ECC'2024 Autumn school, Tapei, Taiwan

Lecture 1: Introduction on Elliptic Curves

Aurore Guillevic

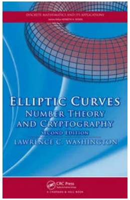
Centre Inria de l'Université de Rennes

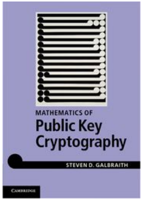
October 28, 2024

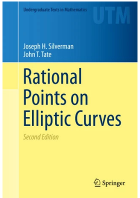
These slides at `https://people.rennes.inria.fr/Aurore.Guillevic/talks/01-intro-ecc.pdf`

References

- Elliptic curves, number theory and cryptography, Lawrence C. Washington
- Mathematics of public key cryptography, Steven Galbraith, freely available in PDF at `https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf`
- Rational points on elliptic curves, Joseph H. Silverman, John Tate `https://link.springer.com/book/10.1007/978-3-319-18588-0`







SageMath installation

SageMath library: a mathematical software suite based on Python, open-source.

Download at `https://www.sagemath.org/download.html` (consider mirrors)
Choose *No development*.

The lecturer: Aurore Guillevic

- Permenent researcher at Inria, France Since 2016
- Visiting professor at Aarhus University, 2021–2022
  See `https://members.loria.fr/AGuillevic/teaching/`
  §Aarhus 2022, for course materials on elliptic curves
- PhD in 2010–2013 at Thales and École Normale Superieure, Paris, France
- `aurore.guillevic@inria.fr`

Content

- Basic introduction on elliptic curves this morning
  - What is an elliptic curve, over $\mathbb{Q}$, over $\mathbb{F}_p$?
  - Group law
  - Scalar multiplication
  - Hard problems in crypto: discrete logarithm computation
  - Elliptic curves in cryptography (requirements, constraints, examples)
- Introduction on pairings and the CM method this afternoon
  - Supersingular curves, ordinary curves
  - Frobenius, torsion
  - Hints on point counting
  - pairings on elliptic curves for crypto

Elliptic curves in cryptography

- 1985 (published in 1987) Hendrik Lenstra Jr., Elliptic Curve Method (ECM) for integer factoring
- 1985, Koblitz, Miller: Elliptic Curves over a finite field form a group suitable for Diffie–Hellman key exchange
- 1985, Certicom: company owning patents on ECC
- 2000 Elliptic curves in IEEE P1363 standard
- 2000 Bilinear pairings over elliptic curves
- NSA cipher suite B, elliptic curves for public-key crypto
- 2014: Quasi-polynomial-time algorithm
  for discrete log computation in GF(2^n), GF(3^m)
  No more pairings on elliptic curves over these fields
- 2015: Tower Number Field Sieve in GF(p^n)
  Pairing-friendly curves should have larger key sizes
- 2016: NIST Post-Quantum competition
  Isogenies on elliptic curves, Hiroshi Onuki's next talk

Widely deployed elliptic curves in cryptosystems

- elliptic curve over the prime field $2^{255} - 19$ of order $8r$ where r is prime
  - `Curve25519` in Montgomery form $E\colon y^2 = x^3 + 48662x^2 + x$
  - `Ed25519` in twisted Edwards form $E\colon -x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$
- NIST P-xxx curves
- `secp256k1`, BLS12-381... in proof systems and blockchains
- ...

Usage:

- Digital signatures (ECDSA): Play Station, EU Covid Certificate...
- Diffie–Hellman key exchange: open-ssl, TLS...
- Encryption: PGP, ...

Why elliptic curves?

Diophantine equations

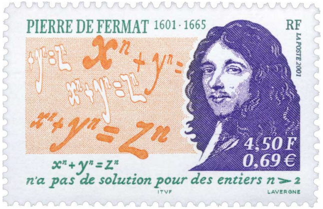
From Diophantus of Alexandria, mathematician
Finding integer or rational solutions to polynomial equations

Bachet equation $y^2 - x^3 = c$

given an integer c, find a cube x^3 and a square y^2 whose difference is c
Claude-Gaspard Bachet de Méziriac (1581–1638)
Translated Diophantus' *Arithmetica* from Greek to latin.

Fermat's conjecture, a.k.a. Fermat's Last Theorem

Pierre de Fermat (1601–1665)
For $n \geq 3$, the equation $X^n + Y^n = Z^n$ has no solutions in non-zero integers X, Y, Z.
Actually not proven by Fermat



https://www.wikitimbres.fr/

Bachet's equation $y^2 - x^3 = c$

Bachet discovered in 1621 this

duplication formula

If (x, y) is a rational solution, then

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right)$$

is another solution in rational numbers.

If $xy \neq 0$ and $c \neq 1, -432$, it gives infinitely many distinct solutions.

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

Starting from $5^2 - 3^3 = 25 - 27 = -2$, one obtains

$$(3, 5), \left(\frac{129}{100}, \frac{383}{1000}\right), \left(\frac{2340922881}{58675600}, \frac{113259286337279}{449455096000}\right)$$

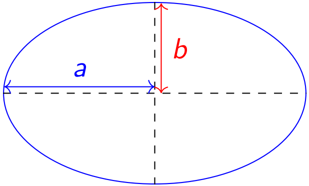
Example in Washington's book

Volume and surface

Rearrange a pyramid of height x layers of fruits into a flat square:
solve $y^2 = x(x+1)(2x+1)/6$ with integer solutions

Conic sections

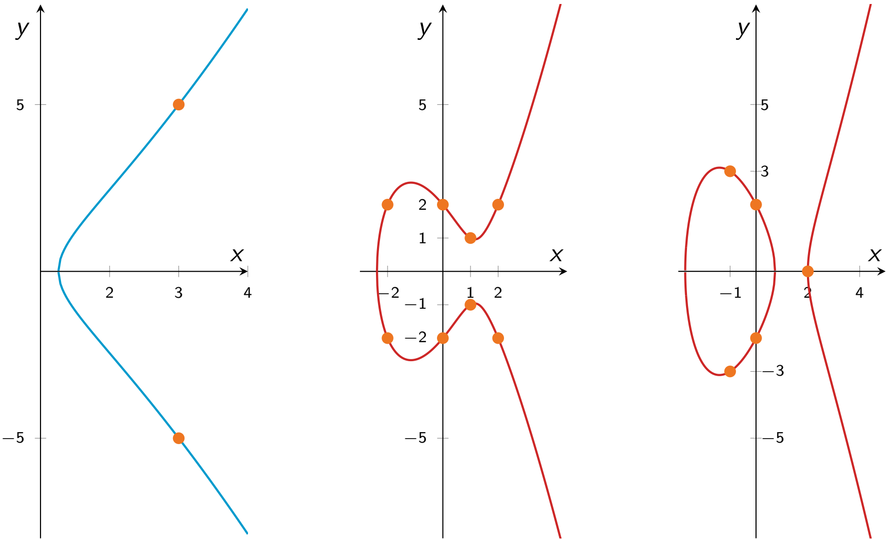
Ellipses are conic sections defined by $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$



Ellipses are not elliptic curves.
This ellipse has **area** πab. What is the **circumference**? $\rightarrow$ complicated formula with *elliptic integral*.

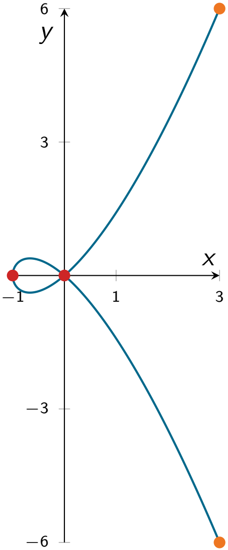
Bachet's equation is an elliptic curve

$y^2 - x^3 = -2$ $\qquad$ $y^2 = x^3 - 4x + 4$ $\qquad$ $y^2 = x^3 - 6x + 4$

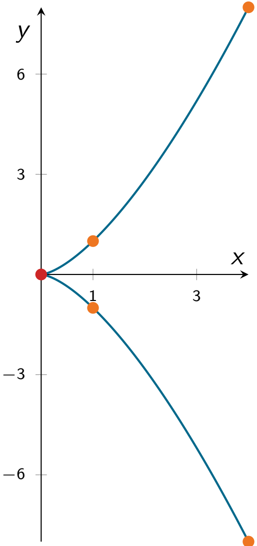


Curves with singularities are not elliptic curves

$$y^2 = x^2(x+1)$$



$$y^2 = x^3$$



The curve is smooth

Let $E\colon f(x,y)=0$ over a field K, $K=\mathbb{Q}$, $K=\mathbb{F}_p$, $K=\mathbb{F}_{2^n}$ for example.
There is no singular point (x_0,y_0) such that

$$\begin{cases} f(x_0,y_0)=0 \\ \dfrac{\partial f}{\partial x}(x_0,y_0)=0 \\ \dfrac{\partial f}{\partial y}(x_0,y_0)=0 \end{cases}$$

where $\partial f/\partial x$, $\partial f/\partial y$ are the partial derivatives.

Definitions

Elliptic Curve

An **Elliptic Curve** over a field K is a smooth curve of *genus 1* with a K-rational point.

Genus 1

A curve given by an equation

$$y^2 = f(x), \text{ where } \deg f \in \{3, 4\}$$

has genus 1.

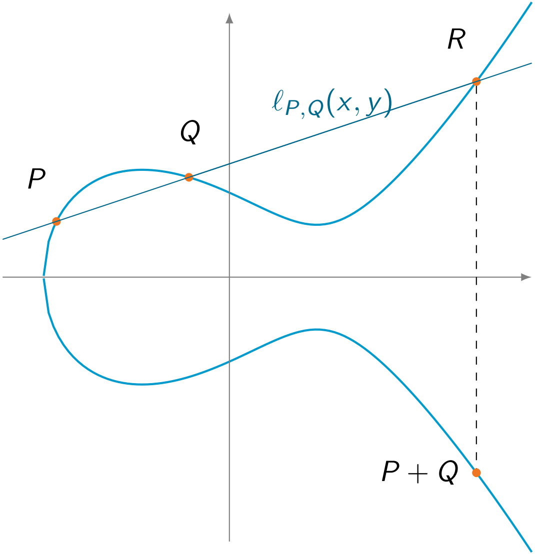
Structure of Group

Given two points $P(x, y)$, $Q(x', y')$, one can *add* two points $P + Q$ and double a point $P + P$ (algebraic point of view) ans the group law has a geometric meaning.

