Cryptography

Itay Genkin

June 2021

Contents

1 Introduction

In this script I would like to describe some algorithms and arithmetic methods in cryptography accompanied by some definitions and examples. Algorithms and methods will not be followed by proofs but will be clearly defined and summarized. The article might be formal on one hand and simple to read on the other hand. Although, it is recommended to know group theory, number theory and basics in linear algebra and field theory.

2 Basic Mathematics Background

2.1 Fermat's Little Theorem

Let p be a prime number. $\forall a \in \{1, ..., p-1\}$ holds $a^{p-1} \equiv 1 \pmod{p}$.

2.2 Quadratic Residues

Definition: Let $x \neq 0$ and $p \geq 2$. It is said that $x \in \mathbb{Z}_p$ is a quadratic residue (modulo p) if there exists $y \in \mathbb{Z}_p$ s.t $y^2 \equiv x \pmod{p}$.
Euler theorem: A number $x \in \mathbb{Z}_p^*$ is a quadratic residue $\iff$ $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
Proposition: For a prime p, there exists $\frac{p-1}{2}$ quadratic residues. And if g is a generator, the quadratic residues are $\{g^0, g^2, g^4, ..., g^{2i}, ..., g^{p-3}\}$.
Corollary: For a prime p, there are $\frac{p-1}{2}$ quadratic non-residues (excluding 0).

2.3 Frobenius' Endomorphism

Definition: Let $\mathbb{F}$ be a finite field, **endomorphism** of $\mathbb{F}$ is a map $\sigma : \mathbb{F} \to \mathbb{F}$ that holds $\sigma(1) = 1$, $\sigma(0) = 0$, $\sigma(ab) = \sigma(a) \cdot \sigma(b)$, $\sigma(a + b) = \sigma(a) + \sigma(b)$.
Example:
Complex conjugate - $\sigma : \mathbb{C} \to \mathbb{C}$, $\sigma(z) = \bar{z}$.
Proposition: Let $\mathbb{F}$ be a field with $\text{char}(\mathbb{F}) = p > 0$. Then there exists endomorphism $\text{Frob} : \mathbb{F} \to \mathbb{F}$ s.t for all $a \in \mathbb{F}$ holds $\text{Frob}(a) = a^p$.
Remark: That endomorphism is called **Frobenius' endomorphism**.

2.4 Extended Euclid Algorithm

If $a, b \in \mathbb{Z} \setminus \{0\}$ and holds $gcd(a, b) = d$, there exist $s, t \in \mathbb{Z}$ s.t $sa + tb = d$.
In the extended Euclid algorithm we write every s_i and t_i by a vector of their representative scalars.

Let $m, n \in \mathbb{Z}$ s.t $gcd(m, n) = d$.

$$m = (1, 0)$$
$$n = (0, 1)$$
$$r_0 = m - q_0 n = (1, -q_0 n)$$
$$r_1 = n - q_1 r_0 = (0, 1) - q_1(1 - q_0 n) = (-q_1, 1 - q_0 q_1 n)$$
$$r_2 = r_0 - q_2 r_1 = (1, -q_0 n) - q_2(-q_1, 1 - q_0 q_1 n) = (1 + q_2 q_1, -q_0 n - q_2 + q_0 q_1 q_2 n)$$
$$\vdots$$
$$d = r_k = r_{k-2} - q_k r_{k-1} = (s, t)$$

Now we've got that $d = s \cdot m + t \cdot n$.
We usually use the extended Euclid algorithm when $d = 1$ and m is the prime number p of the field we use. The purpose is to find the opposite number which perform $t \cdot n = 1$ and in particular means that $t^{-1} \equiv n \pmod{p}$.

Example:
Let $\mathbb{F} = \mathbb{Z}_{59}$. We wish to find 16^{-1}.

$$59 = (1, 0)$$
$$16 = (0, 1)$$
$$11 = 59 - 3 \cdot 16 = (1, 0) - 3(0, 1)$$
$$5 = 16 - 11 = (0, 1) - (1, -3) = (-1, 4)$$
$$1 = 11 - 2 \cdot 5 = (1, -3) - 2(-1, 4) = (3, -11)$$
$$\Downarrow$$
$$3 \cdot 59 - 11 \cdot 16 = 1$$

Since $59 = 0$ in $\mathbb{Z}_{59}$ we got:
$(16)^{-1} = -11 \pmod{59} = 48 \pmod{59}$

2.5 Chinese Remainders Theory

In the last section we saw the extended Euclid algorithm which facilitate the way we find an inverse number of a given number. Now we are going to solve an equation system in modulo. Let $n_1, ..., n_k$ be integers greater than 1 and let us denote N the product of all n_i. If n_i are pairwise co-prime for every i and $a_1, ..., a_k$ are integers s.t $0 \leq a_i < n_i$ for every i, then there is one and only one integer x s.t $0 \leq x < N$ and the remainder of the division & remainder of x by n_i is a_i for every i.

