Topics in Algebra: Cryptography

Univ.-Prof. Dr. Goulnara ARZHANTSEVA

WS 2018

universität wien

Weierstrass equation

Let $\mathbf{k}$ be a field.

Weierstrass equations

The affine Weierstrass equation:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbf{k}.$$

The homogeneous Weierstrass equation:

$$E^*: y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, a_i \in \mathbf{k}.$$

The vanishing set:

$$E(\mathbf{k}) = \{(x : y : z) \in \mathbb{P}^2 \text{ so that } x, y, z \in \mathbf{k} \text{ is a solution of } E^*\} \subseteq \mathbb{P}^2$$

The defining polynomial:

$$F^*: y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3), a_i \in \mathbf{k}.$$

Elliptic curves

Definition: Elliptic curve

E is elliptic if E is smooth.

Normal forms

1. If $\operatorname{char}\mathbf{k} \neq 2$ then in E substitute $y \mapsto y - \frac{a_1x+a_3}{2}$ obtaining

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

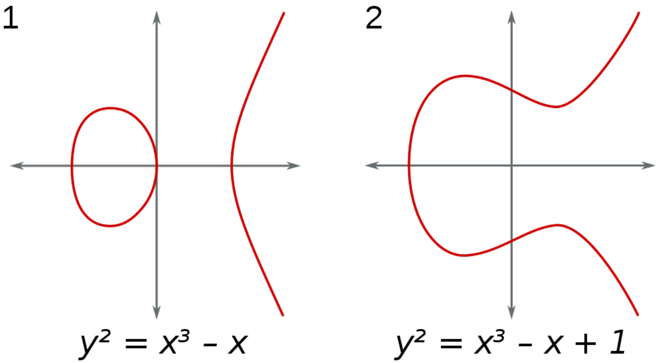
2. If $\operatorname{char}\mathbf{k} \neq 2, 3$ then substitute $x \mapsto x - \frac{1}{3}a_2',\ a_2' = a_2 + \frac{a_1^2}{4}$ obtaining

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

$\operatorname{char}\mathbf{k} \neq 2, 3 : \operatorname{disc}(x^3 + ax + b) = -16(4a^3 + 27b^2)$

$\operatorname{char}\mathbf{k} \neq 2,\ y^2 = f(x) = x^3 + a_2'x^2 + a_4'x + a_6'$ is singular $\iff \operatorname{disc} f = 0$

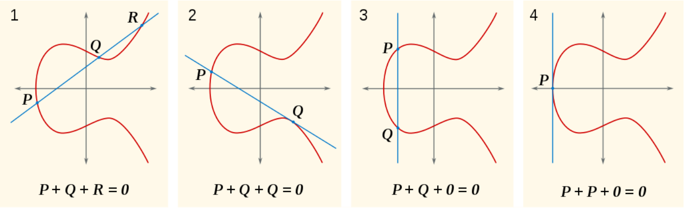
Elliptic curves



Elliptic curves in normal form [image: Wikipedia]

Elliptic curve: The group structure $(E(\overline{\mathbf{k}}), +)$

$\mathbf{k}$ a field, $\overline{\mathbf{k}}$ its algebraic closure, $\mathcal{O} = (0 : 1 : 0) \in E(\overline{\mathbf{k}})$ the point at ∞



Group structure on the $\mathbb{R}$-points of $E : y^2 = x^3 - x + 1$ [image: Wikipedia]

Group structure: collinear triples sum to $\mathcal{O}$.

Elliptic curve: The group structure $(E(\overline{\mathbf{k}}), +)$

$\mathbf{k}$ a field, $\overline{\mathbf{k}}$ its algebraic closure.

$E(\overline{\mathbf{k}})$ is the projective algebraic set defined by a homogeneous Weierstrass equation over the algebraic closure of the field.

An elliptic curve always contains the point at infinity, which is the neutral element in the corresponding abelian group.

An elliptic curve is a special case of a plane algebraic curve.

We can view the addition geometrically, algebraically, and analytically.

Elliptic curve and projective lines

The defining polynomial:

$F^*: y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3), a_i \in \mathbf{k}.$

Let $L = \{(x : y : z) \mid ax + by + cz = 0\} \subset \mathbb{P}^2(\bar{\mathbf{k}})$ be a projective line with $(a, b, c) \neq (0, 0, 0)$

Theorem: Intersection of E with a projective line

Let $L \subset \mathbb{P}^2(\bar{\mathbf{k}})$ be a projective line. Then $|L \cap E(\bar{\mathbf{k}})| = 3$, counted with multiplicity.

