Elliptic curves, number theory and cryptography
Week 2, Lecture 2

Aurore Guillevic

Aarhus University

Spring semester, 2022
Outline

Projective space and the point at infinity

Projective space $\mathbb{P}^2$ as $\mathbb{A}^2 \times \mathbb{P}^1$

Multiplicity of intersection and Bézout theorem

Associativity of the addition law

Scalar multiplication on elliptic curves

Recap on complexity

The Discrete Log Problem in cryptography
\[ P + (-P) \]
$P + (-P)$
\( P + (-P) \)
$P + (-P)$
$P + (-P)$

$L_{R',0} = L_{P,0}$

The graph shows a point $P$ and its reflection $R'$ with respect to the origin $O$, illustrating the concept of vector addition and reflection in a coordinate system.
$P + (-P)$

$L_{R', O} = L_{P, O}$

$P + O = P$

$R'$

$O$
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

\[ E/\mathbb{R} : y^2 = x^3 - 3x + 1 \]
Projective space and point at infinity

\[ \mathbb{P} / \mathbb{R} : y^2 = x^3 - 3x + 1 \]
Projective space and point at infinity

\[ E/K : y^2 = x^3 + Ax + B \quad \text{Char}(K) \neq 2, 3 \]

Affine plane (Euclidean plane) over a field \( K \)

\[ \mathbb{A}^2(K) = \{(x, y) : x, y \in K\} \]

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 \( P_\infty \) is the point at infinity.

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

Projective space

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

\[
\mathbb{P}^n(K) = \left\{ (X_0, X_1, \ldots, X_n) \in K^{n+1} \mid (X_0, X_1, \ldots, X_n) \neq 0 = (0, 0, \ldots, 0) \right\} / \sim
\]

with the equivalence relation \((X_0, X_1, \ldots, X_n) \sim (X'_0, X'_1, \ldots, X'_n) \iff \text{there exists } \lambda \neq 0 \in K \text{ such that } (X_0, X_1, \ldots, X_n) = (\lambda X'_0, \lambda X'_1, \lambda \ldots, X'_n)\).

The **equivalence class** w.r.t. \( \sim \) is denoted \((X_0 : X_1 : \ldots : X_n)\)

with colons instead of commas.
Outline

Projective space and the point at infinity

**Projective space** $\mathbb{P}^2$ as $\mathbb{A}^2 \times \mathbb{P}^1$

Multiplicity of intersection and Bézout theorem

Associativity of the addition law

Scalar multiplication on elliptic curves

Recap on complexity

The Discrete Log Problem in cryptography
Homogenization

A polynomial \( f \in K[x, y] \) defines a plane curve \( C_0 \) in \( \mathbb{A}^2(K) \)
→ a **homogeneous polynomial** \( F \in K[X, Y, Z] \) defines
a projective plane curve \( C \) in \( \mathbb{P}^2(K) \)

**Degree of a bivariate polynomial**

Let the degree \( d = \deg f \) to be the largest value \( i + j \) of the (non-zero) monomials
\( x^i y^j \) of \( f \):

\[
f = \sum_{i, j: \ a_{ij} \neq 0} a_{ij} x^i y^j, \quad d = \max_{i, j: \ a_{ij} \neq 0} i + j .
\]
Homogenization

Homogenization of a polynomial

The **homogenization** of \( f(x, y) = \sum_{i,j: \ a_{ij} \neq 0} a_{ij}x^iy^j \in K[x, y] \) is

\[
F(X, Y, Z) = \sum_{i,j: \ a_{ij} \neq 0} a_{ij}X^i Y^j Z^{d-i-j}, \text{ where } d = \deg(f).
\]

Equivalently (Washington’s book 2.3 page 19),

\[
F(X, Y, Z) = Z^d f \left( \frac{X}{Z}, \frac{Y}{Z} \right), \text{ where } d = \deg(f).
\]

From this definition we have

- \( F \) is homogeneous of degree \( d \);
- \( F(x, y, 1) = f(x, y) \);
- \( F(x, y, 0) \neq 0 \), and
- \( F(X, Y, Z) = 0 \) does not contain the line at infinity
Why homogenization?

