Projective Coordinates and Pairing

Distributed Lab

August 8, 2024

Plan

1. Affine Coordinates Issue: Recap
   - Recap
   - Addition Complexity
2. Relations
   - Definition
   - Equivalence Relation
3. Elliptic Curve in Projective Coordinates
   - Projective Space Definition
   - Elliptic Curve Equation in Projective Space
   - Projective Addition
4. Pairings
   - Basic Definition
   - Elliptic Curve-based Pairing
   - Application #1: BLS Signature
   - Application #2: Quadratic Verifications

Affine Coordinates Issue: Recap

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 $\mathbb{K}$.

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

Point $P \in E(\overline{\mathbb{F}}_p)$, represented by coordinates (x_P, y_P) is called the **affine representation** of P and denoted as $P \in \mathbb{A}^2(\overline{\mathbb{F}}_p)$.

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

Point $P \in E(\overline{\mathbb{F}}_p)$, represented by coordinates (x_P, y_P) is called the **affine representation** of P and denoted as $P \in \mathbb{A}^2(\overline{\mathbb{F}}_p)$.

Definition

$E(\mathbb{K}) = E/\mathbb{K} \cup \{\mathcal{O}\}$. $(E(\mathbb{K}), \oplus)$ forms a group, where $\oplus$ is the **point addition** operation.

Addition and Doubling Illustratins

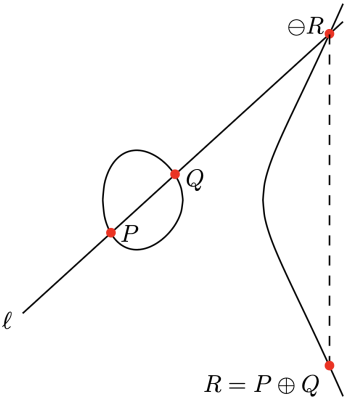


Figure 2.5: Elliptic curve addition.

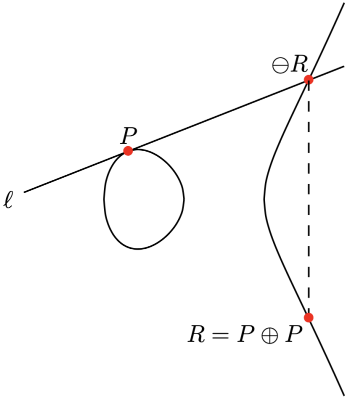


Figure 2.6: Elliptic curve doubling.

Figure: Illustration of chord-and-tangent points addition.

Affine Point Addition

So, how do we add $(x_R, y_R) = (x_P, y_P) \oplus (x_Q, y_Q)$ where (x_P, y_P) and (x_Q, y_Q) are affine representation of points $P, Q \in E(\overline{\mathbb{F}}_p)$?

Affine Point Addition

So, how do we add $(x_R, y_R) = (x_P, y_P) \oplus (x_Q, y_Q)$ where (x_P, y_P) and (x_Q, y_Q) are affine representation of points $P, Q \in E(\overline{\mathbb{F}}_p)$?

Algorithm 1: Classical adding P and Q for $x_P \neq x_Q$

1. Calculate the slope $\lambda \leftarrow (y_P - y_Q)/(x_P - x_Q)$.

Affine Point Addition

So, how do we add $(x_R, y_R) = (x_P, y_P) \oplus (x_Q, y_Q)$ where (x_P, y_P) and (x_Q, y_Q) are affine representation of points $P, Q \in E(\overline{\mathbb{F}}_p)$?

Algorithm 1: Classical adding P and Q for $x_P \neq x_Q$

1. Calculate the slope $\lambda \leftarrow (y_P - y_Q)/(x_P - x_Q)$.
2. Set
$$x_R \leftarrow \lambda^2 - x_P - x_Q, \quad y_R \leftarrow \lambda(x_P - x_R) - y_P.$$

Easy, right? What can go wrong?

Why this is bad?

Let

- **M** — cost of multiplication;
- **S** — cost of squaring;
- **I** — cost of inverse.

(all in some extension $\mathbb{F}_{p^m}$)

Why this is bad?

Let

- $\mathbf{M}$ — cost of multiplication;
- $\mathbf{S}$ — cost of squaring;
- $\mathbf{I}$ — cost of inverse.

(all in some extension $\mathbb{F}_{p^m}$)

Algorithm 1: Calculating $P \oplus Q$

$$\lambda \leftarrow (y_P - y_Q) \times (x_P - x_Q)^{-1}$$
$$x_R \leftarrow \lambda^2 - x_P - x_Q$$
$$y_R \leftarrow \lambda \times (x_P - x_R) - y_P$$

Then, calculating the aforementioned formula costs:

$$2\mathbf{M} + \mathbf{S} + \mathbf{I}$$

Well, just 4 operations... Easy right?

Why this is bad?

Let

- **M** — cost of multiplication;
- **S** — cost of squaring;
- **I** — cost of inverse.

(all in some extension $\mathbb{F}_{p^m}$)

Algorithm 1: Calculating $P \oplus Q$

$$\lambda \leftarrow (y_P - y_Q) \times (x_P - x_Q)^{-1}$$
$$x_R \leftarrow \lambda^2 - x_P - x_Q$$
$$y_R \leftarrow \lambda \times (x_P - x_R) - y_P$$

Then, calculating the aforementioned formula costs:

$$2\mathbf{M} + \mathbf{S} + \mathbf{I}$$

Well, just 4 operations... Easy right?

Main Problem!

Typically, $\mathbf{I} \approx 80\mathbf{M}$. So, the effective cost is roughly **80 operations**. Too bad. We need to fix it!

Relations

Relation

Our solution would be **projective coordinates**, but we need a couple of ingredients first.

Definition

Let $\mathcal{X}, \mathcal{Y}$ be some sets. Then, $\mathcal{R}$ is a **relation** if

$$\mathcal{R} \subset \mathcal{X} \times \mathcal{Y} = \{(x, y) : x \in \mathcal{X}, y \in \mathcal{Y}\}$$

Relation

Our solution would be **projective coordinates**, but we need a couple of ingredients first.

Definition

Let $\mathcal{X}, \mathcal{Y}$ be some sets. Then, $\mathcal{R}$ is a **relation** if

$$\mathcal{R} \subset \mathcal{X} \times \mathcal{Y} = \{(x, y) : x \in \mathcal{X}, y \in \mathcal{Y}\}$$

Example

Let $\mathcal{X} = \{\text{Oleksandr}, \text{Phat}, \text{Anton}\}$, $\mathcal{Y} = \{\text{Backend}, \text{Frontend}, \text{Research}\}$. Define the following relation of "person x works in field y":

Relation

Our solution would be **projective coordinates**, but we need a couple of ingredients first.

Definition

Let $\mathcal{X}, \mathcal{Y}$ be some sets. Then, $\mathcal{R}$ is a **relation** if

$$\mathcal{R} \subset \mathcal{X} \times \mathcal{Y} = \{(x, y) : x \in \mathcal{X}, y \in \mathcal{Y}\}$$

Example

Let $\mathcal{X} = \{\text{Oleksandr}, \text{Phat}, \text{Anton}\}$, $\mathcal{Y} = \{\text{Backend}, \text{Frontend}, \text{Research}\}$. Define the following relation of "person x works in field y":

$$\mathcal{R} = \{(\text{Oleksandr}, \text{Research}), (\text{Phat}, \text{Frontend}), (\text{Anton}, \text{Backend})\}$$

Obviously, $\mathcal{R} \subset \mathcal{X} \times \mathcal{Y}$, so $\mathcal{R}$ is a relation.