If L is $\mathbf{k}$-rational (i.e. $a, b, c \in \mathbf{k}$), and 2 of the intersection points are $\mathbf{k}$-rational, then so is the 3rd point of the intersection.

Elliptic curve and projective lines

The defining polynomial:

$F^*: y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3), a_i \in \mathbf{k}.$

Let $L = \{(x:y:z) \mid ax + by + cz = 0\} \subset \mathbb{P}^2(\overline{\mathbf{k}})$ be a projective line with $(a, b, c) \neq (0, 0, 0)$

Theorem: Intersection of E with a projective line

Let $L \subset \mathbb{P}^2(\overline{\mathbf{k}})$ be a projective line. Then $|L \cap E(\overline{\mathbf{k}})| = 3$, counted with multiplicity.

If L is $\mathbf{k}$-rational (i.e. $a, b, c \in \mathbf{k}$), and 2 of the intersection points are $\mathbf{k}$-rational, then so is the 3rd point of the intersection.

If a polynomial of degree d over $\mathbf{k}$ has $d-1$ roots in $\mathbf{k}$, then the last root is also in $\mathbf{k}$.

Elliptic curve and projective lines

Proof: $a = b = 0$. Then $L = \{(x : y : 0)\}$ is the line at infinity and $L \cap E(\overline{\mathbf{k}}) = \{(0 : 1 : 0)\}$ of multiplicity 3.

Elliptic curve and projective lines

Proof: $a = b = 0$. Then $L = \{(x : y : 0)\}$ is the line at infinity and $L \cap E(\bar{\mathbf{k}}) = \{(0 : 1 : 0)\}$ of multiplicity 3.

$a \neq 0$ or $b \neq 0$. Then $L = \{(x : y : 1) \mid ax + by = -c\} \cup \{(b : -a : 0)\}$ and we have two sub-cases.

Elliptic curve and projective lines

Proof: $a = b = 0$. Then $L = \{(x : y : 0)\}$ is the line at infinity and $L \cap E(\bar{\mathbf{k}}) = \{(0 : 1 : 0)\}$ of multiplicity 3.

$a \neq 0$ or $b \neq 0$. Then $L = \{(x : y : 1) \mid ax + by = -c\} \cup \{(b : -a : 0)\}$ and we have two sub-cases.

1) $b \neq 0$. Then $(b : -a : 0) \neq (0 : 1 : 0)$, hence, $(b : -a : 0) \notin E(\bar{\mathbf{k}})$ as $(0 : 1 : 0)$ is its only point at infinity.

We substitute $y = -\frac{ax+c}{b}$ in E and obtain a cubic polynomial in x with 3 roots in $\bar{\mathbf{k}}$, counted with multiplicity.

Elliptic curve and projective lines

Proof: $a = b = 0$. Then $L = \{(x : y : 0)\}$ is the line at infinity and $L \cap E(\bar{\mathbf{k}}) = \{(0 : 1 : 0)\}$ of multiplicity 3.

$a \neq 0$ or $b \neq 0$. Then $L = \{(x : y : 1) \mid ax + by = -c\} \cup \{(b : -a : 0)\}$ and we have two sub-cases.

1) $b \neq 0$. Then $(b : -a : 0) \neq (0 : 1 : 0)$, hence, $(b : -a : 0) \notin E(\bar{\mathbf{k}})$ as $(0 : 1 : 0)$ is its only point at infinity.

We substitute $y = -\frac{ax+c}{b}$ in E and obtain a cubic polynomial in x with 3 roots in $\bar{\mathbf{k}}$, counted with multiplicity.

2) $b = 0, a \neq 0$. $(0 : 1 : 0) \in L \cap E(\bar{\mathbf{k}})$.

We substitute $x = -\frac{c}{a}$ in E and obtain a quadratic polynomial in y that has two roots in $\bar{\mathbf{k}}$, counted with multiplicity. This gives 3 points.

For the $\mathbf{k}$-rationality assertion use Vieta's formulas. ■

Elliptic curve and projective lines: Bézout's theorem

Alternatively, to obtain $|L \cap E(\overline{\mathbf{k}})| = 3$, we can use the following result.

Theorem: Bézout'1779

Let $\mathcal{C}_1, \mathcal{C}_2$ be two plane projective curves over a field $\mathbf{k}$ whose defining polynomials F_1, F_2 are relatively prime (i.e. their polynomial greatest common divisor is a constant) and have degrees d_1 and d_2.