(slide added to answer a question)

In the projective space, a point $P(X_0, Y_0, Z_0)$ has many possible representations:

$$P = (\lambda X_0, \lambda Y_0, \lambda Z_0) \text{ for any scalar } \lambda \neq 0$$

$P \in C$ a curve of $\mathbb{P}^2$ $\implies$ $P$ is a zero of a polynomial $F(X, Y, Z)$.

But then we require $F(\lambda X_0, \lambda Y_0, \lambda Z_0) = 0$ for all $\lambda \neq 0$.

Thanks to homogenization, we have

$$F(\lambda X_0, \lambda Y_0, \lambda Z_0) = \lambda^d F(X_0, Y_0, Z_0)$$

hence

$$P \in C \iff F(X_0, Y_0, Z_0) = 0 \iff F(\lambda X_0, \lambda Y_0, \lambda Z_0) = 0 \forall \lambda \neq 0$$
A projective plane curve is smooth

Let $E: F(X, Y, Z) = 0$ over a field $K$, where $F$ is a homogeneous polynomial. There is no singular point $(X_0, Y_0, Z_0)$ such that

$$
\begin{align*}
\frac{\partial F}{\partial X}(X_0, Y_0, Z_0) &= 0 \\
\frac{\partial F}{\partial Y}(X_0, Y_0, Z_0) &= 0 \\
\frac{\partial F}{\partial Z}(X_0, Y_0, Z_0) &= 0
\end{align*}
$$

where $\partial F/\partial X$, $\partial F/\partial Y$, $\partial F/\partial Z$ are the partial derivatives.
A line in $\mathbb{P}^2(K)$

Affine plane (Euclidean plane) over a field $K$

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

A line in the affine plane $\mathbb{A}^2(K)$ is defined by an equation of the form

$\mathcal{L}: ax + by + c = 0$, with $(a, b, c) \neq (0, 0, 0)$.

Applying the homogenization formula, one has:

Projective Line

A **projective line** in $\mathbb{P}^2(K)$ has an equation of the form

$\mathcal{L}: aX + bY + cZ = 0$, with $(a, b, c) \neq (0, 0, 0)$.

• Two distinct points of $\mathbb{A}^2$ determine a line in $\mathbb{A}^2$
• two lines of $\mathbb{A}^2$ determine one point in $\mathbb{A}^2$ unless they are parallel.

The projective plane will contain the intersection point of parallel lines at infinity.
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 \( \mathcal{O} \)
Points at infinity

The **Points at infinity** in the projective plane $\mathbb{P}^2(K)$ correspond to **directions** of parallel lines in $\mathbb{A}^2(K)$

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{\text{the directions in } \mathbb{A}^2\}$$

where *direction* is not oriented, like the slope of a line.

The set of directions in $\mathbb{A}^2$ is

$$\{(x, y) \in K^2\} / \sim$$

where $(x, y) \sim (x', y') \iff \exists \lambda \neq 0 \in K, (x, y) = (\lambda x, \lambda y)$.

We have

$$\mathbb{P}^2(K) = \mathbb{A}^2(K) \cup \mathbb{P}^1(K)$$
Correspondence of $\mathbb{A}^2 \cup \mathbb{P}^1$ and $\mathbb{P}^2$

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

\[ \mathbb{P}^2(K) \leftrightarrow \mathbb{A}^2(K) \cup \mathbb{P}^1(K) \]

\[ (X, Y, Z) \mapsto \begin{cases} 
\left( \frac{X}{Z}, \frac{Y}{Z} \right) \in \mathbb{A}^2(K) & \text{if } Z \neq 0 \\
(X, Y) \in \mathbb{P}^1(K) & \text{if } Z = 0
\end{cases} \]

\[ (x, y, 1) \leftrightarrow (x, y) \in \mathbb{A}^2(K) \]

\[ (X, Y, 0) \leftrightarrow (X, Y) \in \mathbb{P}^1(K) \]
A projective plane cubic curve $C$ in $\mathbb{P}^2(K)$ is given by an equation

$$C: F(X, Y, Z) = 0$$

where $F$ is a homogeneous polynomial of degree 3.

