11. Elliptic curves.

A. Ushakov

MA503, April 13, 2022

Contents

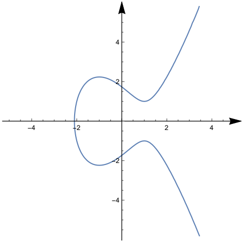
Here we define elliptic curves. Elliptic-curve based cryptography (ECC) allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.

- Elliptic curve.
- Addition on $\mathcal{E}$: geometric definition.
- Formula for $P \oplus Q$. Examples.
- $(\mathcal{E}, +)$ is an abelian group.
- Elliptic curves over finite fields $\mathbb{Z}_p$.
- Example of an elliptic curve over $\mathbb{Z}_{13}$.
- Computing multiples in $\mathcal{E}$.
- Primitive elements in $\mathcal{E}$.

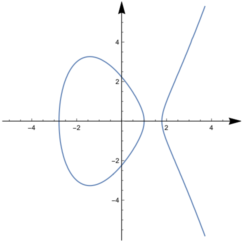
Elliptic curve

Definition

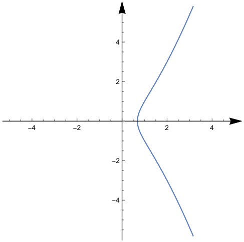
An **elliptic curve** $\mathcal{E}$ is the set of solutions (with a special element $\mathcal{O}$) of an equation of the form $y^2 = x^3 + ax + b$, called a **Weierstrass equation**.



$y^2 = x^3 - 3x + 3$



$y^2 = x^3 - 6x + 5$



$y^2 = x^3 + x - 1$

Proposition (no proof)

The curve is **non-singular** *if it has no cusps or self-intersections* $\Leftrightarrow$ $4a^3 + 27b^2 \neq 0$.

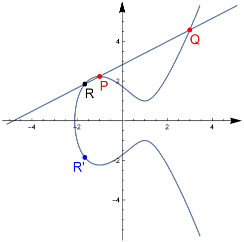
For any $a, b \in \mathbb{R}$ the curve contains infinitely many points.

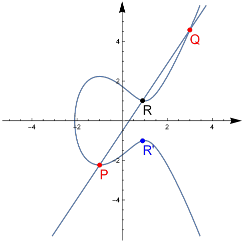
The equation $(y^*)^2 = x^3 + ax + b$ has at least one solution for x for any $y^* \in \mathbb{R}$.

Addition on $\mathcal{E}$: geometric definition

Every elliptic curve is symmetric: $(x, y) \in \mathcal{E} \quad \Rightarrow \quad (x, -y) \in \mathcal{E}$.

For $P(x_1, y_1), Q(x_2, y_2) \in \mathcal{E}$ we define the point $P \oplus Q \in \mathcal{E}$ as follows.





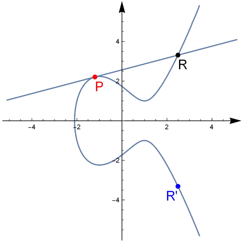
Case-I: $x_1 \neq x_2$.

- consider the line α through P and Q,
- α intersects $\mathcal{E}$ at three points $P, Q, R(x_3, y_3)$
- the point $R'(x_3, -y_3)$ is called the **sum** of P and Q, denoted $P + Q$.

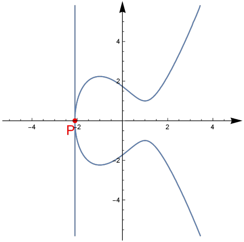
α and $\mathcal{E}$ have three points of intersection.

- The equation of the line α through P and Q is $y = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$.
- Replacing y with $y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$ in $y^2 = x^3 + ax + b$ we get a qubic equation.
- That equation has two real zeros x_1, x_2.
- Hence, it has another real zero x_3.

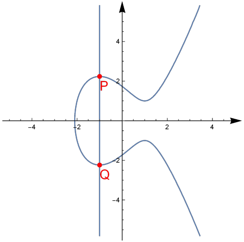
Addition on $\mathcal{E}$: geometric definition



Case-II: If $x_1 = x_2$ and $y_1 = y_2 \neq 0$, then use the tangent line α at P.



Case-III: If $x_1 = x_2$ and $y_1 = y_2 = 0$, then $P + P = \mathcal{O}$.



Case-IV: If $x_1 = x_2$ and $y_1 \neq y_2$, then α has only two intersections. In that case, $P + Q = \mathcal{O}$.