Then their intersection $\mathcal{C}_1 \cap \mathcal{C}_2$ in $\mathbb{P}^2(\mathbf{k}')$, with $\mathbf{k}'$ an algebraically closed field $\mathbf{k}' \supseteq \mathbf{k}$, counted with their multiplicities, consists of $d_1 \cdot d_2$ points.

E has degree 3 (i.e. F^* has degree 3), a projective line has degree 1.

Elliptic curve and projective lines: Tangents

Definition: Tangents

Let $P \in E(\overline{\mathbf{k}})$. The projective line

$$T_P := \left\{(u : v : w) \in \mathbb{P}^2 \mid \frac{\partial F^*}{\partial x}(P) \cdot u + \frac{\partial F^*}{\partial y}(P) \cdot v + \frac{\partial F^*}{\partial z}(P) \cdot w = 0\right\}$$

is the tangent of E at point P.

Let $\nabla = (\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z})$, then T_P is defined by $\nabla F^*(P) \cdot \begin{pmatrix} u \\ v \\ w \end{pmatrix} = 0$.

For $\mathcal{O} = (0 : 1 : 0)$, we have $\nabla F^*(\mathcal{O}) = (0, 0, 1)$, then
$\mathcal{O} \in T_{\mathcal{O}} = \{(u : v : w) \mid w = 0\}$ the line at ∞.

Elliptic curve: The group structure $(E(\bar{\mathbf{k}}), +)$

We can view the addition geometrically, algebraically, and analytically.

Group structure on $E(\bar{\mathbf{k}})$, geometrically

For $P, Q \in E(\bar{\mathbf{k}})$ define $P * Q$ by $E(\bar{\mathbf{k}}) \cap L = \{P, Q, P * Q\}$, where

$$L := \begin{cases} \text{the projective line through } P \text{ and } Q \text{ if } P \neq Q \\ \text{the tangent } T_P \text{ of } E \text{ at } P \text{ if } P = Q \end{cases}$$

We define

$$P + Q := (P * Q) * \mathcal{O}.$$

Elliptic curve: The group structure $(E(\overline{\mathbf{k}}), +)$

Theorem: Group structure on $E(\overline{\mathbf{k}})$

Let $P, Q, R \in E(\overline{\mathbf{k}})$ and $L \subset \mathbb{P}^2(\overline{\mathbf{k}})$ a projective line. Then:

1. $*$ and $+$ are commutative.
2. $(P * Q) * P = Q$.
3. $\mathcal{O} * \mathcal{O} = \mathcal{O}$
4. If $L \cap E(\overline{\mathbf{k}}) = \{P, Q, R\}$, then $(P + Q) + R = \mathcal{O}$.
5. $P + \mathcal{O} = P$.
6. $P + Q = \mathcal{O} \Leftrightarrow P * Q = \mathcal{O}$.
7. $+$ is associative.
8. $(E(\overline{\mathbf{k}}), +)$ is an abelian group with neutral element $\mathcal{O}$ and $-P = P * \mathcal{O}$.
9. $E(\mathbf{k})$ is a subgroup of $E(\overline{\mathbf{k}})$.

Elliptic curve: The group structure $(E(\bar{\mathbf{k}}), +)$

Proof:

1. By definitions of $*$ and $+$.
2. By definition of L in the definition of $*$.
3. Since $\mathcal{O} \in T_{\mathcal{O}}$, see above.
4. $(P + Q) + R = (((P * Q) * \mathcal{O}) * R) * \mathcal{O} \overset{2.}{=} \mathcal{O} * \mathcal{O} \overset{3.}{=} \mathcal{O}$.
5. $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} \overset{1.}{=} (\mathcal{O} * P) * \mathcal{O} \overset{2.}{=} P$.
6. If $P * Q = \mathcal{O}$, then $P + Q = (P * Q) * \mathcal{O} = \mathcal{O} * \mathcal{O} \overset{2.}{=} \mathcal{O}$. If $P + Q = \mathcal{O}$, then
   $P * Q \overset{5.}{=} (P * Q) + \mathcal{O} = ((P * Q) * \mathcal{O}) * \mathcal{O} = (P + Q) * \mathcal{O} = \mathcal{O} * \mathcal{O} \overset{3.}{=} \mathcal{O}$.
7. Case by case analysis (whether $P = Q$ or/and $R = P + Q$, etc.) or, use algebraic formulas, or see the next slide.
8. Follows from 1, 5, 6, and 7.
9. If E is defined over $\mathbf{k}$ and $P, Q \in E(\mathbf{k})$, then $L, L \cap E$ are defined over $\mathbf{k}$. In addition, $P * Q$ is, as the 3rd root of $L \cap E(\bar{\mathbf{k}})$, also in $\mathbf{k}$.