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

$$E: Y^2Z = X^3 + aXZ^2 + bZ^3, \quad 4a^3 + 27b^2 \neq 0$$

and the group of points on $E$ is

$$E(K) = \{(X, Y, Z) \in \mathbb{P}^2(K) : F_E(X, Y, Z) = 0\}$$
Point at infinity in the Projective Plane

\[ \mathcal{E}: Y^2Z = X^3 + aXZ^2 + bZ^3, \quad 4a^3 + 27b^2 \neq 0 \]

\[ Z = 0 \implies \mathcal{E}: 0 = X^3 \]

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 \( Q(x_2, y_2) = (X_2/Z_2, Y_2/Z_2) \).

The line \( \mathcal{L} \) through \( P \) and \( Q \) has slope \( \lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{Y_2Z_1 - Y_1Z_2}{X_2Z_1 - X_1Z_2} \)

If \( P = Q \) then \( \lambda = (3x_1^2 + a)/(2y_1) = (3X_1^2 + aZ_1^2)/(2Y_1Z_1) \)
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 $P_1 = (X_1, Y_1, Z_1)$ and $P_2 = (X_2, Y_2, Z_2)$ be two points on

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

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 $(P_1, P_2)$ is given by

$$\lambda = \begin{cases} 
\frac{Y_2Z_1 - Y_1Z_2}{X_2Z_1 - X_1Z_2} & \text{if } P_1 \neq \pm P_2 \\
\frac{3X_1 + aZ_1}{2Y_1} & \text{if } P_1 = P_2 \text{ and } Y_1 \neq 0 
\end{cases}$$
Addition law in projective coordinates in \( \mathbb{P}^2(K) \)

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

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

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

\[
\begin{align*}
w &= aZ_1^2 + 3X_1^2 \\
s &= Y_1 \cdot Z_1 \\
B &= X_1 \cdot Y_1 \cdot s \\
h &= w^2 - 8B \\
X_3 &= 2h \cdot s \\
Y_3 &= w \cdot (4B - h) - 8 \cdot (Y_1s)^2 \\
Z_3 &= 8s^3
\end{align*}
\]

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 $Q = -P_1 = (X_1, -Y_1, Z_1)$ with $Y_1 \neq 0$ then the addition formula computes 

$$(X_3, Y_3, Z_3) = (0, Y_3, 0) \text{ and } Y_3 = 8Y_1^3Z_1^5 \neq 0$$

This is the point at infinity $\mathcal{O}$, without division by 0.

If $P_1(X_1, 0, Z_1)$ 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
- ... 

→ EFD contains almost all of them.
Outline

Projective space and the point at infinity

Projective space $\mathbb{P}^2$ as $\mathbb{A}^2 \times \mathbb{P}^1$

Multiplicity of intersection and Bézout theorem

Associativity of the addition law

Scalar multiplication on elliptic curves

Recap on complexity

The Discrete Log Problem in cryptography
Étienne Bézout

French mathematician (1730 – 1783)
Scientist in the Navy

You can read about Bézout’s theorem on Wikipedia at this link: https://en.wikipedia.org/wiki/B%C3%A9zout%27s_theorem

https://mathshistory.st-andrews.ac.uk/Biographies/Bezout/pictdisplay/
Multiplicity of intersection

Let \( C \) and \( C' \) be two projective plane curves with no common component, that is they are defined by homogeneous polynomials \( F \) and \( G \) with no common factor. The **Multiplicity of intersection** of \( C \) and \( C' \) at \( P \in \mathbb{P}^2 \) is the unique integer \( I_P(C, C') \geq 0 \) such that

1. \( I_P(C, C') = 0 \iff P \notin C \cap C' \)

2. If \( P \in C_1 \cap C_2 \), if \( P \) is a non-singular point of \( C_1 \) and \( C_2 \), and if \( C_1 \) and \( C_2 \) have different tangent directions at \( P \), then \( I_P(C_1, C_2) = 1 \)

   One often says in this case that \( C_1 \) and \( C_2 \) intersect *transversally* at \( P \).