Weierstrass model

- An elliptic curve over a field K of characteristic $\neq 2, 3$ is given by an equation of the form
$$E\colon y^2 = x^3 + ax + b, \text{ with } a, b \in K$$
and $\Delta = -16(4a^3 + 27b^2) \neq 0$ so that E is smooth
(the cubic $x^3 + ax + b$ has simple roots)
- The set of K-rational points of an elliptic curve is
$$E(K) = \Big\{(x, y) \in K \times K;\ y^2 = x^3 + ax + b\Big\} \cup \{\mathcal{O}\}$$
- In the general case, one considers the long **Weierstrass** form
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$
where $a_1, a_2, a_3, a_4, a_6 \in K$.

Chord and tangent rule



$P(x_1, y_1)$, $Q(x_2, y_2)$, $x_1 \neq x_2$

slope $\lambda = \dfrac{\Delta y}{\Delta x} = \dfrac{y_2 - y_1}{x_2 - x_1}$

line L through P and Q has equation

$L\colon y = \lambda(x - x_1) + y_1$

$\to$ check that $(x_1, y_1) \in L$, $(x_2, y_2) \in L$

compute $\boldsymbol{L \cap E}$

$(x, y) \in L$ and $\in E \Rightarrow$

$$\begin{cases} L\colon y = \lambda(x - x_1) + y_1 \\ E\colon y^2 = x^3 + ax + b \end{cases} \Rightarrow$$

$(\lambda(x - x_1) + y_1)^2 = x^3 + ax + b$

Solve with SageMath to avoid mistakes

Chord and tangent rule

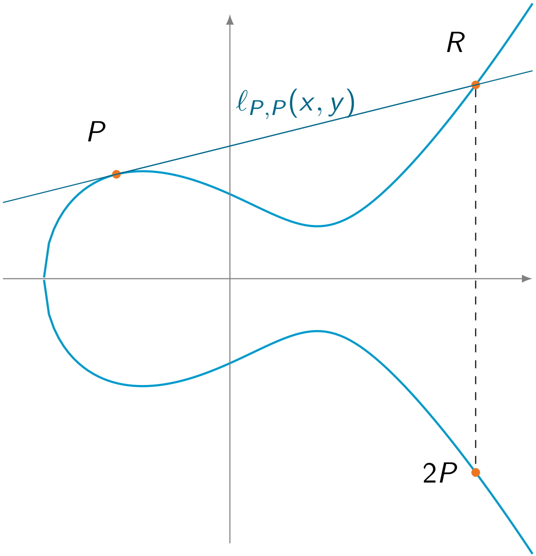
$$\begin{cases} L\colon y = \lambda(x - x_1) + y_1 \\ E\colon y^2 = x^3 + ax + b \end{cases}$$

Substitute $y = \lambda(x - x_1) + y_1$ in E to get a cubic in x:
$x^3 - \lambda^2 x^2 + (2x_1\lambda^2 - 2y_1\lambda + a)x - x_1^2\lambda^2 + 2x_1 y_1 \lambda - y_1^2 + b = 0$
We know that x_1, x_2 are solutions $\implies$
$(x - x_1)(x - x_2)$ is a factor. Take out $(x - x_1)(x - x_2)$:
$x - \lambda^2 + x_1 + x_2 = 0 \implies x_3 = \lambda^2 - x_1 - x_2$ is solution
Use L equation to get $-y_3 = \lambda(x_3 - x_1) + y_1$ (negative sign)
Finally,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

One can check with `group_law_short_weierstrass_affine.sage`

Doubling a point in affine coordinates (x, y)



Doubling a point in affine coordinates (x, y)

The line L tangent at the curve $E\colon f(x,y) = y^2 - x^3 - ax - b = 0$ at $P(x_1, y_1)$ has equation

$$\frac{\partial f}{\partial x}(x_1, y_1) + \frac{\partial f}{\partial y}(x_1, y_1)\frac{dy}{dx} = 0$$

$$\begin{aligned}
(-3x_1^2 - a) + 2y_1\frac{y - y_1}{x - x_1} &= 0 \\
(-3x_1^2 - a)(x - x_1) + 2y_1(y - y_1) &= 0 \\
-\frac{3x_1^2 + a}{2y_1}(x - x_1) + (y - y_1) &= 0 \text{ if } y_1 \neq 0
\end{aligned}$$

The slope is $\lambda = \frac{-\partial f/\partial x}{\partial f/\partial y}(x_1, y_1) = \frac{3x_1^2 + a}{2y_1}$

Again L has equation $\lambda(x - x_1) + (y - y_1) = 0$

This time we know that x_1 is a double root of $E \cap L$

Algebraic description of the addition operation

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on

$$E\colon y^2 = x^3 + ax + b\ .$$

The slope of the line (P, Q) is given by

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq \pm Q \\[2ex] \dfrac{3x_1 + a}{2y_1} & \text{if } P = Q \text{ and } y_1 \neq 0 \end{cases}$$

The sum of P and Q is the point

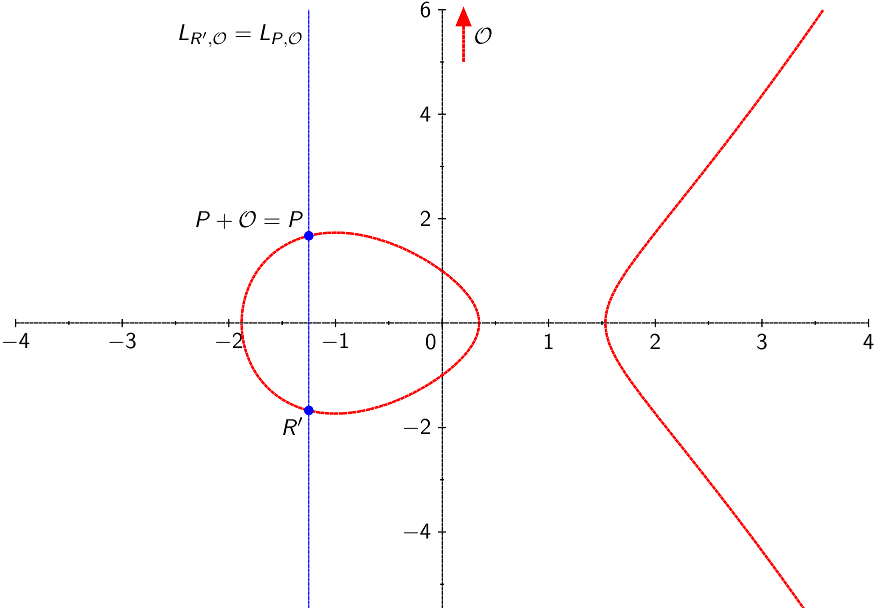
$$P + Q = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)\ .$$

Points of order 2, points of order 3

Points of order 2 are such that $P + P = \mathcal{O}$, that is $P = -P$ and $P = (x_0, 0)$.
At P the tangent is a vertical.

Points of order 3 are **inflexion points**.
$2P = -P$ that is the intersection of the tangent at P with the curve is again at P, is has multiplicity 3.

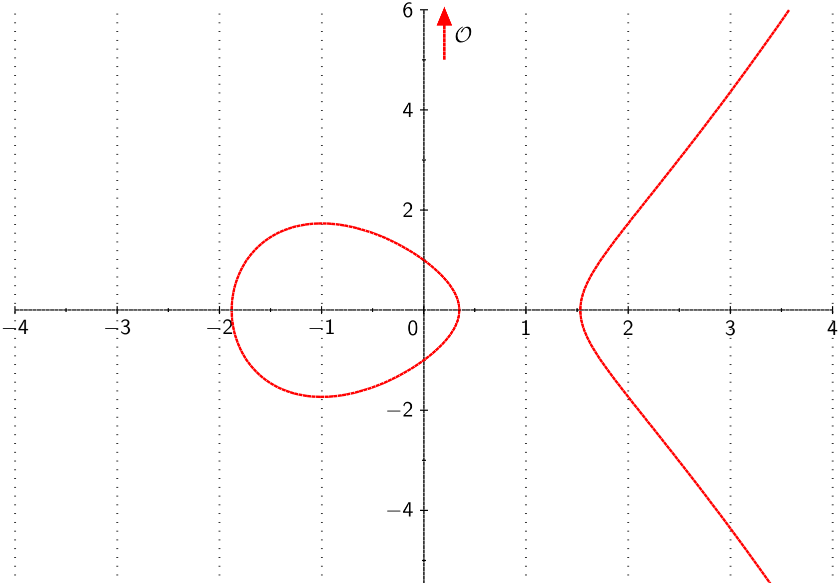
$P + (-P)$



$L_{R',\mathcal{O}} = L_{P,\mathcal{O}}$
$\mathcal{O}$
$P + \mathcal{O} = P$
R'
6
4
2
−2
−4
−4
−3
−2
−1
0
1
2
3
4