The group structure $(E(\overline{\mathbf{k}}), +)$: Associativity

Sketch: Let $P, Q, R \in E(\overline{\mathbf{k}})$.

To compute $-((P+Q)+R)$ we form projective lines $L_1 = \overline{PQ}, M_2 = \overline{\mathcal{O}, P+Q}$ and $L_3 = \overline{R, P+Q}$.

To compute $-(P+(Q+R))$ we form projective lines $M_1 = \overline{QR}, L_2 = \overline{\mathcal{O}, Q+R}$ and $M_3 = \overline{P, Q+R}$.

The group structure $(E(\bar{\mathbf{k}}), +)$: Associativity

Sketch: Let $P, Q, R \in E(\bar{\mathbf{k}})$.

To compute $-((P+Q)+R)$ we form projective lines $L_1 = \overline{PQ}, M_2 = \overline{\mathcal{O}, P+Q}$ and $L_3 = \overline{R, P+Q}$.

To compute $-(P+(Q+R))$ we form projective lines $M_1 = \overline{QR}, L_2 = \overline{\mathcal{O}, Q+R}$ and $M_3 = \overline{P, Q+R}$.

We see that $P_{ij} = L_i \cap M_j \in E$, except possibly P_{33}. By the Theorem below, having 8 points $P_{ij} \neq P_{33}$ on $E \Rightarrow P_{33} \in E$.

Since $L_3 \cap E = \{R, P+Q, -((P+Q)+R)\}$, we must have $-((P+Q)+R) = P_{33}$.

The group structure $(E(\overline{\mathbf{k}}), +)$: Associativity

Sketch: Let $P, Q, R \in E(\overline{\mathbf{k}})$.

To compute $-((P+Q)+R)$ we form projective lines $L_1 = \overline{PQ}, M_2 = \overline{\mathcal{O}, P+Q}$ and $L_3 = \overline{R, P+Q}$.

To compute $-(P+(Q+R))$ we form projective lines $M_1 = \overline{QR}, L_2 = \overline{\mathcal{O}, Q+R}$ and $M_3 = \overline{P, Q+R}$.

We see that $P_{ij} = L_i \cap M_j \in E$, except possibly P_{33}. By the Theorem below, having 8 points $P_{ij} \neq P_{33}$ on $E \Rightarrow P_{33} \in E$.

Since $L_3 \cap E = \{R, P+Q, -((P+Q)+R)\}$, we must have $-((P+Q)+R) = P_{33}$.

Similarly, $-(P+(Q+R)) = P_{33}$, so $-((P+Q)+R) = -(P+(Q+R))$, whence the associativity.

The group structure $(E(\bar{\mathbf{k}}), +)$: Associativity

Sketch: Let $P, Q, R \in E(\bar{\mathbf{k}})$.

To compute $-((P + Q) + R)$ we form projective lines $L_1 = \overline{PQ}$, $M_2 = \overline{\mathcal{O}, P + Q}$ and $L_3 = \overline{R, P + Q}$.

To compute $-(P + (Q + R))$ we form projective lines $M_1 = \overline{QR}$, $L_2 = \overline{\mathcal{O}, Q + R}$ and $M_3 = \overline{P, Q + R}$.

We see that $P_{ij} = L_i \cap M_j \in E$, except possibly P_{33}. By the Theorem below, having 8 points $P_{ij} \neq P_{33}$ on $E \Rightarrow P_{33} \in E$.

Since $L_3 \cap E = \{R, P + Q, -((P + Q) + R)\}$, we must have $-((P + Q) + R) = P_{33}$.

Similarly, $-(P + (Q + R)) = P_{33}$, so $-((P + Q) + R) = -(P + (Q + R))$, whence the associativity.

Cases: $P_{ij} = \mathcal{O}$ or $P_{ij} = P_{kl}$ (a line is tangent) or two lines are equal. ■

The group structure $(E(\overline{\mathbf{k}}), +)$: Associativity

Theorem: Cayley-Bacharach'1886

If $P_1, \ldots, P_8$ are points in $\mathbb{P}^2(\overline{\mathbf{k}})$, no 4 on a line, and no 7 on a conic, then there is a 9th point Q such that any cubic through $P_1, \ldots, P_8$ also passes through Q.

Using the Theorem: Two cubic curves, $L_1 L_2 L_3 = 0$ and $M_1 M_2 M_3 = 0$, pass through 8 points: $\mathcal{O}, P, Q, R, P+Q, Q+R, -(P+Q), -(Q+R)$. By Bezout's theorem, two cubics intersect in 9 points, P_{33} is the 9th point.