3. If \( P \in C_1 \cap C_2 \) and if \( C_1 \) and \( C_2 \) do not intersect transversally at \( P \), then \( I_P(C_1, C_2) \geq 2 \).
Bézout’s theorem

Silverman–Tate book appendix A.
Let $C_1$ and $C_2$ be projective curves with no common component. Then

$$\sum_{P \in C_1 \cap C_2} I_P(C_1, C_2) = (\deg C_1)(\deg C_2),$$

where the sum is over all points of $C_1 \cap C_2$ in the algebraically closed field $K$ (e.g. $\mathbb{C}$ or $\overline{\mathbb{F}_p}$).

In particular, if $C_1$ and $C_2$ are smooth curves with only transversal intersections, then $\#C_1 \cap C_2 = (\deg C_1)(\deg C_2)$; and in all cases there is an inequality

$$\#(C_1 \cap C_2) \leq (\deg C_1)(\deg C_2)$$
Outline

Projective space and the point at infinity

Projective space $\mathbb{P}^2$ as $\mathbb{A}^2 \times \mathbb{P}^1$

Multiplicity of intersection and Bézout theorem

Associativity of the addition law

Scalar multiplication on elliptic curves

Recap on complexity

The Discrete Log Problem in cryptography
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: 

$$(P + Q) + R = P + (Q + R)$$
Idea of the proof using Bézout’s theorem

This will NOT be in the exam
From Bézout’s theorem, two distinct cubic projective plane curves without a common component have exactly 9 intersection points.

Theorem A
Let $C$, $C_1$ and $C_2$ be three cubic curves. Suppose $C$ goes through eight of the nine intersection points of $C_1$ and $C_2$. Then $C$ goes through the ninth intersection point.
Idea of the proof using Bézout’s theorem

Let’s consider an elliptic curve $C$ and the eight points

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

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

\[ -((P + Q) + R) = -(P + (Q + R)). \]
Idea of the proof using Bézout's theorem

Let $C_1$ be defined by the equations of the three lines through the nine distinct points $P, Q, -(P + Q) \in \ell_{P,Q}$, the vertical $-(Q + R), Q + R, O \in v_{Q+R}$, and $R, (P + Q), -(P + Q + R) \in \ell_{P+Q,R}$ multiplied together:

$$C_1: F_1(X, Y, Z) = \ell_{P,Q} \cdot v_{Q+R} \cdot \ell_{P+Q,R} = 0$$
Idea of the proof using Bézout's theorem

Let $\mathcal{C}_1$ be defined by the equations of the three lines through the nine distinct points $P, Q, -(P + Q) \in \ell_{P,Q}$, the vertical $-(Q + R), Q + R, \mathcal{O} \in v_{Q+R}$, and $R, (P + Q), -((P + Q) + R) \in \ell_{P+Q,R}$ multiplied together:

$$\mathcal{C}_1: F_1(X, Y, Z) = \ell_{P,Q} \cdot v_{Q+R} \cdot \ell_{P+Q,R} = 0$$

Let $\mathcal{C}_2$ be defined by the equations of the three lines through the nine distinct points $Q, R, -(Q + R) \in \ell_{Q,R}$, the vertical $P + Q, -(P + Q), \mathcal{O} \in v_{P+Q}$, and $P, Q + R, -(P + (Q + R)) \in \ell_{P,Q+R}$ multiplied together:

$$\mathcal{C}_2: F_2(X, Y, Z) = \ell_{Q,R} \cdot v_{P+Q} \cdot \ell_{P,Q+R} = 0$$
Idea of the proof using Bézout’s theorem

Let $C_1$ be defined by the equations of the three lines through the nine distinct points $P, Q, -(P + Q) \in \ell_{P, Q}$, the vertical $-(Q + R), Q + R, O \in v_{Q+R}$, and $R, (P + Q), -((P + Q) + R) \in \ell_{P+Q,R}$ multiplied together:

$$C_1 : F_1(X, Y, Z) = \ell_{P,Q} \cdot v_{Q+R} \cdot \ell_{P+Q,R} = 0$$

Let $C_2$ be defined by the equations of the three lines through the nine distinct points $Q, R, -(Q + R) \in \ell_{Q,R}$, the vertical $P + Q, -(P + Q), O \in v_{P+Q}$, and $P, Q + R, -(P + (Q + R)) \in \ell_{P,Q+R}$ multiplied together:

$$C_2 : F_2(X, Y, Z) = \ell_{Q,R} \cdot v_{P+Q} \cdot \ell_{P,Q+R} = 0$$

Then $C_1$ and $C_2$ are two cubic curves of $\mathbb{P}^2$ that intersect at nine distinct points, namely the known

$$P, Q, R, O, -(P + Q), P + Q, -(Q + R), (Q + R) \in C_1 \cap C_2$$

and a ninth intersection point $P_9 \in C_1 \cap C_2$. 
Idea of the proof using Bézout's theorem

