Lecture notes on elliptic curve cryptography

Raymond van Bommel

Curves over finite fields, Fall 2017, Leiden

1 Discrete logarithm problem and encryption

In its full generality the discrete logarithm problem is the following: given a group G and elements a and b, find an integer k such that $b^k = a$ (given that such k exists).

Example 1. For the group $(\mathbb{R}_{>0}, \cdot)$ solving this problem for the fixed element $b = e$, is equivalent to taking the natural logarithm.

Example 2. Let p be a (large) prime number and let $g \in \mathbb{F}_p^*$ be a generator of the multiplicative group, then the discrete log problem in $\mathbb{F}_p^*$, with $b = g$, is still asserted to be difficult.[a]

Alice and Bob can make use of this fact in order to encrypt their communications. Suppose Alice wants to send a message $M \in \mathbb{F}_p^*$ to Bob, then they follow the following protocol, due to Elgamal:

1. First Bob takes a random x from $\{1, \dots, p-1\}$ and computes his so-called public key $Q := g^x$ and sends it to Alice.
2. Alice takes a random y from $\{1, \dots, p-1\}$ and computes $R := g^y$ and $S := M \cdot Q^y$, and send them to Bob.
3. Now Bob can compute $S \cdot R^{-x} = (M \cdot Q^y) \cdot (g^y)^{-x} = M \cdot (g^x)^y \cdot g^{-xy} = M$.

Even if anyone would get to know Q, R and S, then still it is believed to be hard (if p is big enough) to find M.[b]

[a] This will not be the case anymore when there will be a quantum computer. Then Shor's algorithm will solve this problem quite easily.

[b] To be complete: this so-called computational Diffie-Hellman assumption is not equivalent to the discrete logarithm assumption, but the latter is a necessary condition for the former.

The encryption scheme described in Example 2 can be used using any group for which the computation of group operations is relatively easy and for which the discrete logarithm problem is relatively hard. An example of such a group is the group of rational points on an elliptic curve.

2 Elliptic curves

Definition 3. An elliptic curve over $\mathbb{F}_q$ is a smooth projective curve of genus 1 together with an $\mathbb{F}_q$-rational point O.

Remark 4. More classicly, elliptic curves are defined as smooth curves of the shape

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

inside the projective plane $\mathbb{P}^2_{\mathbb{F}_q}$.[a] The chosen $\mathbb{F}_q$-rational point on this curve is $O = (0:1:0)$. We will call these *classical elliptic curves.*

[a]In fact, classicly people write $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$, giving an equation for the affine chart $z \neq 0$.

Exercise 5.

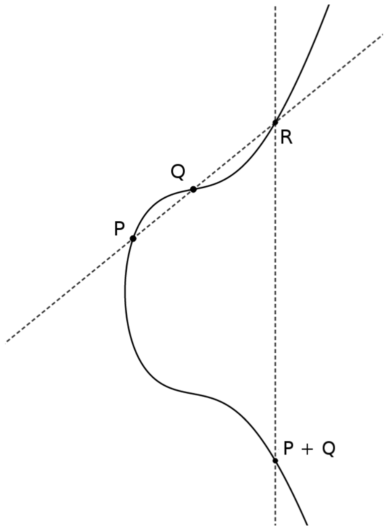
(a) Prove that classical elliptic curves are of genus 1.

(b*) Prove that any elliptic curve is isomorphic to a classical elliptic curve.

One of the properties that makes elliptic curves interesting to study it the fact that its set of $\mathbb{F}_q$-rational points carries a group structure. In order to construct this, we need the following proposition.

Proposition 6. *Let E be a classical elliptic curve over $\mathbb{F}_q$ inside $\mathbb{P}^2_{\mathbb{F}_q}$ and let ℓ be a line in $\mathbb{P}^2_{\mathbb{F}_q}$. Then ℓ intersects E three times, counting intersection points with multiplicity if necessary.*

Proof. Although, we did not define multiplicity properly, it will become immediately clear from this proof. The line ℓ is given by $aX + bY + cZ = 0$ for some $a, b, c \in \mathbb{F}_q$ not all equal to 0. Suppose that we want to find the intersection points of ℓ and E. If $a \neq 0$ (the cases $b \neq 0$ and $c \neq 0$ are similar), then we substitute all occurances of X in the equation for E by $-\frac{b}{a}Y - \frac{c}{a}Z$. What we get is a homogeneous polynomial of degree 3 in the variables Y and Z, whose roots (counted with multiplicity) will give us the intersection points. $\square$



Addition of points on elliptic curves

Definition 7. Let E be a classical elliptic curve over $\mathbb{F}_q$ and let $P, Q \in E(\mathbb{F}_q)$. Let R be the unique third point on E on the line through P and Q (or the line tangent to E at P in case $P = Q$). Then the point $P \oplus Q$ is defined as the third point on the line through R and O.

One can check that this gives $E(\mathbb{F}_q)$ the structure of an abelian group. It is fairly easy to see that O is the neutral element of this group, to find inverses and to prove commutativity. Associativy is a bit more tricky and a consequence of the following classical theorem in geometry.

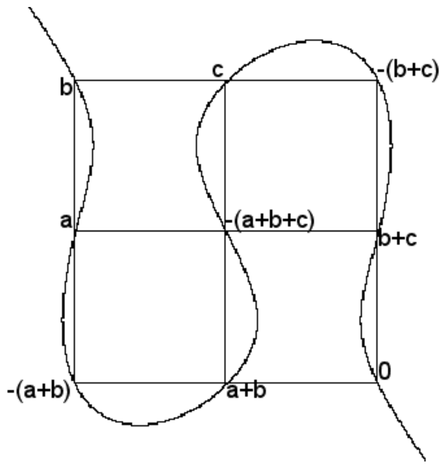


Illustration of associativity proof: one needs to show that the point in the middle, defined in both different ways gives the same point.

