 + ax + b \\ y = \lambda(x - x_P) + y_P \end{cases}$$

Substituting y from the second equation to the first one, we get a cubic equation. Using Vieta's formula, one can derive

$$x_P + x_Q + x_R = \lambda^2$$

The rest is easy to finish.

Group Law

Definition

1. Point at infinity $\mathcal{O}$ is an identity element.
2. If $x_P \neq x_Q$, use the **chord method**. Define $\lambda := \frac{y_P - y_Q}{x_P - x_Q}$ — the slope between P and Q. Set the resultant coordinates as:
$$x_R := \lambda^2 - x_P - x_Q, \quad y_R := \lambda(x_P - x_R) - y_P.$$
3. If $x_P = x_Q$ and $y_P = y_Q$ (that is, $P = Q$), use the **tangent method**. Define the slope of the tangent at P as $\lambda := \frac{3x_P^2 + a}{2y_P}$ and set
$$x_R := \lambda^2 - 2x_P, \quad y_R := \lambda(x_P - x_R) - y_P.$$
4. Otherwise, define $P \oplus Q := \mathcal{O}$.

One more Illustration

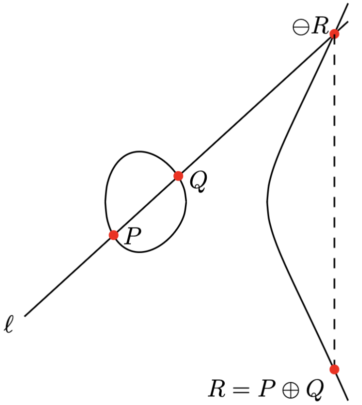


Figure 2.5: Elliptic curve addition.

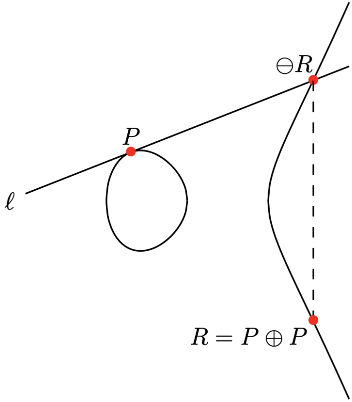


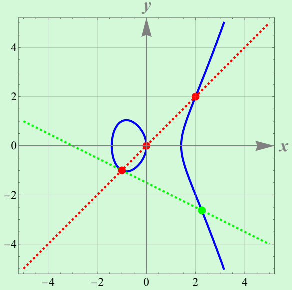
Figure 2.6: Elliptic curve doubling.

Example

Example

Consider $E/\mathbb{R} : y^2 = x^3 - 2x$.

- **Addition:** $(-1,1) \oplus (0,0) = (2,-2)$, $(2,2) \oplus (-1,-1) = (0,0)$.
- **Doubling:** $[2](-1,-1) = \left(\frac{9}{4}, -\frac{21}{8}\right)$.



Hasse's Theorem

Theorem

$(E(\overline{\mathbb{F}}), \oplus)$ *forms an abelian group.*

Now, let us consider the group order $r := |E(\mathbb{F}_{p^m})|$.

Theorem

Hasse's Theorem on Elliptic Curves. *$r = p^m + 1 - t$ for some integer $|t| \leq 2\sqrt{p^m}$. A bit more intuitive explanation: the number of points on the curve is close to $p^m + 1$. The value t is called the* ***trace of Frobenius****.*

Remark

In fact, $r = |E(\mathbb{F}_{p^m})|$ can be computed in $O(\log(p^m))$, so the number of points can be computed efficiently even for fairly large primes p.

Discrete Logarithm

Definition

Let $P \in E(\overline{\mathbb{F}}_p)$ and $\alpha \in \mathbb{Z}_r$. Define the scalar multiplication $[\alpha]P$ as adding P to itself $\alpha - 1$ times (also set $[0]P := \mathcal{O}$).

Definition

Suppose E is cyclic, meaning, $\langle G \rangle = E$ for some $G \in E$. The **discrete logarithm problem** on E consists in the following: suppose $P = [\alpha]G$ for some $\alpha \in \mathbb{Z}_r$. Find α based on P.

Remark

If r is a product of primes $p_1, p_2, \ldots, p_k$ such that $p_1 < p_2 < \cdots < p_k$, then the best-known algorithm to solve the discrete logarithm problem is no significantly better than $O(\sqrt{p_1})$.

Thank you for your attention

♥

zkdl-camp.github.io
github.com/ZKDL-Camp