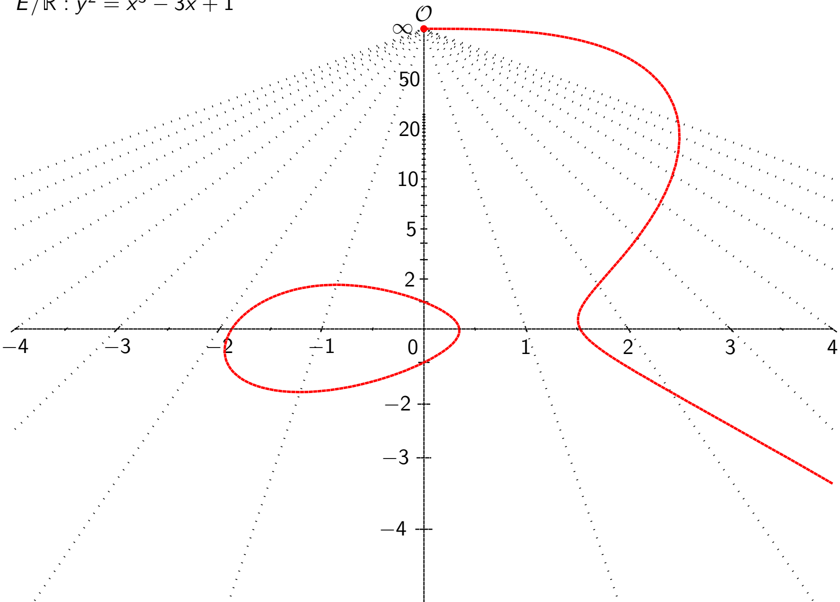
Projective space and point at infinity

$E/\mathbb{R} : y^2 = x^3 - 3x + 1$



Projective space and point at infinity

$E/\mathbb{R} : y^2 = x^3 - 3x + 1$



Projective space and point at infinity

$$E/K\colon y^2 = x^3 + Ax + B \qquad \text{Char}(K) \neq 2,3$$

Affine plane (Euclidean plane) over a field K

$$\mathbb{A}^2(K) = \{(x,y)\colon x,y \in K\}$$

Group of points of E on K

The set of rational points on the curve E/K is

$$E(K) = \left\{(x,y) \in \mathbb{A}^2(K) \mid (x,y) \text{ satisfies } E\right\} \cup \{P_\infty\}$$

where P_∞ is the *point at infinity*.

We cannot represent the point at infinity P_∞ in the affine space $\mathbb{A}$: there is no (∞, ∞).
Intuition: store the denominator z of the coordinates (x,y) in a 3rd coord.

Projective space and point at infinity

Elliptic curves are **projective plane (smooth) curves**

Projective plane

The **projective plane** of dimension 2 defined over a field K, denoted $\mathbb{P}^2(K)$ is

$$\mathbb{P}^2(K) = \left\{(X, Y, Z) \in K^3 \mid (X, Y, Z) \neq (0, 0, 0)\right\} / \sim$$

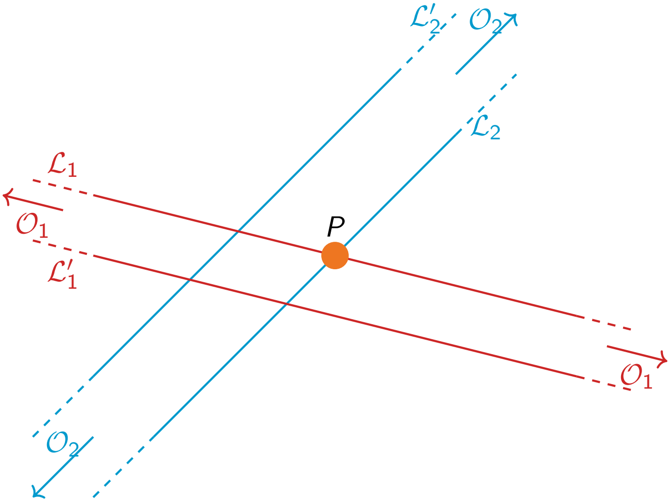
with the equivalence relation $(X, Y, Z) \sim (X', Y', Z') \iff$ there exists $\lambda \neq 0 \in K$ such that $(X, Y, Z) = (\lambda X', \lambda Y', \lambda Z')$.

The **equivalence class** w.r.t. $\sim$ is denoted $(X : Y : Z)$ with colons instead of commas.

Two parallel lines meet at infinity

At infinity is not a single point

Distinct pairs of parallel lines do not meet at the same point at infinity.
$\mathcal{L}_1 \cap \mathcal{L}_2 = \{P\}$ in $\mathbb{A}^2$ so $\mathcal{L}_1, \mathcal{L}_2$ cannot share a 2nd point $\mathcal{O}$



Projective plane smooth curve

A projective plane cubic curve $\mathcal{C}$ in $\mathbb{P}^2(K)$ is given by an equation

$$\mathcal{C}\colon F(X,Y,Z)=0$$

where F is a homogeneous polynomial of degree 3.

An elliptic curve in $\mathbb{P}^2(K)$ is given by an equation

$$\mathcal{E}\colon Y^2Z = X^3 + aXZ^2 + bZ^3,\ 4a^3 + 27b^2 \neq 0$$

and the group of points on $\mathcal{E}$ is

$$\mathcal{E}(K) = \{(X,Y,Z) \in \mathbb{P}^2(K)\colon F_{\mathcal{E}}(X,Y,Z) = 0\}$$

Point at infinity in the Projective Plane

$$\mathcal{E}\colon Y^2Z = X^3 + aXZ^2 + bZ^3,\ 4a^3 + 27b^2 \neq 0$$

$$Z = 0 \implies \mathcal{E}\colon 0 = X^3$$

The **Point at infinity** is

$$(X, Y, Z = 0) \in \mathcal{E}(K) \implies X = 0$$

There is no condition on Y except $Y \neq 0$ because $(0, 0, 0) \notin \mathbb{P}^2$.
Then $(0, \lambda, 0)$ for any $\lambda \neq 0$ is the direction of a vertical line in $\mathbb{A}^2$.

Point at infinity on $\mathcal{E}$

The equivalence class of the point at infinity on $\mathcal{E}$ is $\mathcal{O} = (0 : 1 : 0)$.

Projective coordinates

Washington's book section 2.6.1
Addition and doubling can be done without special treatment of points of order 2
$P(x, 0) \in \mathbb{A}^2 \mapsto (X, 0, 1) \in \mathbb{P}^2$
$P(X_1, Y_1, Z_1) + Q(X_2, Y_2, Z_2)$
Suppose that none is $\mathcal{O}$, then $Z_1 \neq 0$, $Z_2 \neq 0$.
Their affine part is $P(x_1, y_1) = (X_1/Z_1, Y_1/Z_1)$ and $Q(x_2, y_2) = (X_2/Z_2, Y_2/Z_2)$.

$\mathcal{L}$ through P and Q has slope $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1} = \dfrac{Y_2/Z_2 - Y_1/Z_1}{X_2/Z_2 - X_1/Z_1} = \dfrac{Y_2 Z_1 - Y_1 Z_2}{X_2 Z_1 - X_1 Z_2}$

If $P = Q$ then $\lambda = \dfrac{3x_1^2 + a}{2y_1} = \dfrac{3X_1^2/Z_1^2 + a}{2Y_1/Z_1} = \dfrac{3X_1^2 + aZ_1^2}{2Y_1 Z_1}$

Addition law in projective coordinates (in $\mathbb{P}^2(K)$)

See the Elliptic Curve Formula Database (EFD) by Tanja Lange:
`www.hyperelliptic.org/EFD/g1p/auto-shortw-projective.html`
Let $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$ be two points on

$$E\colon Y^2Z = X^3 + aXZ^2 + bZ^3 .$$

Adapting directly the formula $\lambda = (y_2 - y_1)/(x_2 - x_1)$, resp. $\lambda = (3x_1^2 + a)/(2y_1)$ to projective coordinates with $x_i = X_i/Z_i$, $y_i = Y_i/Z_i$, the slope of the line (P, Q) is given by

$$\lambda = \begin{cases} \dfrac{Y_2Z_1 - Y_1Z_2}{X_2Z_1 - X_1Z_2} & \text{if } P \neq \pm Q \\[2ex] \dfrac{3X_1^2 + aZ_1^2}{2Y_1Z_1} & \text{if } P = Q \text{ and } Y_1 \neq 0 \end{cases}$$

Addition law in projective coordinates in $\mathbb{P}^2(K)$

Cohen, Miyaji and Ono published at Asiacrypt'1998 the formulas

$$
\begin{aligned}
u &= Y_2 \cdot Z_1 - Y_1 \cdot Z_2 \\
v &= X_2 \cdot Z_1 - X_1 \cdot Z_2 \\
A &= u^2 \cdot Z_1 \cdot Z_2 - v^3 - 2v^2 \cdot X_1 Z_2 \\
X_3 &= v \cdot A \\
Y_3 &= u \cdot (v^2 X_1 Z_2 - A) - v^3 \cdot Y_1 Z_2 \\
Z_3 &= v^3 \cdot Z_1 Z_2
\end{aligned}
$$

this costs 11 Mult., the squares u^2, v^2, then $v^3 = v^2 \cdot v$, hence
12 Mult. $+$ 2 Squares and negligible additions and subtractions.

Addition law in projective coordinates in $\mathbb{P}^2(K)$

For doubling, Cohen, Miyaji and Ono have

$$
\begin{aligned}
w &= aZ_1^2 + 3X_1^2 \\
s &= Y_1 \cdot Z_1 \\
B &= X_1 \cdot Y_1 \cdot s \\
h &= w^2 - 8B \\
X_3 &= 2h \cdot s \\
Y_3 &= w \cdot (4B - h) - 8 \cdot (Y_1 s)^2 \\
Z_3 &= 8s^3
\end{aligned}
$$

this costs 6 Mult., 5 Squares and $w^3 = w^2 \cdot w$, hence
7 Mult. + 5 Squares and negligible additions, subtractions and a multiplication by a.

Corner cases of addition law in projective coordinates in $\mathbb{P}^2(K)$

If $P = (X_1, Y_1, Z_1)$ and $Q = -P = (X_1, -Y_1, Z_1)$ with $Y_1 \neq 0$
then the addition formula computes
$(X_3, Y_3, Z_3) = (0, Y_3, 0)$ and $Y_3 = 8Y_1^3 Z_1^5 \neq 0$
This is the point at infinity $\mathcal{O}$, without division by 0.

If $P = (X_1, 0, Z_1)$ has order 2, the doubling formula computes
$(0, Y_3, 0) = \mathcal{O}$ without a division by 0.