Equivalence Relation

Definition

Let $\mathcal{X}$ be a set. A relation $\sim$ on $\mathcal{X}$ is called an **equivalence relation** if it satisfies the following properties:

1. **Reflexivity:** $x \sim x$ for all $x \in \mathcal{X}$.

Equivalence Relation

Definition

Let $\mathcal{X}$ be a set. A relation $\sim$ on $\mathcal{X}$ is called an **equivalence relation** if it satisfies the following properties:

1. **Reflexivity:** $x \sim x$ for all $x \in \mathcal{X}$.
2. **Symmetry:** If $x \sim y$, then $y \sim x$ for all $x, y \in \mathcal{X}$.

Equivalence Relation

Definition

Let $\mathcal{X}$ be a set. A relation $\sim$ on $\mathcal{X}$ is called an **equivalence relation** if it satisfies the following properties:

1. **Reflexivity:** $x \sim x$ for all $x \in \mathcal{X}$.
2. **Symmetry:** If $x \sim y$, then $y \sim x$ for all $x, y \in \mathcal{X}$.
3. **Transitivity:** If $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in \mathcal{X}$.

Equivalence Relation

Definition

Let $\mathcal{X}$ be a set. A relation $\sim$ on $\mathcal{X}$ is called an **equivalence relation** if it satisfies the following properties:

1. **Reflexivity:** $x \sim x$ for all $x \in \mathcal{X}$.
2. **Symmetry:** If $x \sim y$, then $y \sim x$ for all $x, y \in \mathcal{X}$.
3. **Transitivity:** If $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in \mathcal{X}$.

Example

Let $\mathcal{X}$ be the set of all people. Define a relation $\sim$ on $\mathcal{X}$ by $x \sim y$ if $x, y \in \mathcal{X}$ have the same birthday. Then $\sim$ is an equivalence relation on $\mathcal{X}$.

1. **Reflexivity:** $x \sim x$ since x has the same birthday as x.

Equivalence Relation

Definition

Let $\mathcal{X}$ be a set. A relation $\sim$ on $\mathcal{X}$ is called an **equivalence relation** if it satisfies the following properties:

1. **Reflexivity:** $x \sim x$ for all $x \in \mathcal{X}$.
2. **Symmetry:** If $x \sim y$, then $y \sim x$ for all $x, y \in \mathcal{X}$.
3. **Transitivity:** If $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in \mathcal{X}$.

Example

Let $\mathcal{X}$ be the set of all people. Define a relation $\sim$ on $\mathcal{X}$ by $x \sim y$ if $x, y \in \mathcal{X}$ have the same birthday. Then $\sim$ is an equivalence relation on $\mathcal{X}$.

1. **Reflexivity:** $x \sim x$ since x has the same birthday as x.
2. **Symmetry:** If $x \sim y$, then $y \sim x$ since x has the same birthday as y.

Equivalence Relation

Definition

Let $\mathcal{X}$ be a set. A relation $\sim$ on $\mathcal{X}$ is called an **equivalence relation** if it satisfies the following properties:

1. **Reflexivity:** $x \sim x$ for all $x \in \mathcal{X}$.
2. **Symmetry:** If $x \sim y$, then $y \sim x$ for all $x, y \in \mathcal{X}$.
3. **Transitivity:** If $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in \mathcal{X}$.

Example

Let $\mathcal{X}$ be the set of all people. Define a relation $\sim$ on $\mathcal{X}$ by $x \sim y$ if $x, y \in \mathcal{X}$ have the same birthday. Then $\sim$ is an equivalence relation on $\mathcal{X}$.

1. **Reflexivity:** $x \sim x$ since x has the same birthday as x.
2. **Symmetry:** If $x \sim y$, then $y \sim x$ since x has the same birthday as y.
3. **Transitivity:** If $x \sim y$ and $y \sim z$, then $x \sim z$.

Equivalence Relation: More Examples

Example

Suppose $\mathcal{X} = \mathbb{Z}$ and n is some fixed integer. Let $a \sim b$ mean that $a \equiv b \pmod{n}$. It is easy to verify that $\sim$ is an equivalence relation:

1. **Reflexivity:** $a \equiv a \pmod{n}$, so $a \sim a$.

Equivalence Relation: More Examples

Example

Suppose $\mathcal{X} = \mathbb{Z}$ and n is some fixed integer. Let $a \sim b$ mean that $a \equiv b \pmod{n}$. It is easy to verify that $\sim$ is an equivalence relation:

1. **Reflexivity:** $a \equiv a \pmod{n}$, so $a \sim a$.
2. **Symmetry:** If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$, so $b \sim a$.

Equivalence Relation: More Examples

Example

Suppose $\mathcal{X} = \mathbb{Z}$ and n is some fixed integer. Let $a \sim b$ mean that $a \equiv b \pmod{n}$. It is easy to verify that $\sim$ is an equivalence relation:

1. **Reflexivity:** $a \equiv a \pmod{n}$, so $a \sim a$.
2. **Symmetry:** If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$, so $b \sim a$.
3. **Transitivity:** If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$, so $(a \sim b) \wedge (b \sim c) \implies a \sim c$.

Equivalence Relation: More Examples

Example

Suppose $\mathcal{X} = \mathbb{Z}$ and n is some fixed integer. Let $a \sim b$ mean that $a \equiv b \pmod{n}$. It is easy to verify that $\sim$ is an equivalence relation:

1. **Reflexivity:** $a \equiv a \pmod{n}$, so $a \sim a$.
2. **Symmetry:** If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$, so $b \sim a$.
3. **Transitivity:** If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$, so $(a \sim b) \wedge (b \sim c) \implies a \sim c$.

Example

Isomorphism $\cong$ is an equivalence relation on the set of all groups.

Equivalence Relation: More Examples

Example

Suppose $\mathcal{X} = \mathbb{Z}$ and n is some fixed integer. Let $a \sim b$ mean that $a \equiv b \pmod{n}$. It is easy to verify that $\sim$ is an equivalence relation:

1. **Reflexivity:** $a \equiv a \pmod{n}$, so $a \sim a$.
2. **Symmetry:** If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$, so $b \sim a$.
3. **Transitivity:** If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$, so $(a \sim b) \wedge (b \sim c) \implies a \sim c$.

Example

Isomorphism $\cong$ is an equivalence relation on the set of all groups.

Question

For $\mathbb{R}$ define $a \sim b$ iff $a \geq b$. Is it an equivalence relation?

Equivalence Classes

Notice that for the set of integers $\mathbb{Z}$ and relation $\sim$ defined by $a \sim b$ iff $a \equiv b \pmod{n}$, we can group all integers into equivalence classes. For example, for $n = 2$:

$$\mathbb{Z} = \{a \in \mathbb{Z} : a \text{ is even}\} \cup \{a \in \mathbb{Z} : a \text{ is odd}\}$$

Can we generalize this observation for general relations?

Equivalence Classes

Notice that for the set of integers $\mathbb{Z}$ and relation $\sim$ defined by $a \sim b$ iff $a \equiv b \pmod{n}$, we can group all integers into equivalence classes. For example, for $n = 2$:

$$\mathbb{Z} = \{a \in \mathbb{Z} : a \text{ is even}\} \cup \{a \in \mathbb{Z} : a \text{ is odd}\}$$

Can we generalize this observation for general relations?