Now $C$ is a curve that goes to the first eight points

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

Hence by Theorem A it also goes through the 9-th point of $C_1 \cap C_2$.
Thus the ninth intersection point of $C_1$ and $C_2$ lies on $C$: $P_9 \in C_1 \cap C_2$, $P_9 \in C$. 
Idea of the proof using Bézout's theorem

Now $C$ is a curve that goes to the first eight points

$$P, Q, R, O, -(P + Q), P + Q, -(Q + R), (Q + R) \in C$$

Hence by Theorem A it also goes through the 9-th point of $C_1 \cap C_2$.
Thus the ninth intersection point of $C_1$ and $C_2$ lies on $C$: $P_9 \in C_1 \cap C_2$, $P_9 \in C$.

Both $-((P + Q) + R) \in C_1$ and $-(P + (Q + R)) \in C_2$ also lies on $C$ by construction.
Hence $-((P + Q) + R), P_9 \in C \cap C_1$ and $-(P + (Q + R)), P_9 \in C \cap C_2$
Idea of the proof using Bézout’s theorem

Now $C$ is a curve that goes to the first eight points

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

Hence by Theorem A it also goes through the 9-th point of $C_1 \cap C_2$.
Thus the ninth intersection point of $C_1$ and $C_2$ lies on $C$: $P_9 \in C_1 \cap C_2$, $P_9 \in C$.

Both $-((P + Q) + R) \in C_1$ and $-(P + (Q + R)) \in C_2$ also lies on $C$ by construction.
Hence $-((P + Q) + R), P_9 \in C \cap C_1$ and $-(P + (Q + R)), P_9 \in C \cap C_2$

But by Bézout’s theorem, $\#(C \cap C_1) \leq 9$ and $\#(C \cap C_2) \leq 9$ as cubic curves,
Idea of the proof using Bézout’s theorem

Now $C$ is a curve that goes to the first eight points

$$P, Q, R, O, -(P + Q), P + Q, -(Q + R), (Q + R) \in C$$

Hence by Theorem A it also goes through the 9-th point of $C_1 \cap C_2$.

Thus the ninth intersection point of $C_1$ and $C_2$ lies on $C$: $P_9 \in C_1 \cap C_2$, $P_9 \in C$.

Both $-((P + Q) + R) \in C_1$ and $-(P + (Q + R)) \in C_2$ also lies on $C$ by construction.

Hence $-((P + Q) + R), P_9 \in C \cap C_1$ and $-(P + (Q + R)), P_9 \in C \cap C_2$

But by Bézout’s theorem, $\#(C \cap C_1) \leq 9$ and $\#(C \cap C_2) \leq 9$ as cubic curves, so finally

$$P_9 = -(P + (Q + R)) = -((P + Q) + R) .$$
Proof of Theorem A

Theorem A
Let $C, C_1$ and $C_2$ be three cubic curves. Suppose $C$ goes through eight of the nine intersection points of $C_1$ and $C_2$. Then $C$ goes through the ninth intersection point.

This will NOT be in the exam
Let $C_1$ and $C_2$ be two distinct cubic smooth plane curves without a common component.
By Bézout’s theorem, $C_1$ and $C_2$ intersect at exactly 9 points $P_1, \ldots, P_9$.
Consider the 9 distinct points $P_1, \ldots, P_9$ in $\mathbb{P}^2(K)$.