Other coordinate systems and forms of elliptic curves

There are many other coordinate systems:

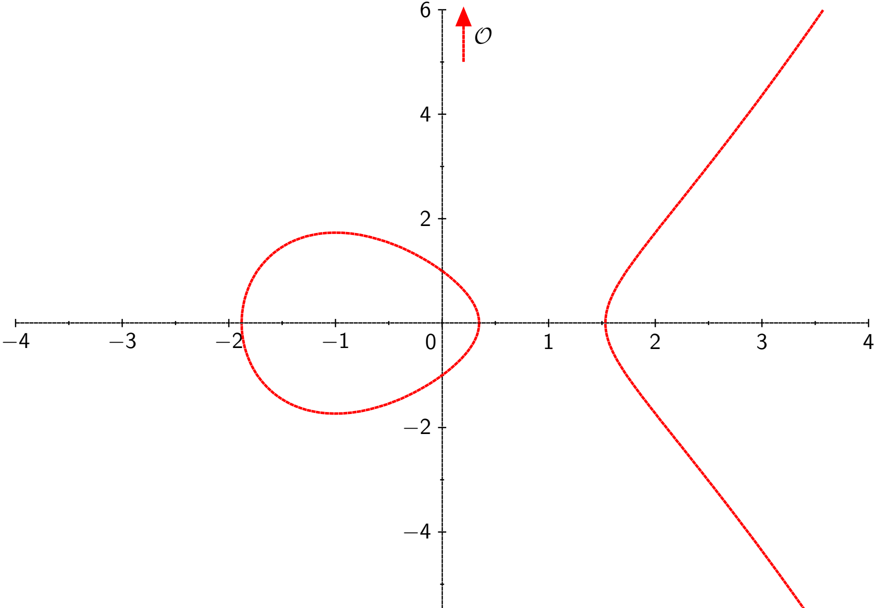
- affine (x, y)
- projective $(X, Y, Z) \mapsto (X/Z, Y/Z)$
- Jacobian $(X, Y, Z) \mapsto (X/Z^2, Y/Z^3)$
- extended Jacobian $(X, Y, Z, Z^2) \mapsto (X/Z^2, Y/Z^3)$
- ...

that can be combined with different **forms of curves**:

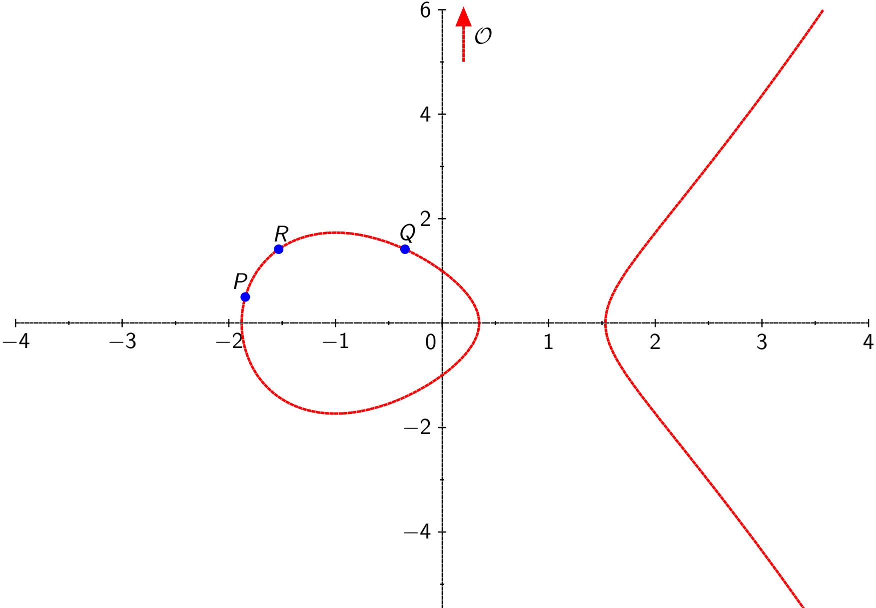
- Short Weierstrass with $a = -3$, $a = 1$, $a = 0$, $b = 0$, etc
- Specificities: points of order 2 or 4 available
- Montgomery form
- Edwards, twisted Edwards form
- Jacobi Quartic
- Huff form
- ...

$\rightarrow$ EFD contains almost all of them.

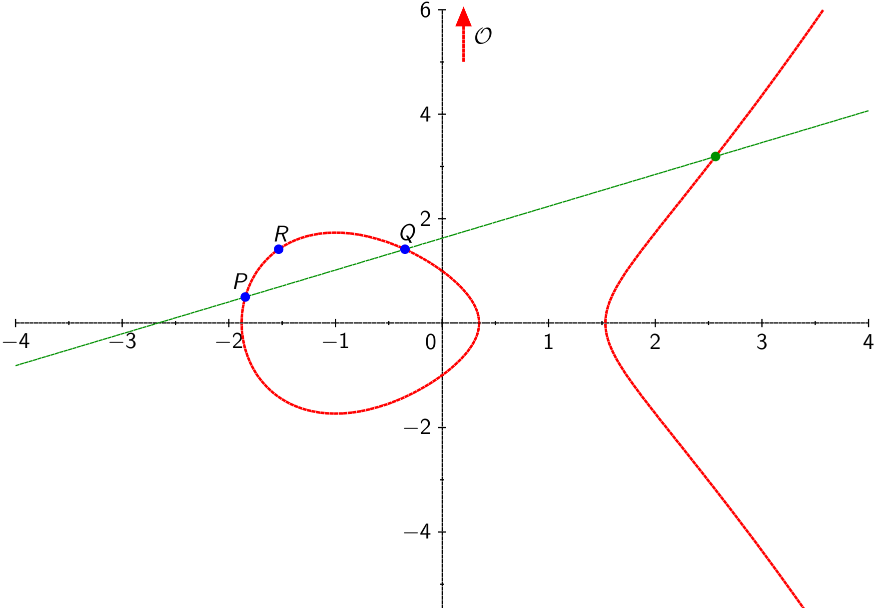
Associativity: $(P + Q) + R = P + (Q + R)$



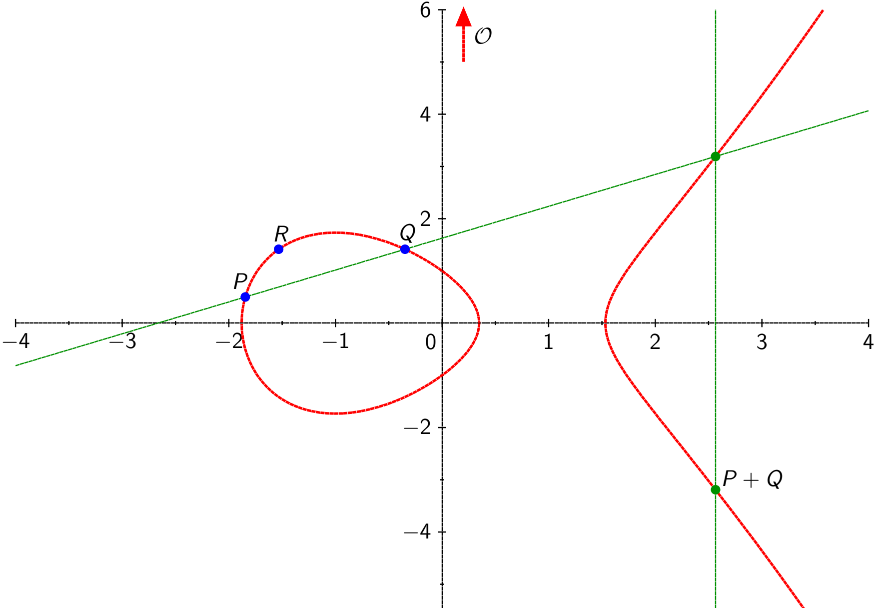
Associativity: $(P + Q) + R = P + (Q + R)$



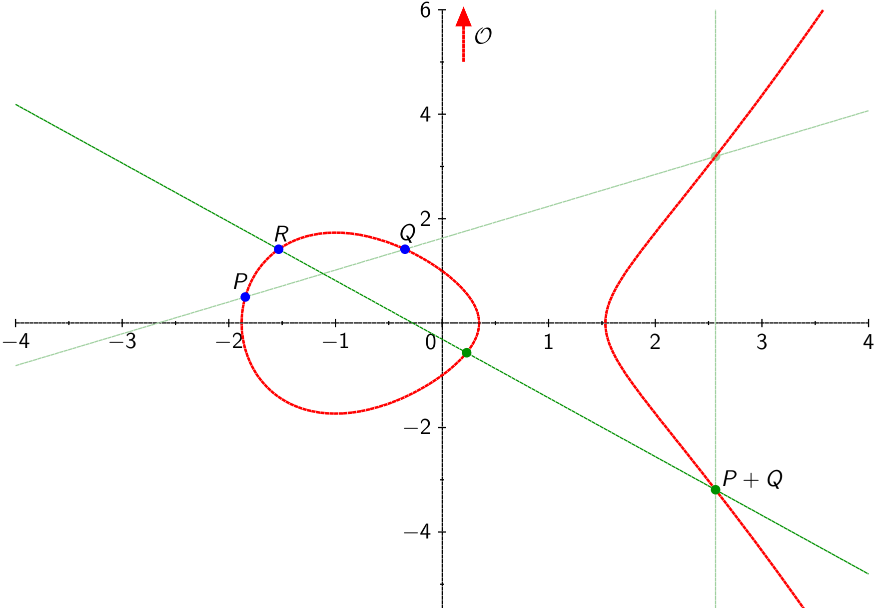
Associativity: $(P + Q) + R = P + (Q + R)$