Definition

Let $\mathcal{X}$ be a set and $\sim$ be an equivalence relation on $\mathcal{X}$. For any $x \in \mathcal{X}$, the **equivalence class** of x is the set

$$[x] = \{y \in \mathcal{X} : x \sim y\}$$

Equivalence Classes

Notice that for the set of integers $\mathbb{Z}$ and relation $\sim$ defined by $a \sim b$ iff $a \equiv b \pmod{n}$, we can group all integers into equivalence classes. For example, for $n = 2$:

$$\mathbb{Z} = \{a \in \mathbb{Z} : a \text{ is even}\} \cup \{a \in \mathbb{Z} : a \text{ is odd}\}$$

Can we generalize this observation for general relations?

Definition

Let $\mathcal{X}$ be a set and $\sim$ be an equivalence relation on $\mathcal{X}$. For any $x \in \mathcal{X}$, the **equivalence class** of x is the set

$$[x] = \{y \in \mathcal{X} : x \sim y\}$$

The **set of all equivalence classes** is denoted by $\mathcal{X}/\sim$ (or, if the relation $\mathcal{R}$ is given explicitly, then $\mathcal{X}/\mathcal{R}$), which is read as "$\mathcal{X}$ modulo relation $\sim$".

Equivalence Classes Properties

Example

Let $\mathcal{X} = \mathbb{Z}$ and n be some fixed integer. Define $\sim$ on $\mathcal{X}$ by $x \sim y$ if $x \equiv y \pmod{n}$. Then the equivalence class of x is the set

$$[x] = \{y \in \mathbb{Z} : x \equiv y \pmod{n}\}$$

For example, $[0] = \{\dots, -2n, -n, 0, n, 2n, \dots\}$ while $[1] = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$.

Equivalence Classes Properties

Example

Let $\mathcal{X} = \mathbb{Z}$ and n be some fixed integer. Define $\sim$ on $\mathcal{X}$ by $x \sim y$ if $x \equiv y \pmod{n}$. Then the equivalence class of x is the set

$$[x] = \{y \in \mathbb{Z} : x \equiv y \pmod{n}\}$$

For example, $[0] = \{\dots, -2n, -n, 0, n, 2n, \dots\}$ while $[1] = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$.

Lemma

Let $\mathcal{X}$ be a set and $\sim$ be an equivalence relation on $\mathcal{X}$. Then,

1. *For each $x \in \mathcal{X}, x \in [x]$ (quite obvious, follows from reflexivity).*

Equivalence Classes Properties

Example

Let $\mathcal{X} = \mathbb{Z}$ and n be some fixed integer. Define $\sim$ on $\mathcal{X}$ by $x \sim y$ if $x \equiv y \pmod{n}$. Then the equivalence class of x is the set

$$[x] = \{y \in \mathbb{Z} : x \equiv y \pmod{n}\}$$

For example, $[0] = \{\dots, -2n, -n, 0, n, 2n, \dots\}$ while $[1] = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$.

Lemma

Let $\mathcal{X}$ be a set and $\sim$ be an equivalence relation on $\mathcal{X}$. Then,

1. *For each $x \in \mathcal{X}, x \in [x]$ (quite obvious, follows from reflexivity).*
2. *For each $x, y \in \mathcal{X}$, $x \sim y$ if and only if $[x] = [y]$.*

Equivalence Classes Properties

Example

Let $\mathcal{X} = \mathbb{Z}$ and n be some fixed integer. Define $\sim$ on $\mathcal{X}$ by $x \sim y$ if $x \equiv y \pmod{n}$. Then the equivalence class of x is the set

$$[x] = \{y \in \mathbb{Z} : x \equiv y \pmod{n}\}$$

For example, $[0] = \{\dots, -2n, -n, 0, n, 2n, \dots\}$ while $[1] = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$.

Lemma

Let $\mathcal{X}$ be a set and $\sim$ be an equivalence relation on $\mathcal{X}$. Then,

1. *For each $x \in \mathcal{X}, x \in [x]$ (quite obvious, follows from reflexivity).*
2. *For each $x, y \in \mathcal{X}$, $x \sim y$ if and only if $[x] = [y]$.*
3. *For each $x, y \in \mathcal{X}$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.*

Equivalence Classes Partition Example

Example

Let $n \in \mathbb{N}$ and, again, $\mathcal{X} = \mathbb{Z}$ with a "modulo n" equivalence relation $\mathcal{R}_n$. Define the equivalence class of x by $[x]_n = \{y \in \mathbb{Z} : x \equiv y \pmod{n}\}$. Then,

$$\mathbb{Z}/\mathcal{R}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-2]_n, [n-1]_n\}$$

Elliptic Curve in Projective Coordinates

Definition

Definition

Projective coordinate, denoted as $\mathbb{P}^2(\mathbb{K})$ (or sometimes simply $\mathbb{K}\mathbb{P}^2$) is a set of triplets of elements $(X : Y : Z)$ from $\mathbb{A}^3(\overline{\mathbb{K}}) \setminus \{0\}$ modulo the equivalence relation:

$$(X_1 : Y_1 : Z_1) \sim (X_2 : Y_2 : Z_2) \text{ iff}$$
$$\exists \lambda \in \overline{\mathbb{K}}^\times : (X_1 : Y_1 : Z_1) = (\lambda X_2 : \lambda Y_2 : \lambda Z_2)$$

Definition

Definition

Projective coordinate, denoted as $\mathbb{P}^2(\mathbb{K})$ (or sometimes simply $\mathbb{KP}^2$) is a set of triplets of elements $(X : Y : Z)$ from $\mathbb{A}^3(\overline{\mathbb{K}}) \setminus \{0\}$ modulo the equivalence relation:

$$(X_1 : Y_1 : Z_1) \sim (X_2 : Y_2 : Z_2) \text{ iff}$$
$$\exists \lambda \in \overline{\mathbb{K}}^{\times} : (X_1 : Y_1 : Z_1) = (\lambda X_2 : \lambda Y_2 : \lambda Z_2)$$

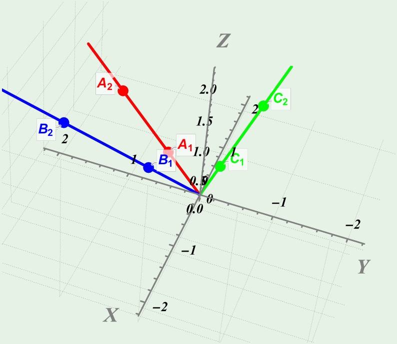
Example

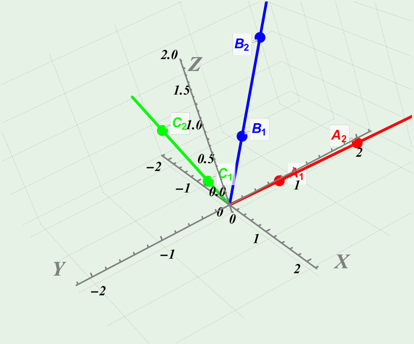
Consider the projective space $\mathbb{P}^2(\mathbb{R})$. Then, two points $(x_1, y_1, z_1), (x_2, y_2, z_2) \in \mathbb{R}^3$ are equivalent if there exists $\lambda \in \mathbb{R} \setminus \{0\}$ such that $(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$. For example, $(1, 2, 3) \sim (2, 4, 6)$ since $(1, 2, 3) = (0.5 \times 2, 0.5 \times 4, 0.5 \times 6)$, so $\lambda = 0.5$.

Illustration

Example

Now, how to geometrically interpret $\mathbb{P}^2(\mathbb{R})$? Consider the Figure below.