The group structure $(E(\overline{\mathbf{k}}), +)$: Associativity

Theorem: Cayley-Bacharach'1886

If $P_1, \ldots, P_8$ are points in $\mathbb{P}^2(\overline{\mathbf{k}})$, no 4 on a line, and no 7 on a conic, then there is a 9th point Q such that any cubic through $P_1, \ldots, P_8$ also passes through Q.

Using the Theorem: Two cubic curves, $L_1 L_2 L_3 = 0$ and $M_1 M_2 M_3 = 0$, pass through 8 points: $\mathcal{O}, P, Q, R, P + Q, Q + R, -(P + Q), -(Q + R)$. By Bezout's theorem, two cubics intersect in 9 points, P_{33} is the 9th point.

By the Theorem, any other cubic through these 8 points also passes through P_{33}. So, E passes through P_{33}.

The group structure $(E(\bar{\mathbf{k}}), +)$: Associativity

Theorem: Cayley-Bacharach'1886

If $P_1, \ldots, P_8$ are points in $\mathbb{P}^2(\bar{\mathbf{k}})$, no 4 on a line, and no 7 on a conic, then there is a 9th point Q such that any cubic through $P_1, \ldots, P_8$ also passes through Q.

Using the Theorem: Two cubic curves, $L_1 L_2 L_3 = 0$ and $M_1 M_2 M_3 = 0$, pass through 8 points: $\mathcal{O}, P, Q, R, P+Q, Q+R, -(P+Q), -(Q+R)$. By Bezout's theorem, two cubics intersect in 9 points, P_{33} is the 9th point.

By the Theorem, any other cubic through these 8 points also passes through P_{33}. So, E passes through P_{33}. On $M_1 M_2 M_3 \cap E$ we have:

$$\mathcal{O}, P, Q, R, P+Q, Q+R, -(P+Q), -(Q+R), -(P+(Q+R)), P_{33}.$$

Only 3 points on a line intersect a cubic, so two of these points must coincide. By definition, P_{33} is $\neq$ any of the first 8 points, so

$$P_{33} = -(P+(Q+R)).$$

The group structure $(E(\overline{\mathbf{k}}), +)$: Associativity

Theorem: Cayley-Bacharach'1886

If $P_1, \ldots, P_8$ are points in $\mathbb{P}^2(\overline{\mathbf{k}})$, no 4 on a line, and no 7 on a conic, then there is a 9th point Q such that any cubic through $P_1, \ldots, P_8$ also passes through Q.

Using the Theorem: Two cubic curves, $L_1 L_2 L_3 = 0$ and $M_1 M_2 M_3 = 0$, pass through 8 points: $\mathcal{O}, P, Q, R, P+Q, Q+R, -(P+Q), -(Q+R)$. By Bezout's theorem, two cubics intersect in 9 points, P_{33} is the 9th point.

By the Theorem, any other cubic through these 8 points also passes through P_{33}. So, E passes through P_{33}. On $M_1 M_2 M_3 \cap E$ we have:

$$\mathcal{O}, P, Q, R, P+Q, Q+R, -(P+Q), -(Q+R), -(P+(Q+R)), P_{33}.$$

Only 3 points on a line intersect a cubic, so two of these points must coincide. By definition, P_{33} is $\neq$ any of the first 8 points, so

$$P_{33} = -(P+(Q+R)).$$

Similarly, for $L_1 L_2 L_3 \cap E$, that gives $P_{33} = -((P+Q)+R)$. ■

The group structure $(E(\bar{\mathbf{k}}), +)$: Associativity

Theorem: Cayley-Bacharach'1886

If $P_1, \ldots, P_8$ are points in $\mathbb{P}^2(\bar{\mathbf{k}})$, no 4 on a line, and no 7 on a conic, then there is a 9th point Q such that any cubic through $P_1, \ldots, P_8$ also passes through Q.

Hypothesis of the Theorem are fulfilled: If 4 of the points $\mathcal{O}, P, Q, R, P+Q, Q+R, -(P+Q), -(Q+R)$ are on a line L, then, as they are also on E, $|L \cap E(\bar{\mathbf{k}})| \geqslant 4$, which contradicts Bezout's theorem (as $1 \cdot 3 = 3$).