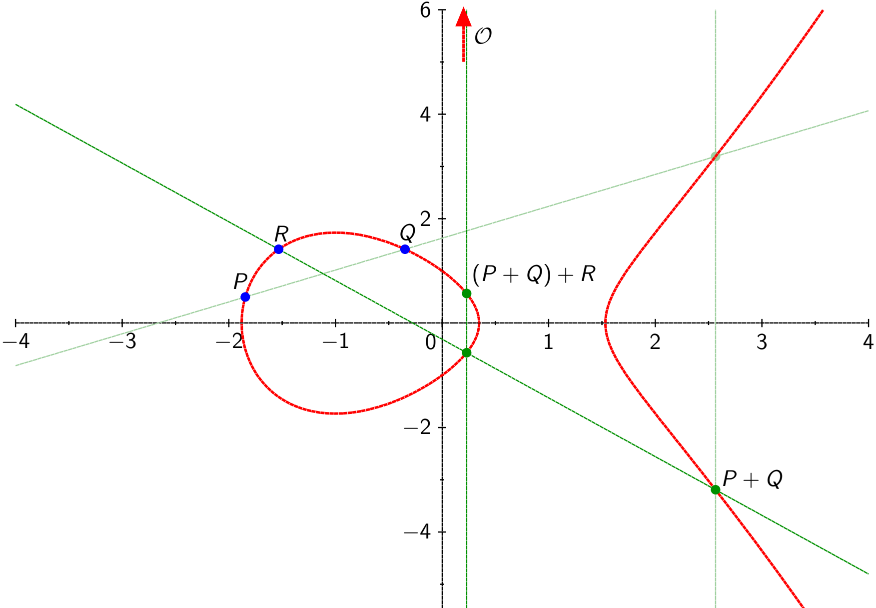
Associativity: $(P+Q)+R = P+(Q+R)$



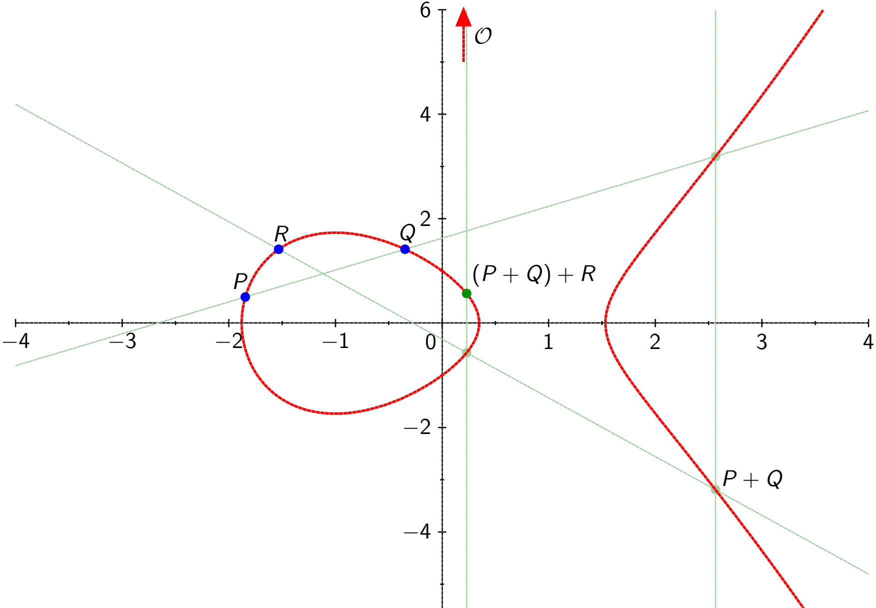
Associativity: $(P+Q)+R = P+(Q+R)$



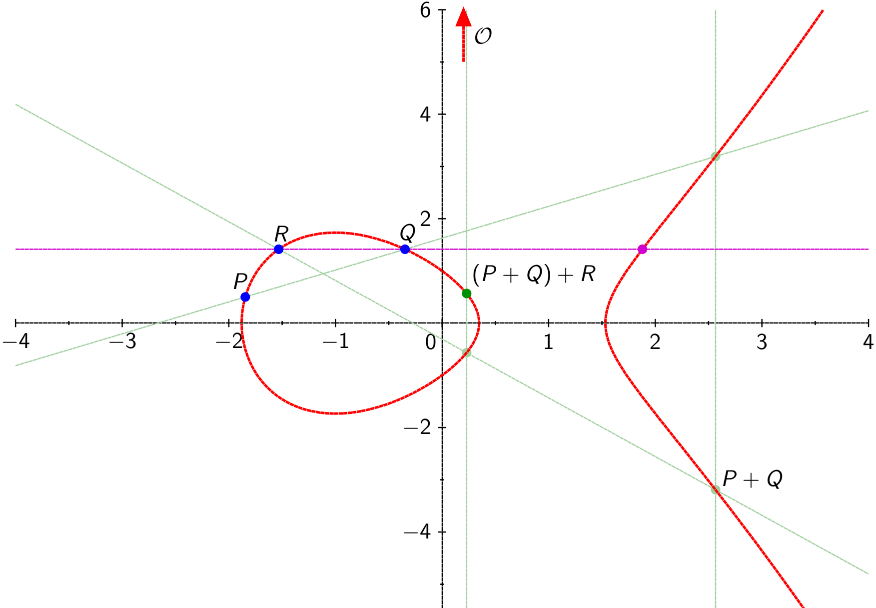
Associativity: $(P+Q)+R = P+(Q+R)$



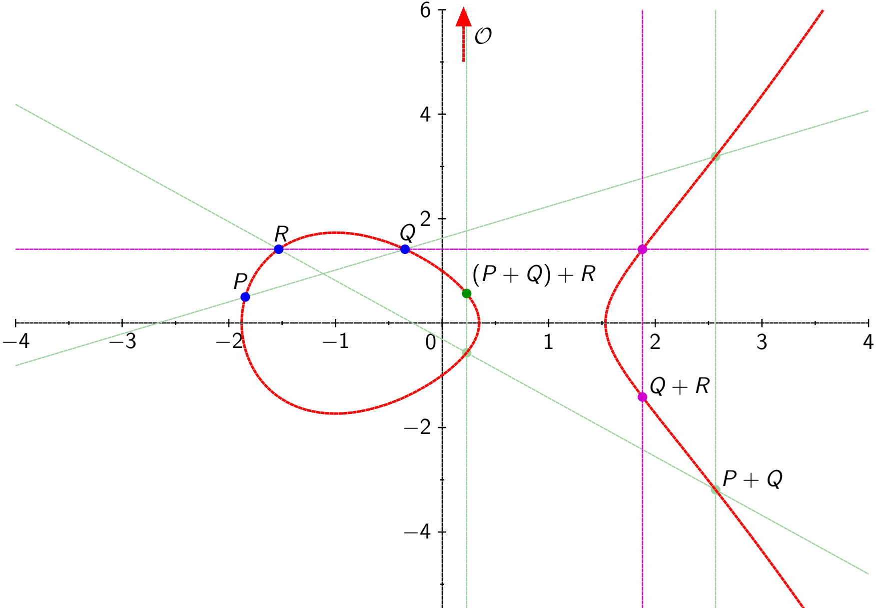
Associativity: $(P + Q) + R = P + (Q + R)$



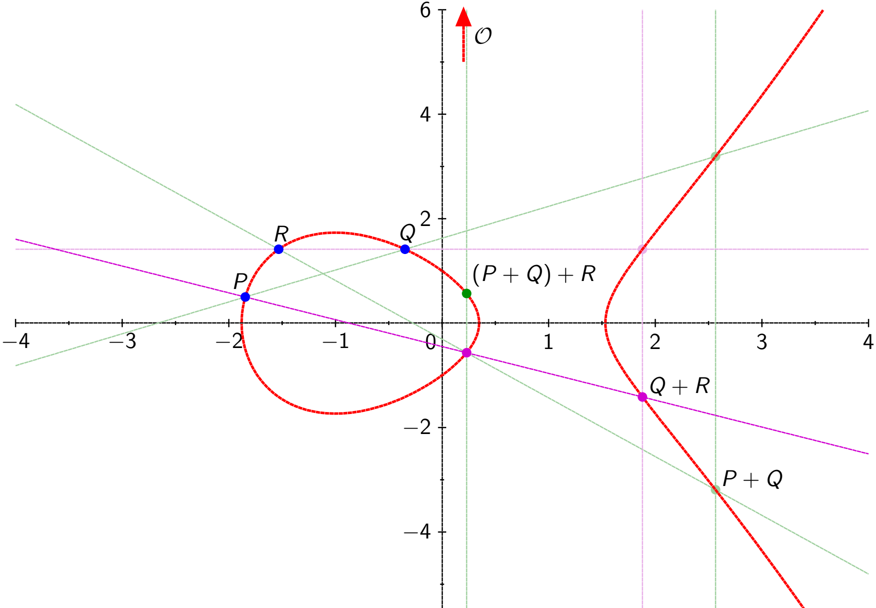
Associativity: $(P + Q) + R = P + (Q + R)$



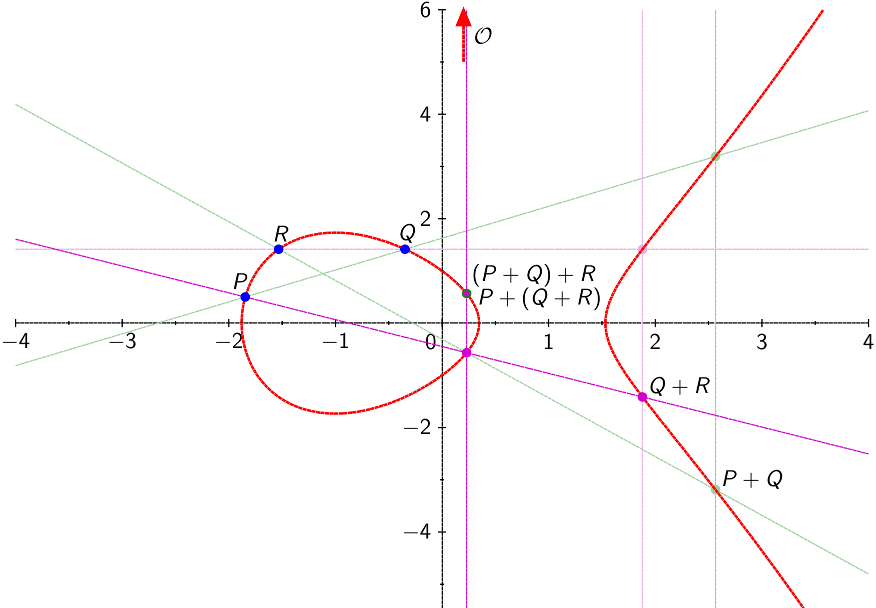
Associativity: $(P + Q) + R = P + (Q + R)$