Case-V: $P + \mathcal{O} = P$.

Formula for $P \oplus Q$

The line α has an equation $y = \lambda x + \nu$, where the slope is $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{in Case-I,} \\ \frac{3x_1^2 + a}{2y_1} & \text{in Case-II,} \end{cases}$

for some $\nu \in \mathbb{R}$ that we don't need to find.

$$\begin{aligned} y^2 = x^3 + ax + b \quad &\Rightarrow \quad (\lambda x + \nu)^2 = x^3 + ax + b \qquad \text{(replacing } y \text{ with } \lambda x + \nu\text{)} \\ &\Rightarrow \quad x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + (b - \nu^2) = 0. \end{aligned}$$

Since x_1 and x_2 are its zeros, there should be $x_3 \in \mathbb{R}$ satisfying

$$\begin{aligned} x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + (b - \nu^2) &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_1x_3)x - x_1x_2x_3. \end{aligned}$$

The coefficients in front of x^2 must be the same and, hence

$$\begin{aligned} \lambda^2 = x_1 + x_2 + x_3 \quad &\Rightarrow \quad x_3 = \lambda^2 - x_1 - x_2 \\ &\Rightarrow \quad y_3 = \lambda x_3 + \nu = \lambda(\lambda^2 - x_1 - x_2) + \nu = y_1 - \lambda(x_1 - x_3). \end{aligned}$$

$P \oplus Q = (x_3, y_3)$, where $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$.

Computing $P \oplus Q$: examples

For the curve $y^2 = x^3 - 15x + 18$ and points $P(7,16)$, $Q(1,2)$, and $R(3,0)$.

To compute $P \oplus Q$ we compute

- $\lambda = \frac{-14}{-6} = \frac{7}{3}$;
- $x_3 = \frac{49}{9} - 7 - 1 = \frac{-23}{9}$;
- $y_3 = \frac{7}{3}\left(7 - \frac{-23}{9}\right) - 16 = \frac{-170}{27}$.

Thus, $P \oplus Q = \left(\frac{-23}{9}, \frac{-170}{27}\right)$.

To compute $P \oplus P$ we compute

- $\lambda = \frac{3 \cdot 7^2 - 15}{2 \cdot 16} = \frac{33}{8}$.
- $x_3 = \left(\frac{33}{8}\right)^2 - 7 - 7 = \frac{193}{64}$.
- $y_3 = \frac{33}{8}\left(7 - \frac{193}{64}\right) - 16 = \frac{223}{512}$.

Thus, $P \oplus P = \left(\frac{193}{64}, \frac{223}{512}\right)$.

$-P = (7, -16)$, $-Q = (1, -2)$, *and* $-R = R$.

Elliptic curve is an abelian group

Theorem

$(\mathcal{E}, +)$ *is an abelian group.*

By design, the following holds:

- $P + Q = Q + P$.
- $P + \mathcal{O} = \mathcal{O} + P = P$. Hence, $\mathcal{O}$ is the identity.
- $Q(x, -y)$ is the inverse of $P(x, y)$.
- $(P + Q) + R = P + (Q + R)$ – hard to prove!

Mention some "geometric identities".

Elliptic curve over $\mathbb{Z}_p$

In general, we can use any finite field $\mathrm{GF}(p^n)$.

Definition

For a prime $p \geq 3$ and an equation $y^2 = x^3 + ax + b$ satisfying $4a^3 + 27b^2 \neq 0$ the set

$$\mathcal{E} = \left\{ (x, y) \in \mathbb{Z}_p \,\middle|\, y^2 = x^3 + ax + b \right\} \cup \{\mathcal{O}\}$$

is called an **elliptic curve** over $\mathbb{Z}_p$.

Addition on a $\mathbb{Z}_p$-curve $\mathcal{E}$ is defined using the formulas for an $\mathbb{R}$-curve.
$(\mathcal{E}, \oplus)$ is a finite abelian group for a $\mathbb{Z}_p$-curve $\mathcal{E}$.

Theorem (Hasse)

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Z}_p$. Then $|\mathcal{E}| = p + 1 - t_p$, for some t_p satisfying $|t_p| \leq 2\sqrt{p}$.

$t_p = p + 1 - |\mathcal{E}|$ is called the **trace of Frobenius for $\mathcal{E}/\mathbb{Z}_p$**.