Let $C'$ be another cubic smooth plane curve going through the first eight points $P_1, \ldots, P_8$.
We will show that $C'$ also goes through $P_9$. 
Consider a generic cubic projective plane curve $C: F(X, Y, Z) = 0$ given by a homogeneous irreducible degree 3 polynomial

$$F = a_0 + a_1 XZ^2 + a_2 X^2 Z + a_3 X^3 + a_4 YZ^2 + a_5 Y^2 Z + a_6 Y^3 + a_7 XYZ + a_8 X^2 Y + a_9 X Y^2$$

with 10 parameters $\{a_i\}_{0 \leq i \leq 9}$. 
Proof of Theorem A

Consider a generic cubic projective plane curve \( C: F(X, Y, Z) = 0 \) given by a homogeneous irreducible degree 3 polynomial

\[
F = a_0 + a_1 XZ^2 + a_2 X^2 Z + a_3 X^3 + a_4 YZ^2 + a_5 Y^2 Z + a_6 Y^3 + a_7 XYZ + a_8 X^2 Y + a_9 XY^2
\]

with 10 parameters \( \{a_i\}_{0 \leq i \leq 9} \).

\( P_1 \in C \implies \) an equation \( F(X_1, Y_1, Z_1) = 0 \) forces a condition on the \( a_i \)s.
Proof of Theorem A

Consider a generic cubic projective plane curve $C: F(X, Y, Z) = 0$ given by a homogeneous irreducible degree 3 polynomial

$$F = a_0 + a_1 X Z^2 + a_2 X^2 Z + a_3 X^3 + a_4 Y Z^2 + a_5 Y^2 Z + a_6 Y^3 + a_7 X Y Z + a_8 X^2 Y + a_9 X Y^2$$

with 10 parameters $\{a_i\}_{0 \leq i \leq 9}$.

$P_1 \in C \implies$ an equation $F(X_1, Y_1, Z_1)$ forces a condition on the $a_i$s. Going through the 8 points $P_1, \ldots, P_8$ forces 8 conditions on the $a_i$s.
Proof of Theorem A

Consider a generic cubic projective plane curve $C: F(X, Y, Z) = 0$ given by a homogeneous irreducible degree 3 polynomial

$$F = a_0 + a_1 XZ^2 + a_2 X^2 Z + a_3 X^3 + a_4 YZ^2 + a_5 Y^2 Z + a_6 Y^3 + a_7 XYZ + a_8 X^2 Y + a_9 XY^2$$

with 10 parameters $\{a_i\}_{0 \leq i \leq 9}$.

$P_1 \in C \implies$ an equation $F(X_1, Y_1, Z_1)$ forces a condition on the $a_i$s.

Going through the 8 points $P_1, \ldots, P_8$ forces 8 conditions on the $a_i$s.

The set of $\{a_i\}_{0 \leq i \leq 9}$ is a $K$-vector space of dimension 10, and the 8 conditions $P_i \in C \iff F(X_i, Y_i, Z_i) = 0$ make it a $K$-vector space of dim 2.
Proof of Theorem A

Let \((F_\lambda, F_\mu)\) a basis of this 2-dimensional vector space. \(F_\lambda, F_\mu\) are homogeneous polynomials of degree 3 and linearly independents. They define curves \(\mathcal{F}_\lambda\) and \(\mathcal{F}_\mu\).
Proof of Theorem A

Let \((F_\lambda, F_\mu)\) a basis of this 2-dimensional vector space. \(F_\lambda, F_\mu\) are homogeneous polynomials of degree 3 and linearly independents. They define curves \(\mathcal{F}_\lambda\) and \(\mathcal{F}_\mu\).

The former generic cubic curve \(C'\) defined by \(F'(X, Y, Z)\) goes through \(P_1, \ldots, P_8\). We have \(F'(X_i, Y_i, Z_i) = 0\) for all \(1 \leq i \leq 8\). We also have \(F' = \lambda F_\lambda + \mu F_\mu\) for a choice of \(\lambda, \mu \in K\) as \(F_\lambda, F_\mu\) form a basis.
Proof of Theorem A

Let \((F_\lambda, F_\mu)\) a basis of this 2-dimensional vector space.
\(F_\lambda, F_\mu\) are homogeneous polynomials of degree 3 and linearly independents.
They define curves \(\mathcal{F}_\lambda\) and \(\mathcal{F}_\mu\).