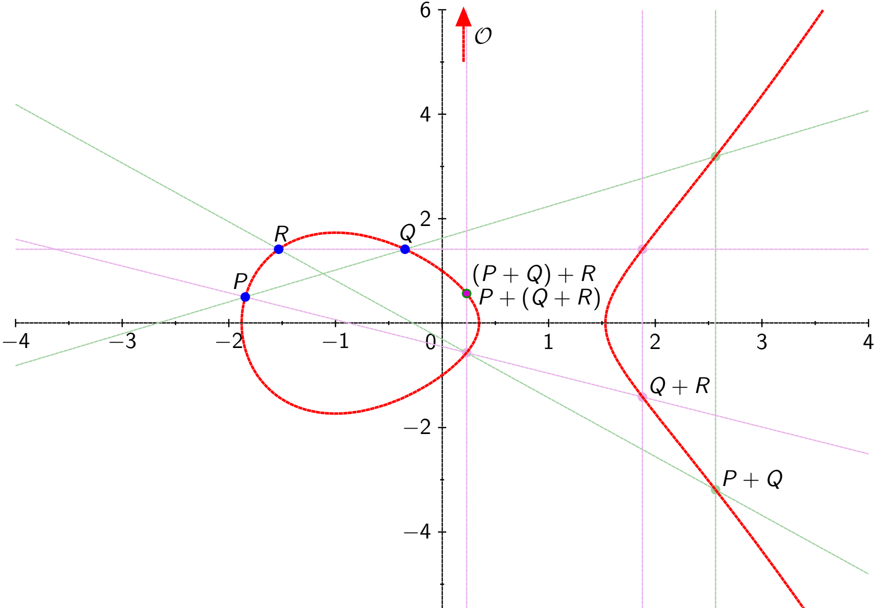
Associativity: $(P+Q)+R = P+(Q+R)$



Associativity: $(P + Q) + R = P + (Q + R)$



Associativity: $(P + Q) + R = P + (Q + R)$



Multiplicity of intersection and Bézout theorem

Idea of the proof using Bézout's theorem

Silverman–Tate book pages 16–21 and 238–240.
From Bézout's theorem, two distinct cubic projective plane curves without a common component have exactly 9 intersection points.

Idea of the proof:
Let's consider an elliptic curve $\mathcal{C}$ and the eight points

$$P, Q, R, \mathcal{O}, -(P+Q), P+Q, -(Q+R), (Q+R) \in \mathcal{C} \ .$$

To show associativity, show that there is a unique ninth point:

$$-((P+Q)+R) = -(P+(Q+R)) \ .$$

Main questions on curves over $\mathbb{Q}$

Given a bivariate polynomial equation $y^2 = f(x)$ with integer coefficients,

1. Are there any solutions in integers?
2. Are there any solutions in rational numbers?
3. Are there infinitely many solutions in integers?
4. Are there infinitely many solutions in rational numbers?

Consider these questions for elliptic curves, where

$$y^2 = x^3 + ax^2 + bx + c$$

Main theorems on curves over $\mathbb{Q}$

A non-singular cubic equation has only finitely many integer solutions (Siegel 1920), bound on the coefficients: Baker–Coates, 1970.

Nagell–Lutz: Points of finite order on an elliptic curve have integer coordinates.

Mordell: the group of points is finitely generated.

Mazur: structure of the group of torsion points (points of finite order)

Main theorems on curves over $\mathbb{Q}$

Nagell–Lutz Theorem

Let

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, c; and let D be the discriminant of the cubic polynomial $f(x)$,

$$= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \ .$$

Let $P = (x, y)$ be a rational point of finite order. Then x and y are integers; and either $y = 0$, in which case P has order two, or else y divides D.

Main theorems on curves over $\mathbb{Q}$

Mazur's theorem

Let $\mathcal{C}$ be a non-singular rational cubic curve, and suppose that $\mathcal{C}(\mathbb{Q})$ contains a point of finite order m. Then either

$$1 \leq m \leq 10 \text{ or } m = 12 \ .$$

More precisely, the set of all points of finite order in $\mathcal{C}(\mathbb{Q})$ forms a subgroup which has one of the following two forms:

1. $\mathbb{Z}/n\mathbb{Z}$ A cyclic group of order n with $1 \leq n \leq 10$ or $n = 12$.
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ The product of a cyclic group of order two and a cyclic group of order $2n$ with $1 \leq n \leq 4$.

Main theorems on curves over $\mathbb{Q}$

Mordell's theorem (Mordell–Weil)

If a non-singular rational plane cubic curve has a rational point, then the group of rational points is finitely generated.

Finite field

Prime finite field: a finite field of *prime* order.
(a *prime* field F has no proper non-trivial subfield $K \subsetneq F$)

3 notations for the same object:

- $\mathbb{Z}/p\mathbb{Z}$: the integers **modulo *p***,
- GF(p) for Galois Field,
- $\mathbb{F}_p$ (the field of p elements).

Representation: the integers $\{0, 1, 2, \ldots, p-1\}$
or the *centered* set $\{-(p-1)/2, \ldots, -1, 0, 1, \ldots, (p-1)/2\}$.

The prime number p is the **characteristic** of the finite field.
Field with $p = 2$: $\{0, 1\}$, where $1 + 1 = 0 \bmod 2$
Field with $p = 3$: $\{0, 1, 2\}$ where $1 + 1 = 2$, $1 + 2 = 0 \bmod 3$, $2 + 2 = 1 \bmod 3$
or $\{-1, 0, 1\}$ where $1 + 1 = -1$, $-1 - 1 = 1$, $1 - 1 = -1 + 1 = 0$

Arithmetic in a prime finite field $\mathbb{F}_p$

reduction mod p

for $x \in \mathbb{Z}$, compute the **Euclidean** division $x = bp + r$ where $0 \leq r < p$. Then $x \bmod p = r$.

neutral elements

0 is the neutral element for addition, 1 is the neutral element for multiplication

addition, subtraction $x + y \bmod p$, $x - y \bmod p$

compute $x + y$ as integers, if $x + y \geq p$, subtract p
Example: $3 + 5 \bmod 7 = 8 \bmod 7 = 1$

multiplication: $x \cdot y \bmod p$

Compute $x \cdot y$ like for integers then *reduce* modulo p

inversion

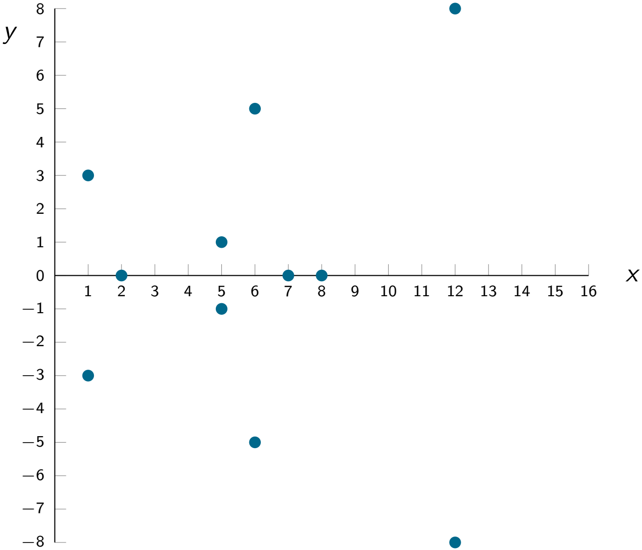
Because p is prime, its **GCD** with any integer $1 \leq x < p$ is 1.
Compute Bézout's identity $ux + vp = 1 = \gcd(x, p)$
Then $ux = 1 \bmod p$ and $1/x = u$

Extensions of prime fields

What does $\mathbb{F}_{p^2}$ mean? **The** field with p^2 elements.
Analogy with the complex numbers $\mathbb{C}$.
If $p = 3 \bmod 4$, -1 is not a square and $X^2 + 1$ is an irreducible polynomial in $\mathbb{F}_p[X]$
Define $\mathbb{F}_{p^2}$ as the quadratic extension $\mathbb{F}_p[X]/(X^2 + 1)$
This notation means: the quotient of all univariate polynomials $a(X)$ with coefficients in $\mathbb{F}_p$, modulo the polynomial $X^2 + 1$.
$X + 5 \bmod (X^2 + 1) = X + 5$
$X^2 \bmod (X^2 + 1) = -1$
$3X^2 + 7X + 1 \bmod (X^2 + 1) = -3 + 7X + 1 = 7X - 2$
$(X + 3) \times (2X - 1) = 2X^2 + 5X - 3 = -2 + 5X - 3 = 5X - 5$
In general, $\mathbb{F}_{p^n}$ is represented as $\mathbb{F}_p[X]/(f(X))$ where $f(X)$ is an irreducible polynomial of degree n.

