OLGA RADKO MATH CIRCLE, SPRING 2024: ADVANCED 3

FERNANDO FIGUEROA AND JOAQUÍN MORAGA

Worksheet 6: Topics on Elliptic curves

Let $\mathbb{F}$ be a field of characteristic different to 2 or 3.

Let $x^3 + ax + b$ be a cubic polynomial with coefficients in $\mathbb{F}$ that has no repeated roots. Remember that an *elliptic curve* over $\mathbb{F}$ is defined as the set of points (x, y) in $\mathbb{F}^2$ satisfying the equation

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

together with a single point denoted O and called the point at infinity.

For the following exercise, you may use that a polynomial $x^3 + ax + b$ has repeated roots in $\mathbb{F}$ if and only if it has common roots in $\mathbb{F}$ with its derivative $3x^2 + a$.

Problem 6.1: Which of the following cubic polynomials have repeated roots:

(1) $x^3 + x$ over $\mathbb{Q}$.
(2) $x^3 - 3x + 2$ over $\mathbb{C}$.
(3) $x^3 + x + 1$ over $\mathbb{F}_5$

Solution 6.1:

Choosing a curve and a point.

Once we have a fixed finite field $\mathbb{F}_q$, we can find an elliptic curve E and a point P on it in the following way:

(1) Let X, Y, A be random elements in $\mathbb{F}_q$, set $B := Y^2 - (X^3 + AX)$
(2) If the cubic $x^3 + Ax + B$ has no repeated roots, one defines the elliptic curve to be $y^2 = x^3 + Ax + B$, with point $P = (X, Y)$.

Problem 6.2:

For the following values of X, Y, A, check if the cubic polynomial $x^3 + Ax + B$ has repeated roots and verify that the point (X, Y) is in the elliptic curve.

(1) $X = 1, Y = 1, A = 2$ over $\mathbb{F}_5$
(2) $X = 2, Y = 3, A = 1$ over $\mathbb{F}_5$
(3) $X = 1, Y = 0, A = 4$ over $\mathbb{F}_5$

Solution 6.2:

For the following exercise, you may use that a polynomial $x^3 + ax + b$ has repeated roots in $\mathbb{F}$ if and only if it has common roots in $\mathbb{F}$ with its derivative $3x^2 + a$.

Problem 6.3: Show that a cubic polynomial $x^3 + ax + b$ has repeated roots if and only if $4a^3 + 27b^2 = 0$.

Solution 6.3:

Let $(\mathbb{Z}/n\mathbb{Z})^\times$ be the set of positive integers less than n that are coprime with n.

Remember that the RSA cryptosystem consists on the following steps:

(1) Picking a secret pair of prime numbers p, q. Define $n := pq$
(2) Picking randomly an integer e coprime with $(p-1)(q-1)$. Define d to be such that $ed \equiv 1 \pmod{(p-1)(q-1)}$
(3) The public key consists on the elements (n, e). While the private key consists of the elements $((p-1)(q-1), d)$.

To encrypt a message, i.e. a number c in in$(\mathbb{Z}/n\mathbb{Z})^\times$, one takes the d power. While the decryption algorithm consists of taking the e power.

Problem 6.4:

(1) Explain why this this algorithm recovers the original plaintext.
(2) Explain why this deciphering method would not work for numbers that are not coprime with n.

Solution 6.4:

The security of RSA relies on the difficulty of the logarithm problem, i.e. given an element g in a group $(G, \cdot)$ and an integer r, finding an element such that $b^r = a$. We will see a similar problem with a group structure on elliptic curves.

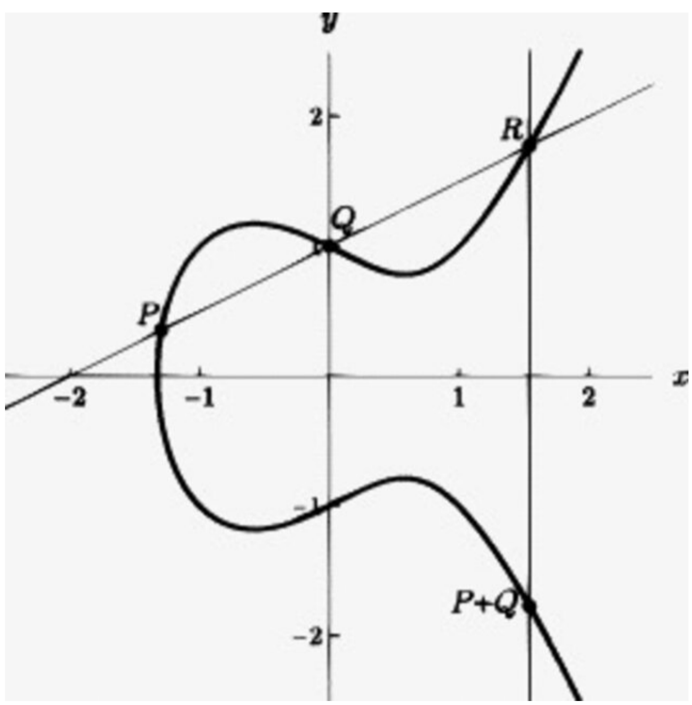
Let us remember how the addition is defined over an elliptic curve.

Let E be an elliptic curve over $\mathbb{R}$, let P and Q be two points in E. We will define $P+Q$ and $-P$ by the following rules.

(1) If $P = O$, then $-P := O$ and $P + Q := Q$, so in the following cases we will assume that no point is the point at infinity.
(2) If the point P has coordinates (x, y), then the point $-P$ is given by the the coordinates $(x, -y)$
(3) If P and Q have different coordinates, then the line $l = \overline{PQ}$ intersects E at a third point R (in case l is tangent to E, we define R to be the point of tangency). We define $P + Q = -R$.
(4) If $Q = -P$, then $P + Q := O$.
(5) If $P = Q$, then let l be the tangent line to E at P, let R be the third point of intersection of l and E. We define $P + Q := -R$.