Equivalent points lie on the same line through the origin $(0, 0, 0)$.

Questions

Question #1

Are points $(1, 2, 3)$ and $(3, 6, 9)$ equivalent in $\mathbb{P}^2(\mathbb{R})$?

Questions

Question #1

Are points $(1, 2, 3)$ and $(3, 6, 9)$ equivalent in $\mathbb{P}^2(\mathbb{R})$?

Question #2

Are points $(1, 2, 3)$ and $(2, 3, 1)$ equivalent in $\mathbb{P}^2(\mathbb{R})$?

Questions

Question #1

Are points $(1, 2, 3)$ and $(3, 6, 9)$ equivalent in $\mathbb{P}^2(\mathbb{R})$?

Question #2

Are points $(1, 2, 3)$ and $(2, 3, 1)$ equivalent in $\mathbb{P}^2(\mathbb{R})$?

Question #3

Are points $(2, 4, 6)$ and $(3, 6, 9)$ equivalent in $\mathbb{P}^2(\mathbb{R})$?

Going back to Affine Space

Observation #1

Define the map $\phi : \mathbb{P}^2(\mathbb{K}) \to \mathbb{A}^2(\mathbb{K})$ as $\phi(X : Y : Z) = (X/Z, Y/Z)$ for $(X : Y : Z) \in \mathbb{P}^2(\mathbb{K})$. This map will map all equivalent points (lying on the same line) to the same point in $\mathbb{A}^2(\mathbb{K})$.

Going back to Affine Space

Observation #1

Define the map $\phi : \mathbb{P}^2(\mathbb{K}) \to \mathbb{A}^2(\mathbb{K})$ as $\phi(X : Y : Z) = (X/Z, Y/Z)$ for $(X : Y : Z) \in \mathbb{P}^2(\mathbb{K})$. This map will map all equivalent points (lying on the same line) to the same point in $\mathbb{A}^2(\mathbb{K})$.

Observation #2

Define the map $\psi : \mathbb{A}^2(\mathbb{K}) \to \mathbb{P}^2(\mathbb{K})$ as $\psi(x, y) = (x : y : 1)$. This map will map all points in $\mathbb{A}^2(\mathbb{K})$ to the corresponding equivalence class in $\mathbb{P}^2(\mathbb{K})$.

Going back to Affine Space

Observation #1

Define the map $\phi : \mathbb{P}^2(\mathbb{K}) \to \mathbb{A}^2(\mathbb{K})$ as $\phi(X : Y : Z) = (X/Z, Y/Z)$ for $(X : Y : Z) \in \mathbb{P}^2(\mathbb{K})$. This map will map all equivalent points (lying on the same line) to the same point in $\mathbb{A}^2(\mathbb{K})$.

Observation #2

Define the map $\psi : \mathbb{A}^2(\mathbb{K}) \to \mathbb{P}^2(\mathbb{K})$ as $\psi(x, y) = (x : y : 1)$. This map will map all points in $\mathbb{A}^2(\mathbb{K})$ to the corresponding equivalence class in $\mathbb{P}^2(\mathbb{K})$.

Question

Given point $(2 : 4 : 2) \in \mathbb{P}^2(\mathbb{R})$, what is the corresponding point in $\mathbb{A}^2(\mathbb{R})$?

Going back to Affine Space: Illustration

Example

Again, consider three lines from the previous example. Now, we additionally draw a plane $\pi : z = 1$ in our 3-dimensional space (see Illustration below).

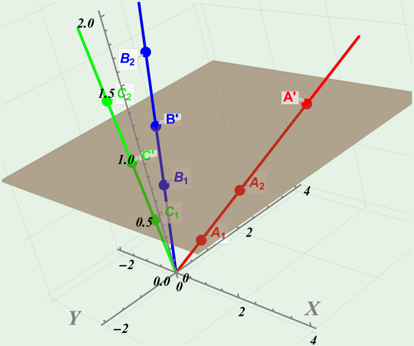


Illustration: Geometric interpretation of converting projective form to the affine form.

Equation over Projective Space

Observation

If $(X : Y : Z)$ lies on the curve, then so does $(X/Z, Y/Z)$.

Equation over Projective Space

Observation

If $(X : Y : Z)$ lies on the curve, then so does $(X/Z, Y/Z)$. Thus, since $y^2 = x^3 + ax + b$ we have:

$$\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 + a\left(\frac{X}{Z}\right) + b$$

Equation over Projective Space

Observation

If $(X : Y : Z)$ lies on the curve, then so does $(X/Z, Y/Z)$. Thus, since $y^2 = x^3 + ax + b$ we have:

$$\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 + a\left(\frac{X}{Z}\right) + b$$

Definition

The **homogeneous projective form** of the elliptic curve is given by the equation:

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where the point at infinity is encoded as $\mathcal{O} = (0 : 1 : 0)$.

Equation over Projective Space

Observation

If $(X : Y : Z)$ lies on the curve, then so does $(X/Z, Y/Z)$. Thus, since $y^2 = x^3 + ax + b$ we have:

$$\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 + a\left(\frac{X}{Z}\right) + b$$

Definition

The **homogeneous projective form** of the elliptic curve is given by the equation:

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where the point at infinity is encoded as $\mathcal{O} = (0 : 1 : 0)$.

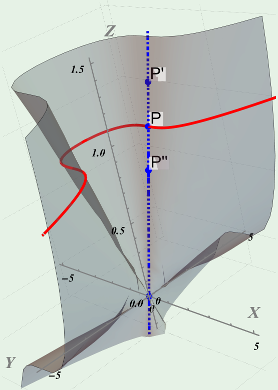
Remark

Why $\mathcal{O} = (0 : 1 : 0)$. Note that all $(0 : \lambda : 0)$ lie on the Elliptic Curve.

Visualization over Projective Space

Example

Consider the BN254 curve $y^2 = x^3 + 3$ over reals $\mathbb{R}$. Its projective form is given by the equation $Y^2 Z = X^3 + 3Z^3$, giving a surface below.



Advantage of Projective Form.

Rhetorical Question

Why having three coordinates instead of two is better?

Consider the **addition** operation:

Advantage of Projective Form.

Rhetorical Question

Why having three coordinates instead of two is better?

Consider the **addition** operation:

$$\begin{aligned}
X_R = (X_P Z_Q - X_Q Z_P)(Z_P Z_Q (Y_P Z_Q - Y_Q Z_P)^2 \\
-(X_P Z_Q - X_Q Z_P)^2 (X_P Z_Q + X_Q Z_P)); \\
Y_R = Z_P Z_Q (X_Q Y_P - X_P Y_Q)(X_P Z_Q - X_Q Z_P)^2 \\
-(Y_P Z_Q - Y_Q Z_P)((Y_P Z_Q - Y_Q Z_P)^2 Z_P Z_Q \\
-(X_P Z_Q + X_Q Z_P)(X_P Z_Q - X_Q Z_P)^2); \\
Z_R = Z_P Z_Q (X_P Z_Q - X_Q Z_P)^3.
\end{aligned}$$

Advantage of Projective Form.