Example:
Let's see the following equations.
$x \equiv 3 \pmod{5}$
$x \equiv 6 \pmod{11}$
Now we write $x = 3 + 5k = 6 \pmod{11} \iff 5k = 3 \pmod{11}$ and we want to find an integer k that perform the equation. As we previously mentioned, we may use the extended Euclid algorithm

to find the inverse number of 5 modulo 11. After computing the Euclid algorithm (with 5 and 11), we got that $5^{-1} \equiv 9 \pmod{11}$. Now we can find such k:
$5k = 3 \pmod{11}$ (multiplying by 9)
$k = 27 \pmod{11} = 5 \pmod{11}$
In the end, we may find: $x = 3 + 5 \implies x = 28$

3 Algorithms

3.1 Rivest-Shamir-Adleman (RSA)

Bob chooses two big primes p and q (the bigger the better) computes $n = p \cdot q$ and the group will be the multiplying group $G = \mathbb{Z}_n^{\mathrm{x}}$. The order of the group is $k = (p-1)(q-1)$. Now Bob chooses two natural numbers d and e s.t $ed = 1 + kl$ for some $l \in \mathbb{Z}$. Bob share the group G and d. Let $f : G \to G$ be defined by $f(m) = m^d$ and we denote $f(m) = c$. Alice restore the message from the encrypted text c by the secret key e by computing $m = c^e \pmod{n}$ so she gets $m = c^e = \left(m^d\right)^e = m^{de} = m^{1+kl} = m \cdot \left(m^k\right)^l = m \cdot 1^l = m$ (remark: the order of the group is k so $m^k = 1 \pmod{n}$).
Remark: it is easy to compute n and k from the primes p and q, but it is pretty hard to compute p and q from n for large enough primes.

3.2 Diffie-Hellman

Alice and Bob want to send messages each other. They openly agree on a big prime number p s.t the solution of the discrete-log problem in the multiply group $\mathbb{F}_p^*$ will be difficult to compute and they also agree on a generator g_0 which are both public. Alice secretly choose $0 < e_a < p - 1$, calculate $A = g_0^{e_a} \pmod{p}$ and sends A to Bob. Similarly, Bob secretly choose $0 < e_b < p - 1$, calculate $B = g_0^{e_b} \pmod{p}$ and sends B to Alice. Now Alice has e_a and B while Bob has e_b and A and they both can compute the public key. So Alice computes $K = B^{e_a} = (g_0^{e_b})^{e_a} = g_0^{e_a e_b} \pmod{p}$ and Bob computes $K = A^{e_b} = (g_0^{e_a})^{e_b} = g_0^{e_a e_b} \pmod{p}$. Finally, they safely shared the public key, K.
The information that has been publicly shared is $\mathbb{F}_p^*$, g_0, A and B, while e_a and e_b have been kept secret. It is considered difficult to compute e_a or e_b from these information which leads us to the known discrete-log-problem.

Example:
Suppose that a prime $p = 857$ and a generator $g = 243$ of the multiplicative group $\mathbb{F}_p^*$ has been agreed. Alice chooses secret integer $a = 315$ and computes $A = g^a \pmod{p} = 243^{315} \pmod{857} = 548 \pmod{857}$.
Bob chooses secret integer $b = 109$ and computes $B = g^b \pmod{p} = 243^{109} \pmod{857} = 491$.
Alice sends to Bob the number $A = 548$ and Bob sends to Alice the number $B = 491$.
Then, Alice compute the key: $K = B^a \pmod{p} = 491^{315} \pmod{857} = 846$ and Bob computes the key $K = A^b \pmod{p} = 548^{109} \pmod{857} = 846$. Now they both have the key $K = 846$.

3.3 El-Gamal

Alice and Bob want to send messages each other. They have a group G and a basic member g_0 which is known. Alice sends $m \in G$, chooses (secret) e_a, computes $A = g_0^{e_a}$ and sends A to Bob. Bob chooses (secret) e_b, computes $B = g_0^{e_b}$ and sends B to Alice. Then, Alice and Bob each calculates

$g_0^{e_a \cdot e_b}$. Alice send to Bob $c = m \cdot (g_0^{e_a e_b})^{-1}$. Bob calculates $m = c \cdot (g_0^{e_a e_b})^{-1}$.
In the next message different e_a and e_b will be chosen.