If 7 of them lie on a conic C, as they are also on E, $|C \cap E(\bar{\mathbf{k}})| \geqslant 7$, which contradicts Bezout's theorem (as $2 \cdot 3 = 6$.) ■

Elliptic curve: The group structure $(E(\overline{\mathbf{k}}), +)$

The defining polynomial:

$$F^*: y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3), a_i \in \mathbf{k}.$$

$P = (x_1, y_1) = (x_1 : y_1 : 1), Q = (x_2, y_2) = (x_2 : y_2 : 1) \in E(\overline{\mathbf{k}})$ with $P, Q \neq \mathcal{O}$.

Let $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ if $P \neq Q$ and $\lambda = \frac{\frac{\partial F^*}{\partial x}(P)}{\frac{\partial F^*}{\partial y}(P)} = -\frac{a_1y_1 - 3x_1^2 - 2a_2x_1 - a_4}{2y_1 + a_1x_1 + a_3}$ if $P = Q$.

Group structure on $E(\overline{\mathbf{k}})$, algebraically (without proof)

$$P + Q = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -y_1 + \lambda(x_1 - x_3) - a_1x_1 - a_3)$$

$$-P = P * \mathcal{O} = (x_1 : -y_1 - a_1x_1 - a_3 : 1)$$

Here: $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$.

Elliptic curve: The group structure $(E(\bar{\mathbf{k}}), +)$

Theorem: Mordell'1922–Weil'1928

For an abelian variety A over a number field $\mathbf{k}$, the group $A(\mathbf{k})$ of $\mathbf{k}$-rational points of A is a finitely-generated abelian group.

Corollary

For a number field $\mathbf{k}$, the abelian group $E(\mathbf{k})$ is finitely generated.

Theorem: Structure of finitely generated abelian groups

Given a finitely generated abelian group A, there exist $r, k \in \mathbb{N}_{>0}$ and $n_1, \ldots, n_k \in \mathbb{N}$ with $n_i | n_{i+1}$ such that $A \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, r is the rank of A and the n_i's are the determinantal divisors of A.

Elliptic curve: Size of $(E(\mathbb{F}_q), +)$

Let p be a prime, $q = p^n$ and $N = |E(\mathbb{F}_q)|$.

Theorem: Hasse'1933 (without proof)

The order of $E(\mathbb{F}_q)$ satisfies:

$$|q + 1 - N| \leqslant 2\sqrt{q}$$

Elliptic curve: Size of $(E(\mathbb{F}_q), +)$

Let p be a prime, $q = p^n$ and $N = |E(\mathbb{F}_q)|$.

Theorem: Hasse'1933 (without proof)

The order of $E(\mathbb{F}_q)$ satisfies:

$$|q + 1 - N| \leqslant 2\sqrt{q}$$

Let $P \in E(\mathbb{F}_q)$, the order of $E(\mathbb{F}_q)$ satisfies $N \cdot P = \mathcal{O}$.

By Hasse's bound, we can find N in $4\sqrt{q}$ steps.

Exercises: Shank's Baby-Step Giant-Step algorithm to solve the DLP in $E(\mathbb{F}_q)$. In particular, we can find N in $4q^{\frac{1}{4}}$ steps.

Elliptic curve: Structure of $(E(\mathbb{F}_q), +)$

Theorem: existence of elliptic curves over finite fields (without proof)

Let p be a prime, $q = p^n$ and $N = q + 1 - a$ for some $a \in \mathbb{Z}$ with $|a| \leqslant 2\sqrt{q}$. Then there is an elliptic curve $E(\mathbb{F}_q)$ with $|E(\mathbb{F}_q)| = N$ if and only if a satisfies one of the following conditions:

1. $\gcd(a, p) = 1$.
2. n is even and $a = \pm 2\sqrt{q}$
3. n is even, $p \not\equiv 1 \bmod 3$, and $a = \pm\sqrt{q}$.
4. n is odd, $p = 2$ or $p = 3$, and $a = \pm p^{\frac{n+1}{2}}$.
5. n is even, $p \not\equiv 1 \bmod 4$, and $a = 0$.
6. n is odd and $a = 0$.

Elliptic curve: Structure of $(E(\mathbb{F}_q), +)$

Theorem: structure for elliptic curves over finite fields (without proof)

Let p be a prime, $q = p^n$ and $N = q + 1 - a$ for some $a \in \mathbb{Z}$ with $|a| \leqslant 2\sqrt{q}$. Write $N = p^e n_1 n_2$ with $p \not| n_1 n_2$ and $n_1 | n_2$ (possibly $n_1 = 1$). Then there is $E(\mathbb{F}_q)$ such that

$$E(\mathbb{F}_q) \cong \mathbb{Z}/p^e\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

if and only if

1. $n_1 | q - 1$ in the cases 1, 3, 4, 5, 6 of the preceding Theorem.
2. $n_1 = n_2$ in the case 2 of the preceding theorem.