The former generic cubic curve \(C'\) defined by \(F'(X, Y, Z)\) goes through \(P_1, \ldots, P_8\).
We have \(F'(X_i, Y_i, Z_i) = 0\) for all \(1 \leq i \leq 8\).
We also have \(F' = \lambda F_\lambda + \mu F_\mu\) for a choice of \(\lambda, \mu \in K\) as \(F_\lambda, F_\mu\) form a basis.

By Bézout’s theorem, \(\mathcal{F}_\lambda\) and \(\mathcal{F}_\mu\) being two general cubic curves, they have 
\((\deg \mathcal{F}_\lambda)(\deg \mathcal{F}_\mu) = 9\) points of intersection, counting multiplicities.
Proof of Theorem A

But actually we know explicitly a basis for this 2-dim vector space: \( C_1 \) and \( C_2 \) that are distinct and go to \( P_1, \ldots, P_8 \).
So a basis is actually \( F_1, F_2 \) and \( F = \nu_1 F_1 + \nu_2 F_2 \) with
\( C_1 : F_1(X, Y, Z) = 0 \) and \( C_2 : F_2(X, Y, Z) = 0 \).
But actually we know explicitly a basis for this 2-dim vector space: \( C_1 \) and \( C_2 \) that are distinct and go to \( P_1, \ldots, P_8 \).

So a basis is actually \( F_1, F_2 \) and \( F = \nu_1 F_1 + \nu_2 F_2 \) with \( C_1: F_1(X, Y, Z) = 0 \) and \( C_2: F_2(X, Y, Z) = 0 \).

And moreover \( P_9 \in C_1 \cap C_2 \implies F_1(P_9) = 0 = F_2(P_9) \)

Because \( C' \) is defined by \( F' = \nu_1 F_1 + \nu_2 F_2 \), then evaluating at \( P_9 \), we get \( F'(P_9) = 0 \) and \( C' \) also goes through \( P_9 \).
Other approaches

In Washington’s book Section 2.4, looking carefully at polynomials and again intersection multiplicities. Alternatively: with resultants of polynomials.

Further optional reading on the topic:
- Washington’s book Section 2.4 pages 20 to 32;
- Silverman–Tate book Appendix A.
Outline

Projective space and the point at infinity

Projective space $\mathbb{P}^2$ as $\mathbb{A}^2 \times \mathbb{P}^1$

Multiplicity of intersection and Bézout theorem

Associativity of the addition law

Scalar multiplication on elliptic curves

Recap on complexity

The Discrete Log Problem in cryptography
Scalar multiplication

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

Scalar multiplication (exponentiation)

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

$$[m]: \mathcal{E} \rightarrow \mathcal{E}$$

$$P \mapsto P + \ldots + P$$

$m$ copies of $P$

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

- 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 $\mathcal{E}$. 
Naive Scalar multiplication: Double-and-Add

**Input:** \( E \) defined over a field \( K \), \( m > 0 \), \( P \in \mathcal{E}(K) \)

**Output:** \([m]P \in \mathcal{E}\)

1. **if** \( m = 0 \) **then** **return** \( \mathcal{O} \)

2. Write \( m \) in binary expansion \( m = \sum_{i=0}^{n-1} b_i 2^i \) where \( b_i \in \{0, 1\} \)

3. \( R \leftarrow P \)

4. **for** \( i = n - 2 \) **dowto** 0 **do**

   - Loop invariant: \( R = \lfloor m/2^i \rfloor P \)

5. \( R \leftarrow [2]R \)

6. **if** \( b_i = 1 \) **then**

7. \( R \leftarrow R + P \)

8. **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 INTEGRER TIMES A POINT p.18, the LSB-first algorithm is given, disadvantage: one extra temporary variable.
Outline

Projective space and the point at infinity

Projective space $\mathbb{P}^2$ as $\mathbb{A}^2 \times \mathbb{P}^1$

Multiplicity of intersection and Bézout theorem

Associativity of the addition law

Scalar multiplication on elliptic curves

Recap on complexity

The Discrete Log Problem in cryptography
Outline

Projective space and the point at infinity

Projective space $\mathbb{P}^2$ as $\mathbb{A}^2 \times \mathbb{P}^1$

Multiplicity of intersection and Bézout theorem

Associativity of the addition law

Scalar multiplication on elliptic curves

Recap on complexity

The Discrete Log Problem in cryptography
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