An example can be seen in the fpicture at the bottom of this page.

If E is an elliptic curve over $\mathbb{F}_q$ and B is a point of E, then the *discrete logarithm problem* on E is the problem of, given a point P in E finding an integer x such that $xB = P$, if such an integer x exists.



Diffie-Hellmann Key Exchange

Alice and Bob want to agree on a common key that they can use for encrypting data. They will do the following steps:

(1) Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$. They also agree on a point P in the curve. These choices can be seen by everybody
(2) Alice chooses a secret integer a, computes aP, and sends it to Bob. Everybody can see aP.
(3) Bob chooses a secret integer b, computes bP and sends it to Alice. Everybody can see bP.
(4) Bob and Alice secretly compute abP and this is the common key.

Diffie-Hellmann Problem.

The Diffie-Hellmann Problem consists on finding the common key defined by the Diffie-Hellman problem. In other words, given an elliptic curve E and points P, aP and bP, finding abP.

Decision Diffie-Hellmann Problem

The decision Diffie-Hellmann Problem consists on checking if a given element is the solution of the Diffie-Helmann Problem. In other words, given an elliptic curve E and points P, aP, bP and Q, checking if $Q = abP$.

Problem 6.5:

Explain why Bob and Alice can find the number abP, but someone else would need to solve the logarithm problem to obtain abP.

Solution 6.5:

ElGamal system on Elliptic curves

They will do the following steps:

(1) Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$. They also agree on a point P in the curve. (This can be though as public information to everybody)

(2) Bob chooses a secret integer b, computes bP, and shares it with everyone. (bP is Bob' public key, and b is Bob's private key).

(3) To send a message M to Bob, Alice will choose a random integer k and send the pair $(kP, M + k(bP))$.

Problem 6.6:

How can Bob decipher the message sent by Alice?

Solution 6.6:

Variant of a signature scheme due to Nyberg and Rueppel.

Let E be an elliptic curve over $\mathbb{F}_q$ and let N be the number of points of E. Alice has a message that she wants to sign. She represents the message as a point M in E. Alice has a secret integer a and makes public points A and B in E, with $B = aA$, as in the ElGamal signature scheme. There is a public function $f : E \to \mathbb{Z}/N\mathbb{Z}$. Alice performs the following steps.

(1) She chooses a random integer k with $\gcd(k, N) = 1$.
(2) She computes $R = M - kA$
(3) She computes $s \equiv k^{-1}(1 - f(R)a) \pmod N$
(4) The signed message is (M, R, s).

Bob verifies the signature as follows:

(1) He computes $V_1 = sR - f(R)B$ and $V_2 = sM - A$
(2) He declares the signature valid if $V_1 = V_2$

Problem 6.7:

Show that if Alice performed the steps correctly, then the signatures V_1 and V_2 should be equal.

Solution 6.7:

Problem 6.8:

Let E be the elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Q}$, let $P = (x, y)$ be a point on E. Let p be a prime not dividing $4a^3 + 27b^2$ or the denominators of the x or y-coordinates of P.

Show that the the order of $P \pmod{p} := (x \pmod{p}, y \pmod{p})$ on the elliptic curve $E \pmod{p}$ defined by the elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is the smallest integer k such that either:

(1) $kP = O$ in E
(2) p divides the denominator of the coordinates of kP.

Solution 6.8:

Let $x^3 + ax + b$ be a polynomial with coefficients in $\mathbb{F}$, having three different solutions in $\mathbb{F}$.

Let E be the elliptic curve associated to the polynomial $y^2 = x^3 + ax + b$ over $\mathbb{F}$.

Problem 6.9:

(1) Show that the elliptic curve E has exactly 3 elements of order 2. *Hint: Elements of order* 2 *have a geometric characterization.*
(2) Show that a cyclic group has 0 or 1 elements of order 2.
(3) Conclude that E is not a cyclic group.

Solution 6.9:

Let $\left(\frac{q}{p}\right)$ be the Legendre Symbol. Remember that this is defined to be 0 if p divides q, 1 if q has a square root modulo p and -1 otherwise.

Problem 6.10: Show that the number of points of an elliptic curve E with equation $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is :

$$p + 1 + \sum_{x \text{ in } \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right)$$

Solution 6.10:

Problem 6.11:

Show that there are $p+1$ points on the elliptic curve $y^2 = x^3 + b$ over $\mathbb{F}_p$, with $p \equiv 2 \pmod 3$

Solution 6.11:

For the following problem you may use the fact that in a finite group, the order of any element divides the number of elements in the group.

Problem 6.12:

Show that the following Elliptic curves have cyclic group structure:

(1) $y^2 = x^3 + 1$ over $\mathbb{F}_2$
(2) $y^2 = x^3 + 1$ over $\mathbb{F}_5$
(3) $y^2 = x^3 + 1$ over $\mathbb{F}_{11}$

Solution 6.12:

Challenge:

(1) Show that a polynomial $p(x)$ with coefficients in $\mathbb{F}$ has repeated roots in $\mathbb{F}$ if and only if $p(x)$ and its derivative $p'(x)$ have a common root in $\mathbb{F}$.
(2) Can a polynomial with coefficients in $\mathbb{R}$ have repeated complex roots, but no repeated real roots?
(3) Can a polynomial with rational coefficients have repeated real roots but no repeated rational root?

Solution :

UCLA Mathematics Department, Los Angeles, CA 90095-1555, USA.
Email address: `fzamora@math.princeton.edu`

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555, USA.
Email address: `jmoraga@math.ucla.edu`