These are all groups that occur as $E(\mathbb{F}_q)$.

Realizations of abelian groups

DLP assumption includes that the DLP in $((\mathbb{Z}/p\mathbb{Z})^{\times}, \cdot)$ is not in BPP.

Exercises: the DLP in $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ is in P.

However,

$$((\mathbb{Z}/p\mathbb{Z})^{\times}, \cdot) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +).$$

Thus, the complexity of the DLP depends on the realization of the abelian group.

Realizations of abelian groups

DLP assumption includes that the DLP in $((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ is not in BPP.

Exercises: the DLP in $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ is in P.

However,

$$((\mathbb{Z}/p\mathbb{Z})^\times, \cdot) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +).$$

Thus, the complexity of the DLP depends on the realization of the abelian group.

$(E(\mathbf{k}), +)$ is an elliptic curve realization of the abelian group.

It is a realization which resists all known attacks on the DLP.

Realizations of abelian groups

DLP assumption includes that the DLP in $((\mathbb{Z}/p\mathbb{Z})^{\times}, \cdot)$ is not in BPP.

Exercises: the DLP in $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ is in P.

However,

$$((\mathbb{Z}/p\mathbb{Z})^{\times}, \cdot) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +).$$

Thus, the complexity of the DLP depends on the realization of the abelian group.

$(E(\mathbf{k}), +)$ is an elliptic curve realization of the abelian group.

It is a realization which resists all known attacks on the DLP.

SafeCurves = curves with efficient and secure implementation.

ECC versus RSA

A smaller key size with ECC

ECC with 256-bit key $\sim$ RSA with 3072-bit key

Protection	Symmetric	RSA modulus	Elliptic curve
Standard: not now	80	1024	160
Near-term: 2018-28	128	3072	256
Long-term: 2018-68	256	15360	512

Table: ECRYPT-CSA Recommendations (2018)

ECC versus RSA

A smaller key size with ECC

ECC with 256-bit key $\sim$ ElGamal 3072-bit group size

General number field sieve (GNFS) for DLP in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ runs in time $2^{O(n^{1/3}\cdot(\log_2 n)^{2/3})}$ for p of length $O(n)$.

So, for a 512-bit prime p, the GNFS solves the DLP in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ in roughly

$$2^{512^{1/3}.9^{2/3}} \sim 2^{8\cdot 4} = 2^{32} \text{ steps.}$$

The best generic algorithm solves DLP in $E(\mathbb{F}_q)$ with $N = |E(\mathbb{F}_q)|$, where N is a 64-bit prime, in roughly

$$\sqrt{N} \sim 2^{64/2} = 2^{32} \text{ steps.}$$

ECC in Practice: Example

SSL / TLS protocols

SSL=Secure Sockets Layer, TLS=Transport Layer Security

They use public key cryptography to derive symmetric keys and then use symmetric key cryptography to ensure confidentiality and data integrity of the communication.

Web browsing, email, instant messaging, communication between a browser and a server.

Diffie-Hellman key agreement

To exchange keys securely over an insecure communication channel:

Diffie-Hellman'1976 Key exchange protocol

1. Alice and Bob agree publicly on a cyclic group $G = \langle g \rangle$.
2. Alice choses randomly $0 \leqslant a \leqslant |G|$ and computes $A := g^a$. Bob chooses randomly $0 \leqslant b \leqslant |G|$ and computes $B := g^b$.
3. Alice sends A, Bob sends B.
4. Alice computes $S := B^a$. Bob computes $S := A^b$.
5. Since it is the same S, they can use it as their secrete key to encrypt and decrypt messages.

Standard choice: $G = (\mathbb{Z}/p\mathbb{Z})^\times$, Public information: $G = \langle g \rangle, A, B$.

Diffie-Hellman key agreement: Interceptor attacks

Passive attack by Eve

Eve= eavesdropper should solve the DHP, i.e. given g^a and g^b (but not a or b) she wants to find $S = g^{ab}$.

Solving the DLP in G would solve the DHP in G. Hence, DHP $\notin$ BPP is at least as strong as DLP $\notin$ BPP. The equivalence is unknown.

Diffie-Hellman key agreement: Interceptor attacks

Passive attack by Eve

Eve= eavesdropper should solve the DHP, i.e. given g^a and g^b (but not a or b) she wants to find $S = g^{ab}$.

Solving the DLP in G would solve the DHP in G. Hence, DHP $\notin$ BPP is at least as strong as DLP $\notin$ BPP. The equivalence is unknown.