Theorem 8 (Cayley-Bacharach)**.** *Suppose two cubics in the projective plane meet in nine points. Then any cubic going through eight of these points, also goes through the ninth.*

Exercise 9. To which three cubics in the illustration above should you apply Cayley-Bacharach to obtain the associativity of the group operation?

Already knowing the Riemann-Roch theorem, we can take a much easier route to show that the operation above gives an abelian group structure.

Lemma 10. *Let E be an elliptic curve. Then the map*

$$E(\mathbb{F}_q) \to \mathrm{Pic}(E) : P \mapsto [P] - [O]$$

is a bijection.

Proof. Let us first prove surjectivity. Let D be a divisor of degree 0. Then $D + O$ is of degree 1 and by Riemann-Roch $\dim_{\mathbb{F}_q} \mathcal{L}(D + O) = 1$. Hence, there is a function f for which $\mathrm{div}(f) + D + O$ is effective. On the other hand, $\mathrm{div}(f) + D + O$ is also of degree 1 and hence equals R for an $R \in E(\mathbb{F}_q)$. Therefore, inside $\mathrm{Pic}(E)$ we have $[D] = [R] - [O]$.

Now let us prove injectivity. Suppose that $P \neq Q$ map to the same divisor class. Then $[P] - [Q] = 0$, or in other words there exists a function $f : E \to \mathbb{P}^1$ having a simple zero at P, a simple pole at Q and no other zeros or poles. Due to the following exercise, this function is an isomorphism, which cannot exist as E is of genus 1 and $\mathbb{P}^1$ is of genus 0. □

Exercise 11. Consider the function $f : E \to \mathbb{P}^1$ having a simple zero at P and a simple pole at $Q \neq P$. Prove that f is an isomorphism.
(This should be an isomorphism of curves, but for the purpose of this course, it suffices if you prove that it is a bijection.)

Now we can use Lemma 10 to provide $E(\mathbb{F}_q)$ with the structure of a group.

Exercise 12. For classical elliptic curves, prove that Lemma 10 gives the same group structure as Definition 7.

3 Elliptic curve cryptography

In order to encrypt messages using elliptic curves we mimic the scheme in Example 2.

First of all Alice and Bob agree on an elliptic curve E over $\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$. As the discrete logarithm problem is easier to solve for groups whose order is composite, they will choose their curve such that $n := |E(\mathbb{F}_q)|$ is prime. Suppose Alice wants to send a message $M \in E(\mathbb{F}_q)$ to Bob.

Bob takes a random $x \in \{1, \ldots, n\}$ and computes his so-called public key

$$Q := x \cdot P = \underbrace{P \oplus P \oplus \ldots \oplus P}_{x \text{ times}}$$

and sends it to Alice. Alice, in her turn, takes a random $y \in \{1, \ldots, n\}$ and computes $R := y \cdot P$ and sends it to Bob. Moreover, she computes $S := M \oplus y \cdot Q$ and also sends this to Bob. Bob can now compute

$$S \ominus x \cdot R = M \oplus y \cdot Q \ominus xy \cdot P = M \oplus xy \cdot P \ominus xy \cdot P = M.$$

For any observer, who got hold of P, Q, R and S, it is still believed to be very difficult to find M, as the discrete logarithm problem for $E(\mathbb{F}_q)$ is believed to be hard.

4 Elliptic curve factorisation (not examined)

Another nice application of elliptic curves is the factorisation of large integers. Suppose for simplicity that $n = pq$ is the product of two primes, both greater than 3, and that we would like to factor n. The following factorisation algorithm is due to H. W. Lensta Jr.

Classically, elliptic curves are given by equations of the shape $y^2 = x^3 + ax + b$, where it is understood that a point O at infinity is to be added to the curve. Given the coordinates (x_1, y_1) and (x_2, y_2) of two points, there are so-called addition formuled to compute the coordinates of their sum. These addition formulas can be found in many resources, but one of their properties is, that if you add a point to its inverse, and you get O, then somewhere in these formules you would have to divide by 0.

Now, the algorithm goes as follows. Take an elliptic curve E over $\mathbb{Z}/n\mathbb{Z}$ given by an equation $y^2 = x^3 + ax + b$, and a random point $P \in E(\mathbb{Z}/n\mathbb{Z})$.

Notice that $\mathbb{Z}/n\mathbb{Z}$ is not a field, as n is not prime. However, we can still use the addition formulas. Points Q in $E(\mathbb{Z}/n\mathbb{Z})$ can be considered as a pair (Q_1, Q_2) of points $Q_1 \in E(\mathbb{F}_p)$ and $Q_2 \in E(\mathbb{F}_q)$.

Now we compute eP for $e = m!$ for some reasonably chosen m. If we are lucky, it will happen that for one of the points Q that we encouter in the intermediate calculations $Q_1 \in E(\mathbb{F}_p)$ becomes the point at infinity, and $Q_2 \in E(\mathbb{F}_q)$ does not (or the other way around). In this case, in one of the addition formulas we have to divide by a number that is divisible by p and not by q. By calculating the greatest common divisor with n, we can then find p.

By trying multiple elliptic curves E and base points P, it is very likely that we will find a factor of n. The interested reader is encouraged to look up more details theirselves.