Rhetorical Question

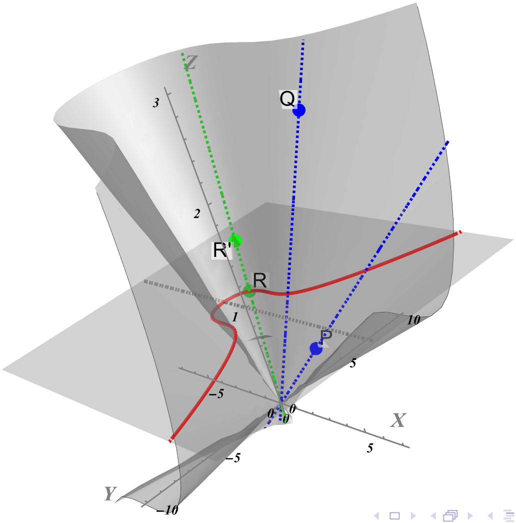
Why having three coordinates instead of two is better?

Consider the **addition** operation:

$$
\begin{aligned}
X_R = (X_P Z_Q - X_Q Z_P)(Z_P Z_Q (Y_P Z_Q - Y_Q Z_P)^2 \\
-(X_P Z_Q - X_Q Z_P)^2 (X_P Z_Q + X_Q Z_P)); \\
Y_R = Z_P Z_Q (X_Q Y_P - X_P Y_Q)(X_P Z_Q - X_Q Z_P)^2 \\
-(Y_P Z_Q - Y_Q Z_P)((Y_P Z_Q - Y_Q Z_P)^2 Z_P Z_Q \\
-(X_P Z_Q + X_Q Z_P)(X_P Z_Q - X_Q Z_P)^2); \\
Z_R = Z_P Z_Q (X_P Z_Q - X_Q Z_P)^3.
\end{aligned}
$$

Although looks much more complicated, it takes only **14M** compared to **80M**.

Illustration of adding two points



General Strategy

1. Convert affine form (X_P, Y_P) to the projective $(X_P : Y_P : 1)$.

General Strategy

1. Convert affine form (X_P, Y_P) to the projective $(X_P : Y_P : 1)$.
2. Make many additions, doubling, multiplications etc. in projective form, getting $(X_R : Y_R : Z_R)$ at the end.

General Strategy

1. Convert affine form (X_P, Y_P) to the projective $(X_P : Y_P : 1)$.
2. Make many additions, doubling, multiplications etc. in projective form, getting $(X_R : Y_R : Z_R)$ at the end.
3. Convert back to affine coordinates:

$$(X_R : Y_R : Z_R) \mapsto (X_R/Z_R, Y_R/Z_R)$$

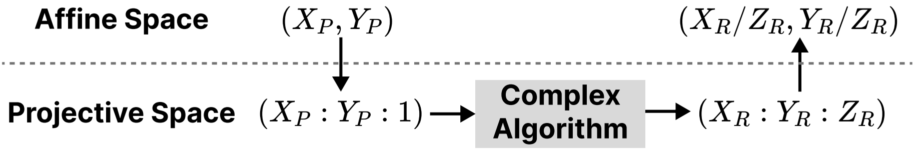


Figure: General strategy with EC operations.

General Projective Coordinates

$$(X : Y : Z) \sim (X' : Y' : Z') \text{ iff}$$
$$\exists \lambda \in \overline{\mathbb{K}} : (X, Y, Z) = (\lambda^n X', \lambda^m Y', \lambda Z')$$

General Projective Coordinates

$$(X : Y : Z) \sim (X' : Y' : Z') \text{ iff}$$
$$\exists \lambda \in \overline{\mathbb{K}} : (X, Y, Z) = (\lambda^n X', \lambda^m Y', \lambda Z')$$

In this case, to come back to the affine form, we need to use the map $\phi : (X : Y : Z) \mapsto (X/Z^n, Y/Z^m)$.

General Projective Coordinates

$$(X : Y : Z) \sim (X' : Y' : Z') \text{ iff}$$
$$\exists \lambda \in \overline{\mathbb{K}} : (X, Y, Z) = (\lambda^n X', \lambda^m Y', \lambda Z')$$

In this case, to come back to the affine form, we need to use the map $\phi : (X : Y : Z) \mapsto (X/Z^n, Y/Z^m)$.

Example

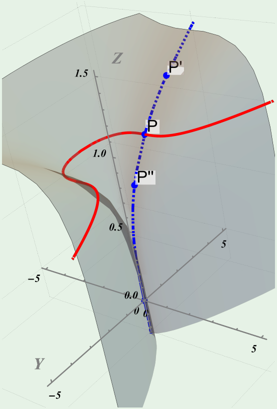
The case $n = 2, m = 3$ is called the **Jacobian Projective Coordinates**. An Elliptic Curve equation might be then rewritten as:

$$Y^2 = X^3 + aXZ^4 + bZ^6$$

Illustration of General Projective Coordinates

Example

Consider the BN254 curve $y^2 = x^3 + 3$ over reals $\mathbb{R}$, again. Its *Jacobian projective form* is given by $Y^2 = X^3 + 3Z^6$.



Pairings

Definition

Definition

Pairing is a bilinear, non-degenerate, efficiently computable map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where $\mathbb{G}_1, \mathbb{G}_2$ are two groups (typically, elliptic curve groups) and $\mathbb{G}_T$ is a target group (typically, a set of scalars). Let us decipher the definition:

- **Bilinearity** means essentially the following:

$$e([a]P, [b]Q) = e([ab]P, Q) = e(P, [ab]Q) = e(P, Q)^{ab}.$$

Definition

Definition

Pairing is a bilinear, non-degenerate, efficiently computable map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where $\mathbb{G}_1, \mathbb{G}_2$ are two groups (typically, elliptic curve groups) and $\mathbb{G}_T$ is a target group (typically, a set of scalars). Let us decipher the definition:

- **Bilinearity** means essentially the following:

$$e([a]P, [b]Q) = e([ab]P, Q) = e(P, [ab]Q) = e(P, Q)^{ab}.$$

- **Non-degeneracy** means that $e(G_1, G_2) \neq 1$ (where G_1, G_2 are generators of $\mathbb{G}_1, \mathbb{G}_2$, respectively). This property basically says that the pairing is not trivial.

Definition

Definition

Pairing is a bilinear, non-degenerate, efficiently computable map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where $\mathbb{G}_1, \mathbb{G}_2$ are two groups (typically, elliptic curve groups) and $\mathbb{G}_T$ is a target group (typically, a set of scalars). Let us decipher the definition:

- **Bilinearity** means essentially the following:

$$e([a]P, [b]Q) = e([ab]P, Q) = e(P, [ab]Q) = e(P, Q)^{ab}.$$

- **Non-degeneracy** means that $e(G_1, G_2) \neq 1$ (where G_1, G_2 are generators of $\mathbb{G}_1, \mathbb{G}_2$, respectively). This property basically says that the pairing is not trivial.
- **Efficient computability** means that the pairing can be computed in a reasonable time.

Primitive Example

Example

Suppose $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}_T = \mathbb{Z}_r$ are scalars. Then, the following map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a pairing:

$$e(x, y) = 2^{xy}$$

Primitive Example

Example

Suppose $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}_T = \mathbb{Z}_r$ are scalars. Then, the following map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a pairing:

$$e(x, y) = 2^{xy}$$

- **Bilinearity:**

$$e(ax, by) = 2^{abxy} = (2^{xy})^{ab} = e(x, y)^{ab}$$
$$e(ax, by) = 2^{abxy} = 2^{(x)(aby)} = e(x, aby)$$

Primitive Example

Example

Suppose $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}_T = \mathbb{Z}_r$ are scalars. Then, the following map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a pairing:

$$e(x, y) = 2^{xy}$$

- **Bilinearity:**

$$e(ax, by) = 2^{abxy} = (2^{xy})^{ab} = e(x, y)^{ab}$$
$$e(ax, by) = 2^{abxy} = 2^{(x)(aby)} = e(x, aby)$$

- **Non-degeneracy:** $e(1, 1) = 2 \neq 1$.