Active attack by Mallory

Mallory= (wo)man-in-the middle attack tells Allice to be Bob and does the exchange getting S.

He/she tells to Bob to be Alice and does the exchange getting S'.

Whenever Alice sends Bob a message, Mallory takes the cyphertext, decrypts it with S, reads it, then encrypts it with S' and sends to Bob.

EC based Diffie-Hellman

Standard choice: $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$, Public information: $G = \langle g \rangle, A, B$.

ECC choice: $G = E(\mathbb{F}_q)$ and the elliptic-curve public-private key pair.

Practice: ECDHE protocol, last E=ephemeral, i.e. the public keys are not static, they are temporary.

Digital Signature Scheme

To ensure the authenticity of data over an insecure channel:

Definition: Signature scheme is a 5-tuple $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$, satisfying:

- $\mathcal{P}$ is a finite set of possible messages;
- $\mathcal{A}$ is a finite set of possible signatures;
- $\mathcal{K}$, the keyspace, is a finite set of possible keys;
- $\mathcal{S} = \{\mathrm{sig}_k : k \in \mathcal{K}\}$ consists of polynomial signing algorithms $\mathrm{sig}_k : \mathcal{P} \to \mathcal{A}$;
- $\mathcal{V} = \{\mathrm{ver}_k : k \in \mathcal{K}\}$ consists of polynomial verification algorithms $\mathrm{ver}_k : \mathcal{P} \times \mathcal{A} \to \{\text{true}, \text{false}\}$;
- $\forall x \in \mathcal{P}, \forall y \in \mathcal{A}$: $\mathrm{ver}_k(x, y) = \begin{cases} \text{true}, & \text{if } y = \mathrm{sig}_k(x) \\ \text{false}, & \text{otherwise.} \end{cases}$

  A pair (x, y) with $x \in \mathcal{P}, y \in \mathcal{A}$ is called a signed message.

Digital Signature Scheme (DSS)

$\forall k \in \mathcal{K}$, ver_k is public and sig_k is private.

There might by more than one $y \in \mathcal{A}$ such that $\mathrm{ver}_k(x, y) = \text{true}$, depending on the definition of ver_k.

We require that the problem that, given a message $x \in \mathcal{P}$, anyone other than Alice can compute a signature $y \in \mathcal{A}$ such that $\mathrm{ver}_k(x, y) = \text{true}$, is not in BPP.

Digital Signature Scheme (DSS)

$\forall k \in \mathcal{K}$, ver_k is public and sig_k is private.

There might by more than one $y \in \mathcal{A}$ such that $\mathrm{ver}_k(x, y) = \text{true}$, depending on the definition of ver_k.

We require that the problem that, given a message $x \in \mathcal{P}$, anyone other than Alice can compute a signature $y \in \mathcal{A}$ such that $\mathrm{ver}_k(x, y) = \text{true}$, is not in BPP.

A forged signature is a valid signature produced by someone other than Alice.

Usually, one signs only hash values of messages for performance reasons: ‘hash-then-sign’.

A digital signature should lose its validity if anything in the signed data was altered.

RSA and EC variants of Digital Signature

RSA Signature Algorithm

It is the DSS with sig_k defined by the RSA decryption function D_k and ver_k defined by the RSA encryption function E_k:

$$\mathrm{sig}_k(x) = D_k(x) \text{ and } \mathrm{ver}_k(x, y) = \text{true} \Leftrightarrow x = E_k(y)$$

Reminder: $D_k(x) = x^d \mod n$ and $E_k(y) = y^e \mod n$,

Analogously: DSS using one-way functions with trapdoors.

EC variant of Digital Signature

ElGamal Signature Scheme: a suitable signature scheme, not just use of the ElGamal cryptosystem in the DSS.

Digital Signature Algortihm (DSA)

ECDSA

Every day example

‘The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with X25519 (a strong key exchange), and AES_128_GCM (a strong cipher).’

Test questions

Question 12

1. Why does ElGamal produce two components ciphertext?
2. Why the exponents used for decryption are smaller for ElGamal compared to RSA?
3. Why ECC is more popular than the original ElGamal?

Question 13

Which of the following statements are true?

1. Breaking ElGamal is equivalent to solving Asymmetry of ElGamal.
2. ElGamal is less efficient for encryption than RSA.
3. ElGamal is more efficient for decryption than RSA.
4. There is no message expansion in the RSA-OAEP cryptosystem.

Test questions

Question 14

Prove Cayley-Bacharach's theorem.

Question 15

Check that for a prime q, each natural number in the Hasse interval occurs as the order of $E(\mathbb{F}_q)$.