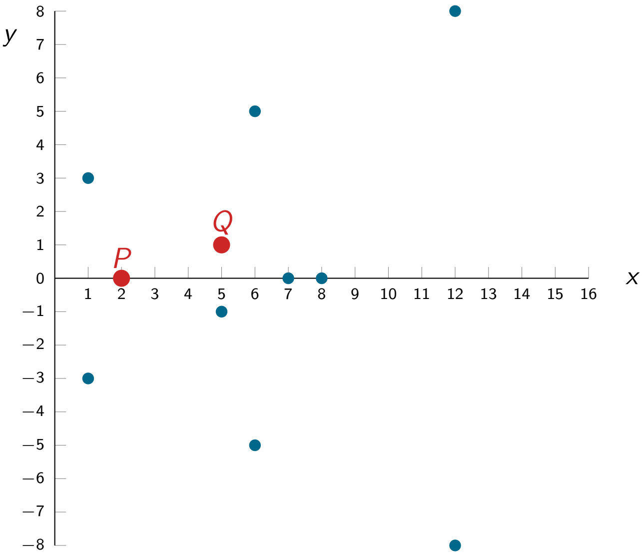
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}\colon y^2 = x^3 + x + 7$$



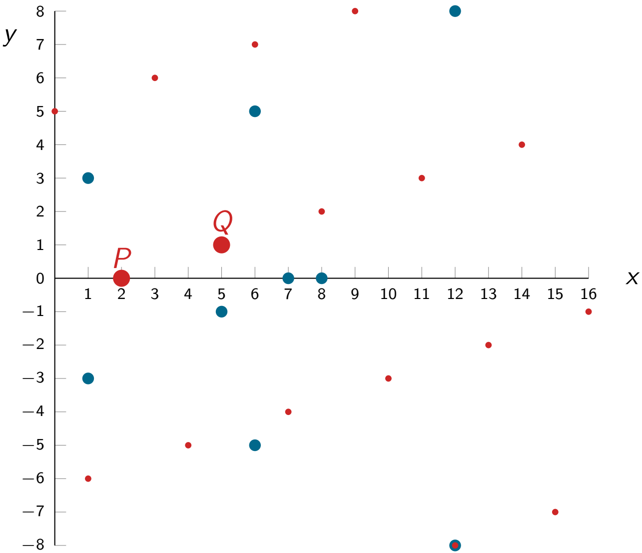
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}\colon y^2 = x^3 + x + 7$$



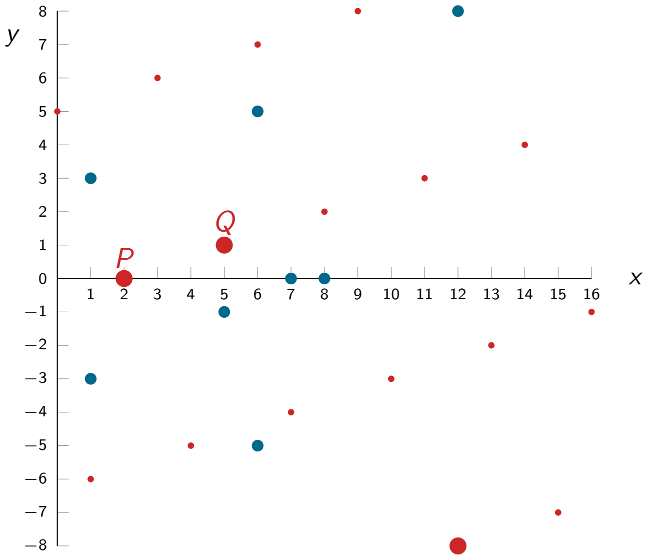
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}\colon y^2 = x^3 + x + 7$$



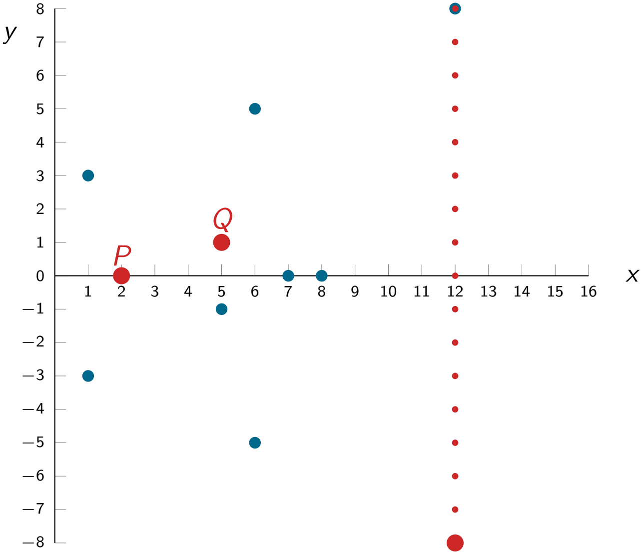
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}\colon y^2 = x^3 + x + 7$$



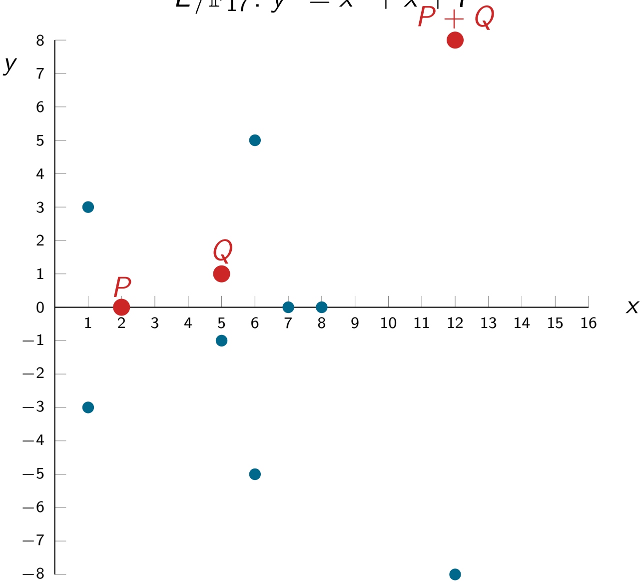
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}\colon y^2 = x^3 + x + 7$$



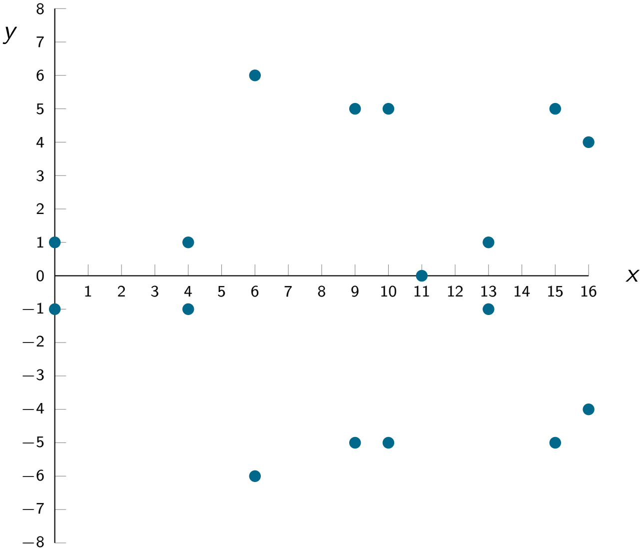
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}\colon y^2 = x^3 + x + 7$$



Elliptic curves over finite fields

$$E/\mathbb{F}_{17}\colon y^2 = x^3 + x + 1$$



Python

How to generate the set of points (x, y) of the curves

- $y^2 = x^3 + x + 7$
- $y^2 = x^3 + x + 1$

over $\mathbb{F}_{17}$? Over $\mathbb{F}_{31}$?

Scalar multiplication

With an addition law on E, the points on the curve form a group $E(K)$.

Scalar multiplication (exponentiation)

The **multiplication-by-**m map, or **scalar multiplication** is

$$\begin{array}{rcl} [m]\colon E & \to & E \\ P & \mapsto & \underbrace{P + \ldots + P}_{m \text{ copies of } P} \end{array}$$

for any $m \in \mathbb{Z}$, with $[-m]P = [m](-P)$ and $[0]P = \mathcal{O}$.

- a key-ingredient operation in public-key cryptography
- given $m > 0$, computing $[m]P$ as $P + P + \ldots P$ with $m - 1$ additions is **exponential** in the size of m: $m = e^{\ln m}$
- we can compute $[m]P$ in $O(\log m)$ operations on E.

Naive Scalar multiplication: Double-and-Add

Input: E defined over a field K, $m > 0$, $P \in E(K)$
Output: $[m]P \in E$

if $m = 0$ **then** **return** $\mathcal{O}$
Write m in binary expansion $m = \sum_{i=0}^{n-1} b_i 2^i$ where $b_i \in \{0, 1\}$
$R \leftarrow P$
for $i = n - 2$ *dowto* 0 **do** — loop invariant: $R = [\lfloor m/2^i \rfloor]P$
    $R \leftarrow [2]R$
    if $b_i = 1$ **then**
        $R \leftarrow R + P$
return R

Question: What are the best- and worst-case costs of the algorithm?
Question: Why is this algorithm dangerous if m is secret?

Naive Scalar multiplication: Double-and-Add

msb = most significant bits (highest powers)
lsb = least significant bits (units)
Pervious slide: **Most Significant Bits First** algorithm.

In Washington's book, §2.2 INTEGER TIMES A POINT p.18,
the LSB-first algorithm is given, disadvantage: one extra temporary variable.

Frobenius map, curve trace

Let E an elliptic curve defined over a finite field $\mathbb{F}_q$, q a prime power: $q = p$ or $q = p^\ell$, p prime.

- $E/\mathbb{F}_q$ means E defined over $\mathbb{F}_q$
- $E(\mathbb{F}_q)$ means the group of points defined over $\mathbb{F}_q$ (coordinates $x, y \in \mathbb{F}_q$)

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6b,\ a_i \in \mathbb{F}_q,\ \Delta \neq 0$$

The *Frobenius map* in $\mathbb{F}_q$ is $x \mapsto x^q$.
The *Frobenius map* on E is

$$\begin{array}{rcl} \pi_q\colon E(\mathbb{F}_q) & \to & E(\mathbb{F}_q) \\ (x, y) & \mapsto (x^q, y^q) & \end{array}$$

Note that we use x^q, not x^p, otherwise $(x^p, y^p) \in E^p$ not $E^q = E$.

The *trace* of the endomorphism π_q is denoted t. It satisfies the Hasse bound:

$$-2\sqrt{q} \leq t \leq 2\sqrt{q} \iff t^2 - 4q \leq 0$$

The *curve order* is

$$\#E(\mathbb{F}_q) = q + 1 - t = \#\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q,\ (x, y) \in E\} \cup \{\mathcal{O}\}$$

Ordinary and supersingular curves

Let E an elliptic curve defined over a finite field $\mathbb{F}_q$, $q = p^\ell$ a prime power ($\ell = 1$ allowed):

- a *ordinary curve* is such that $t \neq 0 \bmod p$
- a *supersingular curve* meaning "super special" satisfies $t = 0 \bmod p$.