Primitive Example

Example

Suppose $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}_T = \mathbb{Z}_r$ are scalars. Then, the following map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a pairing:

$$e(x, y) = 2^{xy}$$

- **Bilinearity:**

$$e(ax, by) = 2^{abxy} = (2^{xy})^{ab} = e(x, y)^{ab}$$
$$e(ax, by) = 2^{abxy} = 2^{(x)(aby)} = e(x, aby)$$

- **Non-degeneracy:** $e(1, 1) = 2 \neq 1$.
- **Efficient computability:** Obvious.

Elliptic Curve-based Pairing

Example

Pairing for BN254. For BN254 (with equation $y^2 = x^3 + 3$), the pairing function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is defined over the following groups:

Elliptic Curve-based Pairing

Example

Pairing for BN254. For BN254 (with equation $y^2 = x^3 + 3$), the pairing function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is defined over the following groups:

- $\mathbb{G}_1$ — points on the regular curve $E(\mathbb{F}_p)$.

Elliptic Curve-based Pairing

Example

Pairing for BN254. For BN254 (with equation $y^2 = x^3 + 3$), the pairing function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is defined over the following groups:

- $\mathbb{G}_1$ — points on the regular curve $E(\mathbb{F}_p)$.
- $\mathbb{G}_2$ — r-torsion points on the twisted curve $E'(\mathbb{F}_{p^2})$ over the field extension $\mathbb{F}_{p^2}$ (with equation $y^2 = x^3 + \frac{3}{\xi}$ for $\xi = 9 + u \in \mathbb{F}_{p^2}$).

Elliptic Curve-based Pairing

Example

Pairing for BN254. For BN254 (with equation $y^2 = x^3 + 3$), the pairing function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is defined over the following groups:

- $\mathbb{G}_1$ — points on the regular curve $E(\mathbb{F}_p)$.
- $\mathbb{G}_2$ — r-torsion points on the twisted curve $E'(\mathbb{F}_{p^2})$ over the field extension $\mathbb{F}_{p^2}$ (with equation $y^2 = x^3 + \frac{3}{\xi}$ for $\xi = 9 + u \in \mathbb{F}_{p^2}$).
- $\mathbb{G}_T$ — rth roots of unity $\Omega_r \subset \mathbb{F}_{p^{12}}^{\times}$.

Elliptic Curve-based Pairing

Example

Pairing for BN254. For BN254 (with equation $y^2 = x^3 + 3$), the pairing function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is defined over the following groups:

- $\mathbb{G}_1$ — points on the regular curve $E(\mathbb{F}_p)$.
- $\mathbb{G}_2$ — r-torsion points on the twisted curve $E'(\mathbb{F}_{p^2})$ over the field extension $\mathbb{F}_{p^2}$ (with equation $y^2 = x^3 + \frac{3}{\xi}$ for $\xi = 9 + u \in \mathbb{F}_{p^2}$).
- $\mathbb{G}_T$ — rth roots of unity $\Omega_r \subset \mathbb{F}_{p^{12}}^{\times}$.

Some clarifications:

- ***r*-torsion subgroup**: $E(\mathbb{F}_{p^m})[r] = \{P \in E(\mathbb{F}_{p^m}) : [r]P = \mathcal{O}\}$.

Elliptic Curve-based Pairing

Example

Pairing for BN254. For BN254 (with equation $y^2 = x^3 + 3$), the pairing function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is defined over the following groups:

- $\mathbb{G}_1$ — points on the regular curve $E(\mathbb{F}_p)$.
- $\mathbb{G}_2$ — r-torsion points on the twisted curve $E'(\mathbb{F}_{p^2})$ over the field extension $\mathbb{F}_{p^2}$ (with equation $y^2 = x^3 + \frac{3}{\xi}$ for $\xi = 9 + u \in \mathbb{F}_{p^2}$).
- $\mathbb{G}_T$ — rth roots of unity $\Omega_r \subset \mathbb{F}_{p^{12}}^{\times}$.

Some clarifications:

- ***r*-torsion subgroup**: $E(\mathbb{F}_{p^m})[r] = \{P \in E(\mathbb{F}_{p^m}) : [r]P = \mathcal{O}\}$.
- ***r*th roots of unity**: $\Omega_r = \{z \in \mathbb{F}_{p^{12}}^{\times} : z^r = 1\}$.

Elliptic Curve-based Pairing

Example

Pairing for BN254. For BN254 (with equation $y^2 = x^3 + 3$), the pairing function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is defined over the following groups:

- $\mathbb{G}_1$ — points on the regular curve $E(\mathbb{F}_p)$.
- $\mathbb{G}_2$ — r-torsion points on the twisted curve $E'(\mathbb{F}_{p^2})$ over the field extension $\mathbb{F}_{p^2}$ (with equation $y^2 = x^3 + \frac{3}{\xi}$ for $\xi = 9 + u \in \mathbb{F}_{p^2}$).
- $\mathbb{G}_T$ — rth roots of unity $\Omega_r \subset \mathbb{F}_{p^{12}}^{\times}$.

Some clarifications:

- ***r*-torsion subgroup**: $E(\mathbb{F}_{p^m})[r] = \{P \in E(\mathbb{F}_{p^m}) : [r]P = \mathcal{O}\}$.
- ***r*th roots of unity**: $\Omega_r = \{z \in \mathbb{F}_{p^{12}}^{\times} : z^r = 1\}$.

Question

If $E(\mathbb{F}_p)$ is cyclic, $r = |E(\mathbb{F}_p)|$, what is $E(\mathbb{F}_p)[r]$?

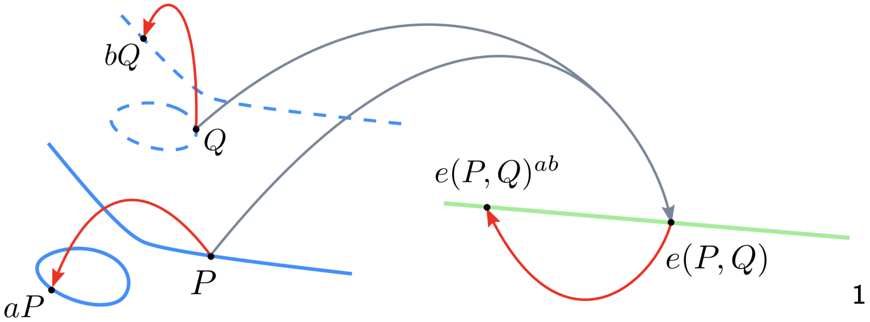


Figure: Pairing illustration. It does not matter what we do first: (a) compute $[a]P$ and $[b]Q$ and then compute $e([a]P, [b]Q)$ or (b) first calculate $e(P, Q)$ and then transform it to $e(P, Q)^{ab}$.

Pairing-friendliness

Remark

One might have a reasonable question: where does this 12 come from? The answer is following: the so-called **embedding degree** of BN254 curve is $k = 12$.

Pairing-friendliness

Remark

One might have a reasonable question: where does this 12 come from? The answer is following: the so-called **embedding degree** of BN254 curve is $k = 12$.

Definition

The following conditions are equivalent **definitions** of an embedding degree k of an elliptic curve $E(\overline{\mathbb{F}}_p)$:

Pairing-friendliness

Remark

One might have a reasonable question: where does this 12 come from? The answer is following: the so-called **embedding degree** of BN254 curve is $k = 12$.