3.4 Pohlig-Hellman

Pohlig-Hellman algorithm is a method for computing discrete logarithms in finite fields. Given a cyclic group $G = \langle g \rangle$. We wish to solve the discrete logarithm problem relate to g:
Given $h \in G$, we wish to find $m \in \mathbb{N}$ s.t $g^m = h$.
If $|G| = \prod p_i^{k_i}$ finding m is as hard as finding discrete logarithm in cyclic groups of order p_i for all i.
First, present the order of G by $N = \prod\limits_{i=0}^{n} q_i^{e_i}$ where every q_i is prime.
Second, $\forall 1 \leq i \leq n$, set up $x = a_0 + a_1 \cdot q_i + a_2 \cdot q_i^2 + ... + a_{e_{i-1}} \cdot q_i^{e_{i-1}}$.
Third, $\forall 1 \leq i \leq n$ compute: $g_i = g^{N/q_i^{e_i}}$ and $h_i = h^{N/q_i^{e_i}}$.
By Lagrange's theorem, $ord(g_i) = q_i^{e_i}$ and by construction, $h_i \in \langle g_i \rangle$.
Practically, it holds that $(h)^{\frac{N}{q_i^{e_i-1}}} = (g^x)^{\frac{N}{q_i^{e_i-1}}} = (g^{q_i^{e_i-1}})^{a_0} \cdot (g^{q_i^{e_i}})^{a_1 + a_2 q_i + ... + x_{e_i-1} q_i^{e_i-2}}$ (the main idea in the equation is the order of the group - if $g^x = h$ and the order is e.g q^e then $(g^{q^{e-1}})_0^x = h^{q^{e-1}}$).
Now using an algorithm for solving discrete logarithm in cyclic group $\langle g_i \rangle$ and compute $x_i \in G_i = \{0, 1, ..., q_i^{e_i} - 1\}$ s.t $g_i^{x_i} = h_i$.
Finally, we get an equation system:

$$\begin{aligned} x &= x_1 \pmod{q_1^{e_1}} \\ x &= x_2 \pmod{q_2^{e_2}} \\ &\vdots \\ x &= x_n \pmod{q_n^{e_n}} \end{aligned}$$

Using Chinese remainder theory may solve the equation system, x.

Example:
Let $\mathbb{F} = \mathbb{Z}_{353}^{x}$. We want to solve the equation $3^m = 135$ i.e $m = \log_3 135$.
Notation: $g = 3$, $h = 135$, $p = 353$, $N = p - 1 = 352 = 2^5 \cdot 11$ so we respectively write $q_1^{e_1} = 2^5$ and $q_2^{e_2} = 11^1$.

- Step 1: $i = 1$, $q_1 = 2$, $e_1 = 5$.

$x = 2^0 \cdot x_0 + 2^1 \cdot x_1 + 2^2 \cdot x_2 + 2^3 \cdot x_3 + 2^4 \cdot x_4 \Longrightarrow\ x = (x_4, x_3, x_2, x_1, x_0)$
$g_1 = g^{\frac{N}{q_1^{e_1}}} = 3^{11} = 294 \pmod{353}$, $h_1 = h^{\frac{N}{q_1^{e_1}}} = 135^{11} = 42 \pmod{353}$.
$294^x = 42$, $16 \cdot x = (x_0, 0, 0, 0, 0)$
$(294^{16})^{x_0} = 42^{16}$
$352^{x_0} = 1$
$x_0 = 0 \Longrightarrow x - x_0 = (x_4, x_3, x_2, x_1, 0) \Longrightarrow 8(x - x_0) = (x_1, 0, 0, 0, 0)$
$(294^8)^{x_0} \cdot (294^{16})^{x_1} = 42^8$
$352^{x_1} = 1$
$x_1 = 0 \Longrightarrow x - x_0 - x_1 = (x_4, x_3, x_2, 0, 0) \Longrightarrow 4 \cdot (x - x_0 - x_1) = (x_2, 0, 0, 0, 0)$
$(294^4)^{x_0} \cdot (294^8)^{x_1} \cdot (294^{16})^{x_2} = 42^4$
$352^{x_2} = 1$
$x_2 = 0 \Longrightarrow x - x_0 - x_1 - x_2 = (x_4, x_3, 0, 0, 0) \Longrightarrow 2 \cdot (x - x_0 - x_1 - x_2) = (x_3, 0, 0, 0, 0)$
$(294^2)^{x_0} \cdot (294^4)^{x_1} \cdot (294^8)^{x_2} \cdot (294^{16})^{x_3} = 42^2$

$352^{x_3} = 352$
$x_3 = 1 \Longrightarrow x - x_0 - x_1 - x_2 - x_3 = (x_4, 0, 0, 0, 0)$
$294^{x_0} \cdot (294^2)^{x_1} \cdot (294^4)^{x_2} \cdot (294^8)^{x_3} \cdot (294^{16})^{x_4} = 42$
$311 \cdot 352^{x_4} = 42/ \cdot 311^{-1} = 42$
$352^{x_4} = 42^2$
$352^{x_4} = 352$
$x_4 = 1$
$\Longrightarrow \mathbf{x} = \mathbf{24} \pmod{\mathbf{32}}$