Theorem (Schoof–Elkies–Atkin)

- *There is a polynomial-time algorithm to compute $|\mathcal{E}|$.*
- *There is a polynomial-time algorithm to compute $|g|$ for any $g \in \mathcal{E}$.*

Example of an elliptic curve over $\mathbb{Z}_{13}$

For instance, for $y^2 = x^3 + 3x + 8$ and $p = 13$ we get all solutions by taking square root of $x^3 + 3x + 8$ for $x = 0, \ldots, 12$

- For $x = 0$ we get $y^2 \equiv_{13} 8$ that has no solutions.
- For $x = 1$ we get $y^2 \equiv_{13} 12$ that has solutions $5, 8$. This contributes two points $(1, 5)$ and $(1, 8)$ to $\mathcal{E}$.
- For $x = 2$ we get $y^2 \equiv_{13} 22$ that has solutions $3, 10$. This contributes two points $(2, 3)$ and $(2, 10)$ to $\mathcal{E}$. Etc.

$\mathcal{E} = \{\mathcal{O}, (1, 5), (1, 8), (2, 3), (2, 10), (9, 6), (9, 7), (12, 2), (12, 11)\}$

To compute $(1, 8) \oplus (1, 8)$

$$\lambda = \frac{3 \cdot 1^2 + 3}{2 \cdot 8} = \frac{6}{16} \equiv \frac{6}{3} = 2 \quad \textit{and} \quad \begin{cases} x_3 = 2^2 - 1 - 1 = 2 \\ y_3 = 2(1 - 2) - 8 = -10 = 3 \end{cases}$$

To compute $(2, 3) \oplus (9, 7)$

$$\lambda = \frac{7 - 3}{9 - 2} = \frac{4}{7} \equiv_{13} 8 \quad \textit{and} \quad \begin{cases} x_3 = 8^2 - 2 - 9 = 53 \equiv_{13} 1 \\ y_3 = 8(2 - 1) - 3 = 5 \end{cases}$$

Example of an elliptic curve (cont)

For $\mathcal{E} = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}$ we have the following addition table:

$+$	$\mathcal{O}$	**(1,5)**	**(1,8)**	**(2,3)**	**(2,10)**	**(9,6)**	**(9,7)**	**(12,2)**	**(12,11)**
$\mathcal{O}$	$\mathcal{O}$	(1,5)	(1,8)	(2,3)	(2,10)	(9,6)	(9,7)	(12,2)	(12,11)
(1,5)	(1,5)	(2,10)	O	(1,8)	(9,7)	(2,3)	(12,2)	(12,11)	(9, 6)
(1,8)	(1,8)	$\mathcal{O}$	(2,3)	(9,6)	(1,5)	(12,11)	(2,10)	(9,7)	(12, 2)
(2,3)	(2, 3)	(1, 8)	(9, 6)	(12, 11)	$\mathcal{O}$	(12, 2)	(1, 5)	(2, 10)	(9, 7)
(2, 10)	(2, 10)	(9, 7)	(1, 5)	$\mathcal{O}$	(12, 2)	(1, 8)	(12, 11)	(9, 6)	(2, 3)
(9, 6)	(9, 6)	(2, 3)	(12, 11)	(12, 2)	(1, 8)	(9, 7)	$\mathcal{O}$	(1, 5)	(2, 10)
(9, 7)	(9, 7)	(12, 2)	(2, 10)	(1, 5)	(12, 11)	$\mathcal{O}$	(9, 6)	(2, 3)	(1, 8)
(12, 2)	(12, 2)	(12, 11)	(9, 7)	(2, 10)	(9, 6)	(1, 5)	(2, 3)	(1, 8)	$\mathcal{O}$
(12, 11)	(12, 11)	(9, 6)	(12, 2)	(9, 7)	(2, 3)	(2, 10)	(1, 8)	$\mathcal{O}$	(1, 5)

Elliptic curve over $\mathbb{Z}_p$: computing multiples

Addition in $\mathcal{E}$ is efficient (can be computed in time polynomial in $\log_2(p)$).

Because it requires basic operations modulo p to compute $(x_1, y_1) + (x_2, y_2)$.

An elliptic curve $\mathcal{E}$ is an additive group, i.e., it uses addition as a group operation. Hence, if we compose n copies of $g \in \mathcal{E}$ we get a **multiple** of g

$$\mathsf{n} \cdot \mathsf{g} = \underbrace{g + \ldots + g}_{n \text{ times}}.$$

For $(x, y) \in \mathcal{E}$ and $n \in \mathbb{N}$ we can efficiently compute $n \cdot g$.