Definition

The following conditions are equivalent **definitions** of an embedding degree k of an elliptic curve $E(\overline{\mathbb{F}}_p)$:

- k is the smallest positive integer such that $r \mid (p^k - 1)$.

Pairing-friendliness

Remark

One might have a reasonable question: where does this 12 come from? The answer is following: the so-called **embedding degree** of BN254 curve is $k = 12$.

Definition

The following conditions are equivalent **definitions** of an embedding degree k of an elliptic curve $E(\overline{\mathbb{F}}_p)$:

- k is the smallest positive integer such that $r \mid (p^k - 1)$.
- k is the smallest positive integer such that $\mathbb{F}_{p^k}$ contains all of the r-th roots of unity in $\overline{\mathbb{F}}_p$, that is $\Omega_r \subset \mathbb{F}_{p^k}$.

Pairing-friendliness

Remark

One might have a reasonable question: where does this 12 come from? The answer is following: the so-called **embedding degree** of BN254 curve is $k = 12$.

Definition

The following conditions are equivalent **definitions** of an embedding degree k of an elliptic curve $E(\overline{\mathbb{F}}_p)$:

- k is the smallest positive integer such that $r \mid (p^k - 1)$.
- k is the smallest positive integer such that $\mathbb{F}_{p^k}$ contains all of the r-th roots of unity in $\overline{\mathbb{F}}_p$, that is $\Omega_r \subset \mathbb{F}_{p^k}$.
- k is the smallest positive integer such that $E(\overline{\mathbb{F}}_p)[r] \subset E(\mathbb{F}_{p^k})$

Pairing-friendliness

Remark

One might have a reasonable question: where does this 12 come from? The answer is following: the so-called **embedding degree** of BN254 curve is $k = 12$.

Definition

The following conditions are equivalent **definitions** of an embedding degree k of an elliptic curve $E(\overline{\mathbb{F}}_p)$:

- k is the smallest positive integer such that $r \mid (p^k - 1)$.
- k is the smallest positive integer such that $\mathbb{F}_{p^k}$ contains all of the r-th roots of unity in $\overline{\mathbb{F}}_p$, that is $\Omega_r \subset \mathbb{F}_{p^k}$.
- k is the smallest positive integer such that $E(\overline{\mathbb{F}}_p)[r] \subset E(\mathbb{F}_{p^k})$

An elliptic curve is called **pairing-friendly** if it has a relatively small embedding degree k (typically, $k \leq 16$).

Application #1: BLS Signature

Suppose we have pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ (with generators G_1, G_2, respectively), and a hash function H, mapping message space $\mathcal{M}$ to $\mathbb{G}_1$.

Application #1: BLS Signature

Suppose we have pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (with generators G_1, G_2, respectively), and a hash function H, mapping message space $\mathcal{M}$ to $\mathbb{G}_1$.

Definition

BLS Signature consists of the following algorithms:

- $\text{Gen}(\cdot)$: Key generation. $\text{sk} \xleftarrow{R} \mathbb{Z}_q, \text{pk} \leftarrow [\text{sk}]G_2 \in \mathbb{G}_2$.

Application #1: BLS Signature

Suppose we have pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (with generators G_1, G_2, respectively), and a hash function H, mapping message space $\mathcal{M}$ to $\mathbb{G}_1$.

Definition

BLS Signature consists of the following algorithms:

- $\mathsf{Gen}(\cdot)$: Key generation. $\mathsf{sk} \xleftarrow{R} \mathbb{Z}_q, \mathsf{pk} \leftarrow [\mathsf{sk}]G_2 \in \mathbb{G}_2$.
- $\mathsf{Sign}(\mathsf{sk}, m)$. Signature is $\sigma \leftarrow [\mathsf{sk}]\mathsf{H}(m) \in \mathbb{G}_1$.

Application #1: BLS Signature

Suppose we have pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (with generators G_1, G_2, respectively), and a hash function H, mapping message space $\mathcal{M}$ to $\mathbb{G}_1$.

Definition

BLS Signature consists of the following algorithms:

- $\mathsf{Gen}(\cdot)$: Key generation. $\mathsf{sk} \xleftarrow{R} \mathbb{Z}_q, \mathsf{pk} \leftarrow [\mathsf{sk}]G_2 \in \mathbb{G}_2$.
- $\mathsf{Sign}(\mathsf{sk}, m)$. Signature is $\sigma \leftarrow [\mathsf{sk}]\mathsf{H}(m) \in \mathbb{G}_1$.
- $\mathsf{Verify}(\mathsf{pk}, m, \sigma)$. Check whether $e(\mathsf{H}(m), \mathsf{pk}) = e(\sigma, G_2)$.

Application #1: BLS Signature

Suppose we have pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (with generators G_1, G_2, respectively), and a hash function H, mapping message space $\mathcal{M}$ to $\mathbb{G}_1$.

Definition

BLS Signature consists of the following algorithms:

- $\mathsf{Gen}(\cdot)$: Key generation. $\mathsf{sk} \xleftarrow{R} \mathbb{Z}_q, \mathsf{pk} \leftarrow [\mathsf{sk}]G_2 \in \mathbb{G}_2$.
- $\mathsf{Sign}(\mathsf{sk}, m)$. Signature is $\sigma \leftarrow [\mathsf{sk}]\mathsf{H}(m) \in \mathbb{G}_1$.
- $\mathsf{Verify}(\mathsf{pk}, m, \sigma)$. Check whether $e(\mathsf{H}(m), \mathsf{pk}) = e(\sigma, G_2)$.

Let us check the correctness:

$$e(\sigma, G_2) = e([\mathsf{sk}]\mathsf{H}(m), G_2) =$$

Application #1: BLS Signature

Suppose we have pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (with generators G_1, G_2, respectively), and a hash function H, mapping message space $\mathcal{M}$ to $\mathbb{G}_1$.

Definition

BLS Signature consists of the following algorithms:

- $\mathsf{Gen}(\cdot)$: Key generation. $\mathsf{sk} \xleftarrow{R} \mathbb{Z}_q, \mathsf{pk} \leftarrow [\mathsf{sk}]G_2 \in \mathbb{G}_2$.
- $\mathsf{Sign}(\mathsf{sk}, m)$. Signature is $\sigma \leftarrow [\mathsf{sk}]\mathsf{H}(m) \in \mathbb{G}_1$.
- $\mathsf{Verify}(\mathsf{pk}, m, \sigma)$. Check whether $e(\mathsf{H}(m), \mathsf{pk}) = e(\sigma, G_2)$.

Let us check the correctness:

$$e(\sigma, G_2) = e([\mathsf{sk}]\mathsf{H}(m), G_2) = e(\mathsf{H}(m), [\mathsf{sk}]G_2) =$$

Application #1: BLS Signature

Suppose we have pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (with generators G_1, G_2, respectively), and a hash function H, mapping message space $\mathcal{M}$ to $\mathbb{G}_1$.

Definition

BLS Signature consists of the following algorithms:

- $\mathsf{Gen}(\cdot)$: Key generation. $\mathsf{sk} \xleftarrow{R} \mathbb{Z}_q, \mathsf{pk} \leftarrow [\mathsf{sk}]G_2 \in \mathbb{G}_2$.
- $\mathsf{Sign}(\mathsf{sk}, m)$. Signature is $\sigma \leftarrow [\mathsf{sk}]\mathsf{H}(m) \in \mathbb{G}_1$.
- $\mathsf{Verify}(\mathsf{pk}, m, \sigma)$. Check whether $e(\mathsf{H}(m), \mathsf{pk}) = e(\sigma, G_2)$.