Textbook example:
$p = 3 \bmod 4$, $E\colon y^2 = x^3 + x$, $(x, y) \mapsto (-x, iy)$
$\#E(\mathbb{F}_p) = p + 1$, $t = 0$.

n-torsion points, isogenies, isomorphisms, j-invariant

A n-torsion point is such that its n-th multiple adds to the point at infinity, $[n]P = \mathcal{O}$.

$$E[n] = \{P \in E,\ [n]P = \mathcal{O}\}$$

Elliptic curves of the same order are *isogenous* but not necessary isomorphic.
Isomorphic curves are such that their *j-invariant* is equal:

$$E\colon y^2 = x^3 + ax + b,\ j(E) = \frac{4a^3}{4a^3 + 27b^2}$$

Public-key cryptography

Introduced in 1976 (Diffie–Hellman, DH) and 1977 (Rivest–Shamir–Adleman, RSA)
Asymmetric means distinct public and private keys

- encryption with a public key
- decryption with a private key
- deducing the private key from the public key is a very hard problem

Two hard problems:

- Integer factorization (for RSA)
- Discrete logarithm computation in a finite group (for Diffie–Hellman)

Discrete logarithm problem

$\mathbf{G}$ multiplicative group of order r
g generator, $\mathbf{G} = \{1, g, g^2, g^3, \ldots, g^{r-2}, g^{r-1}\}$

Given $h \in \mathbf{G}$, find integer $x \in \{0, 1, \ldots, r-1\}$ such that $h = g^x$.
Exponentiation easy: $(g, x) \mapsto g^x$
Discrete logarithm hard in well-chosen groups $\mathbf{G}$

Choice of group

Prime finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is a prime integer
Multiplicative group: $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$
Multiplication *modulo p*

Finite field $\mathbb{F}_{2^n} = \mathrm{GF}(2^n)$, $\mathbb{F}_{3^m} = \mathrm{GF}(3^m)$ for efficient arithmetic, now broken

Elliptic curves $E \colon y^2 = x^3 + ax + b / \mathbb{F}_p$

Diffie-Hellman key exchange

Alice **Bob**

Diffie-Hellman key exchange

Alice		**Bob**
$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$	public parameters	$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

Diffie-Hellman key exchange

Alice

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

secret key $\mathsf{sk}_A = a \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public value $\mathsf{PK}_A = g^a$

Bob

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

secret key $\mathsf{sk}_B = b \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public value $\mathsf{PK}_B = g^b$

Diffie-Hellman key exchange

Alice

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

secret key $\mathsf{sk}_A = a \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public value $\mathsf{PK}_A = g^a$

Bob

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

secret key $\mathsf{sk}_B = b \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public value $\mathsf{PK}_B = g^b$

PK_B

$\longleftrightarrow$

PK_A

Diffie-Hellman key exchange

Alice

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

secret key $\mathrm{sk}_A = a \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public value $\mathrm{PK}_A = g^a$

Bob

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

secret key $\mathrm{sk}_B = b \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public value $\mathrm{PK}_B = g^b$

PK_B ←→ PK_A

Alice: gets Bob's public key PK_B

$sk = {\mathrm{PK}_B}^a = g^{ab}$

Bob: gets Alice's public key PK_A

$sk = {\mathrm{PK}_A}^b = g^{ab}$

Asymmetric cryptography

Factorization (RSA cryptosystem)

Discrete logarithm problem (use in Diffie-Hellman, etc)

Given a finite cyclic group $(\mathbf{G}, \cdot)$, a generator g and $h \in \mathbf{G}$, compute x s.t. $h = g^x$.
$\rightarrow$ can we invert the exponentiation function $(g, x) \mapsto g^x$?

Common choice of $\mathbf{G}$:

- prime finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (1976)
- characteristic 2 field $\mathbb{F}_{2^n}$ ($\approx$ 1979)
- elliptic curve $E(\mathbb{F}_p)$ (1985)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in G$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#G\}$
- naive search, try them all: $\#G$ tests
- $O(\sqrt{\#G})$ generic algorithms

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in G$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#G\}$
- naive search, try them all: $\#G$ tests
- $O(\sqrt{\#G})$ generic algorithms
  - Shanks baby-step-giant-step (BSGS): $O(\sqrt{\#G})$, deterministic
  - random walk in G, cycle path finding algorithm in a connected graph (Floyd) $\rightarrow$ Pollard: $O(\sqrt{\#G})$, probabilistic
    (the cycle path encodes the answer)
  - parallel search (parallel Pollard, Kangarous)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in G$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#G\}$
- naive search, try them all: $\#G$ tests
- $O(\sqrt{\#G})$ generic algorithms
  - Shanks baby-step-giant-step (BSGS): $O(\sqrt{\#G})$, deterministic
  - random walk in G, cycle path finding algorithm in a connected graph (Floyd) $\rightarrow$ Pollard: $O(\sqrt{\#G})$, probabilistic
    (the cycle path encodes the answer)
  - parallel search (parallel Pollard, Kangarous)
- independent search in each distinct subgroup
  $+$ Chinese remainder theorem (Pohlig-Hellman)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

$\rightarrow$ choose G of large prime order (no subgroup)

$\rightarrow$ complexity of inverting exponentiation in $O(\sqrt{\#G})$

$\rightarrow$ security level 128 bits means $\sqrt{\#G} \geq 2^{128}$
take $\#G = 2^{256}$
analogy with symmetric crypto, keylength 128 bits (16 bytes)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $\rightarrow$ choose G of large prime order (no subgroup)
- $\rightarrow$ complexity of inverting exponentiation in $O(\sqrt{\#G})$
- $\rightarrow$ security level 128 bits means $\sqrt{\#G} \geq 2^{128}$
  take $\#G = 2^{256}$
  analogy with symmetric crypto, keylength 128 bits (16 bytes)

Use additional structure of G if any.
$\Longrightarrow$ Number Field Sieve algorithms.

Sony Play-Station 3 (PS3) hacking

- Revealed in 2010 at Chaos Communication Congress in Germany
- Problem of bad randomness in the *ephemeral key* of the ECDSA signature: Same one used to sign everything

→ With two valid signatures, the attackers can deduce Sony's private key then forge valid signatures themselves for anything

ECDSA signature, NIST FIPS 186-4, updated to 186-5 (February 3, 2023)

Domain parameters

- field size $q = p$ an odd prime or $q = 2^m$ a binary field
- elliptic curve parameters: curve type (Koblitz, binary, short Weierstrass, Montgomery), curve coefficients a, b,
- group $\mathbf{G}$ parameters: prime order $n = \#\mathbf{G}$, curve cofactor h, $G = (x_G, y_G)$ a generator of order n, optional *domain parameter seed*

Key pair (d, P) generation, secret d and public P

- generate a private secret random $0 < d < n$ (in the scalar field)
- compute the public key: curve point $P = [d]G$

ECDSA signature of a message m, under the private key d

- generate a new secret random ephemeral key $k \leftarrow \{1, \ldots, n-1\}$
- compute its inverse $k^{-1} \bmod n$
- compute $R = [k]G = (x_R, y_R)$ and set $r = x_R$
- compute the signature (r, s) with

$$s = k^{-1} \cdot (H(m) + r \cdot d) \bmod n$$

- securely erase k and k^{-1}

Moreover the standard specifies how to generate random ephemeral keys k_i and how to select a secure cryptographic hash function H.

ECDSA signature of a message m, under the private key d

- generate a new secret random ephemeral key $k \leftarrow \{1, \ldots, n-1\}$
- compute its inverse $k^{-1} \bmod n$
- compute $R = [k]G = (x_R, y_R)$ and set $r = x_R$
- compute the signature (r, s) with

$$s = k^{-1} \cdot (H(m) + r \cdot d) \bmod n$$

- securely erase k and k^{-1}

Moreover the standard specifies how to generate random ephemeral keys k_i and how to select a secure cryptographic hash function H.

Verify (r, s): with $P = [d]G$, check that Q has $x_Q = r \bmod n$, with

$$\begin{aligned} Q &= [s^{-1} \cdot H(m) \bmod n]G + [s^{-1} \cdot r \bmod n]P = (x_Q, y_Q) \\ &= [s^{-1}(H(m) + r \cdot d)]G \stackrel{?}{=} R = [k]G \end{aligned}$$

PS3 attack (2010)

Same ephemeral key k used to sign different messages, say m_1, m_2

- $(r, s_1 = k^{-1} \cdot (H(m_1) + r \cdot d) \bmod n)$
- $(r, s_2 = k^{-1} \cdot (H(m_2) + r \cdot d) \bmod n)$

Recover the private key d

- compute the difference $s_1 - s_2 = k^{-1} \cdot (H(m_1) - H(m_2)) \bmod n$
- the secret part $r \cdot d$ vanished!
- publicly compute $H(m_1) - H(m_2) \bmod n$ and recover the ephemeral secret key

$$k = (s_1 - s_2)^{-1} \cdot (H(m_1) - H(m_2)) \bmod n$$

- from (r, s_1) and k, recover $d = (k \cdot s_1 - H(m_1)) \cdot r^{-1} \bmod n$

Knowing the manufacturer's private key d allows anyone to sign any non-legitimate documents (software, games for the PS3). The signature will be accepted as valid by any verifier.

Credits

- Rémi Clarisse PhD thesis at tel-03506116
- Jérémie Detrey for many slides and support from ARCHI'2017 summer school
- Laurent Imbert for slides from ECC'11 summer school
- Simon Masson for the graph on page 20 from his PhD thesis
- Christophe Ritzenthaler for ressources at his webpage
- Emmanuel Thomé and Cyril Bouvier for slides from a winter school at ISI Delhi in 2017
- Ben Smith for his slides from MPRI