$G$ multiplicative group of order $r$

g generator, $G = \{1, g, g^2, g^3, \ldots, g^{r-2}, g^{r-1}\}$

Given $h \in G$, 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 $G$
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** $\mathbb{F}_{2^n} = \text{GF}(2^n)$, $\mathbb{F}_{3^m} = \text{GF}(3^m)$ for efficient arithmetic, now broken

**Elliptic curves** $E: y^2 = x^3 + ax + b/\mathbb{F}_p$
Diffie-Hellman key exchange

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>\text{public parameters}</td>
<td>\text{public parameters}</td>
</tr>
<tr>
<td>$\text{secret key } s_k^A = a \leftarrow \mathbb{Z}/r\mathbb{Z}$</td>
<td>$\text{secret key } s_k^B = b \leftarrow \mathbb{Z}/r\mathbb{Z}$</td>
</tr>
<tr>
<td>$\text{public value } PK^A = g^a$</td>
<td>$\text{public value } PK^B = g^b$</td>
</tr>
<tr>
<td>$PK^A$ gets Alice's public key $PK^A$</td>
<td>$PK^B$ gets Bob's public key $PK^B$</td>
</tr>
<tr>
<td>$s_k^A = PK^B$</td>
<td>$s_k^B = PK^A$</td>
</tr>
<tr>
<td>$g^{ab}$</td>
<td>$g^{ab}$</td>
</tr>
</tbody>
</table>
Diffie-Hellman key exchange

Alice
$(G, \cdot), g, r = \#G$ public parameters

Bob
$(G, \cdot), g, r = \#G$
Diffie-Hellman key exchange

Alice

\((G, \cdot), g, r = \#G\)

secret key \(sk_A = a \leftarrow (\mathbb{Z}/r\mathbb{Z})^*\)

public value \(PK_A = g^a\)

Bob

\((G, \cdot), g, r = \#G\)

secret key \(sk_B = b \leftarrow (\mathbb{Z}/r\mathbb{Z})^*\)

public value \(PK_B = g^b\)
Diffie-Hellman key exchange

**Alice**

\[(G, \cdot), g, r = \#G\]

- Secret key: \(sk_A = a \leftarrow (\mathbb{Z}/r\mathbb{Z})^*\)
- Public value: \(PK_A = g^a\)

**Bob**

\[(G, \cdot), g, r = \#G\]

- Secret key: \(sk_B = b \leftarrow (\mathbb{Z}/r\mathbb{Z})^*\)
- Public value: \(PK_B = g^b\)
Diffie-Hellman key exchange

**Alice**

$(G, \cdot), g, r = \#G$

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

public value $PK_A = g^a$

gets Bob's public key $PK_B$

$sk = PK_B^a = g^{ab}$

**Bob**

$(G, \cdot), g, r = \#G$

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

public value $PK_B = g^b$

gets Alice's public key $PK_A$

$sk = PK_A^b = g^{ab}$
Asymmetric cryptography

Factorization (RSA cryptosystem)

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

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

Common choice of \(G\):
- prime finite field \(\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}\) (1976)
- characteristic 2 field \(\mathbb{F}_{2^n}\) (≈ 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 \((g, x) \mapsto g^x\)?

→ choose \(G\) of large prime order (no subgroup)
→ complexity of inverting exponentiation in \(O(\sqrt{|G|})\)
→ security level 128 bits means \(\sqrt{|G|} \geq 2^{128}\)
  
  take \(|G| = 2^{256}\)

analogy with symmetric crypto, keylength 128 bits (16 bytes)
How fast can we invert the exponentiation function \((g, x) \mapsto g^x\)?

- choose \(G\) of large prime order (no subgroup)
- complexity of inverting exponentiation in \(O(\sqrt{\#G})\)
- 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.

\(\Rightarrow\) Number Field Sieve algorithms.
Credits

- Rémi Clarisse PhD thesis at tel-03506116
- Jérémie Detrey summer school lecture at ARCHI’2017 summer school