Let us check the correctness:

$$e(\sigma, G_2) = e([\mathsf{sk}]\mathsf{H}(m), G_2) = e(\mathsf{H}(m), [\mathsf{sk}]G_2) = e(\mathsf{H}(m), \mathsf{pk})$$

Application #1: BLS Signature

Suppose we have pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (with generators G_1, G_2, respectively), and a hash function H, mapping message space $\mathcal{M}$ to $\mathbb{G}_1$.

Definition

BLS Signature consists of the following algorithms:

- $\text{Gen}(\cdot)$: Key generation. $\text{sk} \xleftarrow{R} \mathbb{Z}_q, \text{pk} \leftarrow [\text{sk}]G_2 \in \mathbb{G}_2$.
- $\text{Sign}(\text{sk}, m)$. Signature is $\sigma \leftarrow [\text{sk}]\text{H}(m) \in \mathbb{G}_1$.
- $\text{Verify}(\text{pk}, m, \sigma)$. Check whether $e(\text{H}(m), \text{pk}) = e(\sigma, G_2)$.

Let us check the correctness:

$$e(\sigma, G_2) = e([\text{sk}]\text{H}(m), G_2) = e(\text{H}(m), [\text{sk}]G_2) = e(\text{H}(m), \text{pk})$$

Remark: $\mathbb{G}_1$ and $\mathbb{G}_2$ might be switched: public keys might live instead in $\mathbb{G}_1$ while signatures in $\mathbb{G}_2$.

Application #2: Quadratic Verifications

Task

Alice wants to convince Bob that she knows such α, β such that $\alpha + \beta = 2$, but she does not want to reveal α, β. How to do that?

Application #2: Quadratic Verifications

Task

Alice wants to convince Bob that she knows such α, β such that $\alpha + \beta = 2$, but she does not want to reveal α, β. How to do that?

Example

1. Alice computes $P \leftarrow [\alpha]G, Q \leftarrow [\beta]G$ — points on the curve.

Application #2: Quadratic Verifications

Task

Alice wants to convince Bob that she knows such α, β such that $\alpha + \beta = 2$, but she does not want to reveal α, β. How to do that?

Example

1. Alice computes $P \leftarrow [\alpha]G, Q \leftarrow [\beta]G$ — points on the curve.
2. Alice sends (P, Q) to Bob.

Application #2: Quadratic Verifications

Task

Alice wants to convince Bob that she knows such α, β such that $\alpha + \beta = 2$, but she does not want to reveal α, β. How to do that?

Example

1. Alice computes $P \leftarrow [\alpha]G, Q \leftarrow [\beta]G$ — points on the curve.
2. Alice sends (P, Q) to Bob.
3. Bob verifies whether $P \oplus Q = [2]G$.

Application #2: Quadratic Verifications

Task

Alice wants to convince Bob that she knows such α, β such that $\alpha + \beta = 2$, but she does not want to reveal α, β. How to do that?

Example

1. Alice computes $P \leftarrow [\alpha]G, Q \leftarrow [\beta]G$ — points on the curve.
2. Alice sends (P, Q) to Bob.
3. Bob verifies whether $P \oplus Q = [2]G$.

Let us verify the **correctness:**

$$P \oplus Q = [\alpha]G \oplus [\beta]G = [\alpha + \beta]G = [2]G$$

Application #2: Quadratic Verifications

Task

Alice wants to convince that she knows α, β such that $\alpha\beta = 2$ without revealing α, β.

Application #2: Quadratic Verifications

Task

Alice wants to convince that she knows α, β such that $\alpha\beta = 2$ without revealing α, β.

Example

1. Alice computes $P \leftarrow [\alpha]G_1 \in \mathbb{G}_1$, $Q \leftarrow [\beta]G_2 \in \mathbb{G}_2$ — points on two curves.

Application #2: Quadratic Verifications

Task

Alice wants to convince that she knows α, β such that $\alpha\beta = 2$ without revealing α, β.

Example

1. Alice computes $P \leftarrow [\alpha]G_1 \in \mathbb{G}_1$, $Q \leftarrow [\beta]G_2 \in \mathbb{G}_2$ — points on two curves.
2. Alice sends $(P, Q) \in \mathbb{G}_1 \times \mathbb{G}_2$ to Bob.

Application #2: Quadratic Verifications

Task

Alice wants to convince that she knows α, β such that $\alpha\beta = 2$ without revealing α, β.

Example

1. Alice computes $P \leftarrow [\alpha]G_1 \in \mathbb{G}_1$, $Q \leftarrow [\beta]G_2 \in \mathbb{G}_2$ — points on two curves.
2. Alice sends $(P, Q) \in \mathbb{G}_1 \times \mathbb{G}_2$ to Bob.
3. Bob checks whether: $e(P, Q) = e(G_1, G_2)^2$.

Application #2: Quadratic Verifications

Task

Alice wants to convince that she knows α, β such that $\alpha\beta = 2$ without revealing α, β.

Example

1. Alice computes $P \leftarrow [\alpha]G_1 \in \mathbb{G}_1$, $Q \leftarrow [\beta]G_2 \in \mathbb{G}_2$ — points on two curves.
2. Alice sends $(P, Q) \in \mathbb{G}_1 \times \mathbb{G}_2$ to Bob.
3. Bob checks whether: $e(P, Q) = e(G_1, G_2)^2$.

Again let us verify the **correctness:**

$$e(P, Q) = e([\alpha]G_1, [\beta]G_2) = e(G_1, G_2)^{\alpha\beta} = e(G_1, G_2)^2$$

Application #2: Quadratic Verifications

Task

Alice wants to convince that she knows x_1, x_2 such that $x_1^2 + x_1x_2 = x_2$ without revealing x_1, x_2.

Application #2: Quadratic Verifications

Task

Alice wants to convince that she knows x_1, x_2 such that $x_1^2 + x_1x_2 = x_2$ without revealing x_1, x_2.

Example

Alice calculates $P_1 \leftarrow [x_1]G_1 \in \mathbb{G}_1$, $P_2 \leftarrow [x_1]G_2 \in \mathbb{G}_2$, $Q \leftarrow [x_2]G_2 \in \mathbb{G}_2$. Then, the condition can be verified by checking whether

$$e(P_1, P_2 \oplus Q)e(G_1, \ominus Q) = 1$$

Application #2: Quadratic Verifications

Task

Alice wants to convince that she knows x_1, x_2 such that $x_1^2 + x_1 x_2 = x_2$ without revealing x_1, x_2.

Example

Alice calculates $P_1 \leftarrow [x_1]G_1 \in \mathbb{G}_1$, $P_2 \leftarrow [x_1]G_2 \in \mathbb{G}_2$, $Q \leftarrow [x_2]G_2 \in \mathbb{G}_2$. Then, the condition can be verified by checking whether

$$e(P_1, P_2 \oplus Q)e(G_1, \ominus Q) = 1$$

Let us see the correctness of this equation:

$$\begin{aligned} e(P_1, P_2 \oplus Q)e(G_1, \ominus Q) &= e([x_1]G_1, [x_1 + x_2]G_2)e(G_1, [x_2]G_2)^{-1} \\ &= e(G_1, G_2)^{x_1(x_1+x_2)}e(G_1, G_2)^{-x_2} = e(G_1, G_2)^{x_1^2+x_1x_2-x_2} \end{aligned}$$

Thanks for your attention!