We can use binary-exponentiation-like method. We can compute sufficiently many multiples of the form

$$\begin{aligned}
2 \cdot (x, y) &= (x, y) + (x, y) \\
2^2 \cdot (x, y) &= 2 \cdot (x, y) + 2 \cdot (x, y) \\
2^3 \cdot (x, y) &= 2^2 \cdot (x, y) + 2^2 \cdot (x, y) \\
2^4 \cdot (x, y) &= 2^3 \cdot (x, y) + 2^3 \cdot (x, y) \\
&\ldots
\end{aligned}$$

Then write n in binary $n = b_k 2^k + \ldots + b_1 2 + b_0$ (for $b_i = 0, 1$) and compute

$$\mathsf{n} \cdot (\mathsf{x}, \mathsf{y}) = \sum_{\mathsf{i}=0}^{\mathsf{k}} \mathsf{b_i} 2^{\mathsf{i}} \cdot (\mathsf{x}, \mathsf{y}).$$

Multiples: example

For an elliptic curve $\mathcal{E}$ defined by $y^2 = x^3 + 23x + 13$ over $\mathbb{Z}_{83}$. A point $(24, 14)$ belongs to $\mathcal{E}$ because

$$14^2 \equiv_{83} 24^3 + 23 \cdot 24 + 13.$$

To compute $17(24, 14)$ we compute

$$\begin{aligned} 2 \cdot (24, 14) &= (30, 8) \\ 4 \cdot (24, 14) &= (24, 69) \\ 8 \cdot (24, 14) &= (30, 75) \\ 16 \cdot (24, 14) &= (24, 14). \end{aligned}$$

Then $17 \cdot (24, 14) = 16 \cdot (24, 14) + (24, 14) = (24, 14) + (24, 14) = (30, 8)$.

Primitive elements

Definition

$g \in \mathcal{E}$ is a **primitive element** $\Leftrightarrow$ $\mathcal{E} = \langle g \rangle$ $\Leftrightarrow$ $|g| = |\mathcal{E}|$.

For instance, for $y^2 = x^3 + 3x + 8$ over $\mathbb{Z}_{13}$ and $g = (1,5)$ we have

$$0(1,5) = \mathcal{O} \qquad 5(1,5) = (12,11)$$
$$1(1,5) = (1,5) \qquad 6(1,5) = (9,6)$$
$$2(1,5) = (2,10) \qquad 7(1,5) = (2,3)$$
$$3(1,5) = (9,7) \qquad 8(1,5) = (1,8)$$
$$4(1,5) = (12,2) \qquad 9(1,5) = \mathcal{O}.$$

Hence, $|(1,5)| = 9$, $\mathcal{E} = \langle(1,5)\rangle$, and, $(1,5)$ is primitive in $\mathcal{E}$. Now, for $g = (9,6)$

$$0(9,6) = \mathcal{O} \qquad 2(9,6) = (9,7)$$
$$1(9,6) = (9,6) \qquad 3(9,6) = \mathcal{O}.$$

Hence, $|(9,6)| = 3$ and $(9,6)$ is not primitive in $\mathcal{E}$.

Proposition (How do we check if g is primitive in $\mathcal{E}$?)

If $\mathrm{PPF}(|\mathcal{E}|) = p_1^{a_1} \dots p_k^{a_k}$, *then*

$$g \text{ is primitive} \quad \Leftrightarrow \quad g^{|\mathcal{E}|/p_i} \neq \mathcal{O} \text{ for every } i.$$

The numbers $|\mathcal{E}|/p_i$ are the **greatest proper divisors** of $|\mathcal{E}|$.

Primitive elements: example

The elliptic curve $\mathcal{E}$ defined by $y^2 = x^3 + 2x + 9$ over $\mathbb{Z}_{67}$ contains 75 elements, i.e., $|\mathcal{E}| = 75 = 3 \cdot 5^2$. 75 has two greatest proper divisors: 15 and 25.

- $25(0,3) = \mathcal{O} \quad \Rightarrow \quad (0,3)$ is not primitive.
- $15(6,6) = \mathcal{O} \quad \Rightarrow \quad (6,6)$ is not primitive.
- $15(8,1) \neq \mathcal{O}$ and $25(8,1) \neq \mathcal{O} \quad \Rightarrow \quad (8,1)$ is primitive.