• Step 2: $i = 2$, $q_2 = 11$, $e_2 = 1$.
$x = 11^0 \cdot x_0$
$g_2 = g^{\frac{N}{q_2{}^{e_2}}} = 3^{32} = 140 \pmod{353}$, $h_2 = h^{\frac{N}{q_2{}^{e_2}}} = 135^{32} = 337 \pmod{353}$.
$140^{x_0} = 337$
$\Longrightarrow \mathbf{x} = \mathbf{x_0} = \mathbf{4} \pmod{\mathbf{11}}$

Finally we got an equations system:
$x = 24 \pmod{32}$
$x = 4 \pmod{11}$
Using the Chinese remainder theorem follows to solution: $\mathbf{x} = \mathbf{312}$.
$\Longrightarrow 3^{312} = 135$

3.5 Tonelli-Shanks

Theorem: Let p be an odd prime number and assume that $gcd(a, p) = 1$. Let x be a solution to the equation $x^2 \equiv a \pmod p$, let n and k be integers s.t $p - 1 = 2^n \cdot k$ where $n \geq 1$ and k is odd and let q be a quadratic non-residue modulo p. x may be found by repeating the following loop:
Set $t_0 = a^{\frac{k+1}{2}} \pmod p$ and find the least i which holds $r_0^{2^i} \equiv 1 \pmod p$ where $r_0 = a^k \pmod p$. If $i = 0$ then the solution is $x = \pm t \pmod p$. Else, set $u_0 \equiv q^{k(2^{n-i-1})} \pmod p$, $t_1 = t_0 u_0$ and $r_1 = r_0 u^2$ and repeat the algorithm until $i = 0$.

Example:
Let $p = 641$ and $a = 421$. We want to find x s.t $x^2 \equiv a \pmod p$.
First, we find n and k s.t $p - 1 = 2^n k \pmod p$ where $n \geq 1$ and k is odd. In our example, $n = 7$ and $k = 5$.
Second, we need an arbitrary q that is quadratic non-residue, so we set $q = 3$ and we can see that $3^{320} = 640 \neq 1 \pmod{641}$.
Third, before we go to the iteration we set $t = 421^3 = 292 \pmod{641}$ and $r = 421^5 \pmod{641} = 32$.
Then we find the least i s.t $32^{2^i} = 1 \pmod{641}$ and it follows that $i = 6$.
Since $i \neq 0$, we set $u_1 = 3^{5 \cdot 2^{7-6-1}} = 3^5 = 243 \pmod{641}$ and we set $t_1 = 292 \cdot 243 = 446 \pmod{641}$, $r_1 = 32 \cdot 243^2 = 541 \pmod{641}$.
Computing minimal i again: $541^{2^i} \equiv 1 \pmod{641} \Rightarrow i = 4$
Since $i \neq 0$, $u_2 = 3^{5 \cdot 2^{7-4-1}} = 3^{20} = 160 \pmod{641}$, $t_2 = 446 \cdot 160 = 209 \pmod{641}$, $r_2 = 541 \cdot 160^2 = 154 \pmod{641}$.
Computing minimal i: $154^{2^i} \equiv 1 \pmod{641} \Rightarrow i = 2$
$i \neq 0$, $u_3 = 3^{5 \cdot 2^{7-2-1}} = 3^{80} = 318 \pmod{641}$, $t_3 = 209 \cdot 318 = 439 \pmod{641}$, $r_3 = 154 \cdot 318^2 = 1$ (mod 641).
Computing minimal i: $1^{2^i} \equiv 1 \Rightarrow i = 0$

After all, we got minimal $i = 0$ so the solution is $x = \pm t \pmod{641}$ that is to say $x_1 = 439 \pmod{641}$, $x_2 = 202 \pmod{641}$.

3.6 Baby Step - Giant Step

Given a cyclic group G of order n, a generator g of G and an element h, the problem is to find integer x s.t $g^x = h$ (i.e discrete logarithm). Suppose we know that $0 \leq x < a \cdot b$ for some $a, b \in \mathbb{N}$. We wish to find s, t that holds $0 \leq s < a$ and $0 \leq t < b$ so $x = t \cdot a + s$. Then we may get $h = g^x = g^{ta+s} = (g^a)^t \cdot g^s$ then $h \cdot (g^{-1})^s = (g^a)^t$.
In order to find such s and t, we compute $h \cdot (g^{-1})^s$ for all $0 \leq s < a$, we compute $(g^a)^t$ for all $0 \leq t < b$ and search them in our table.
Searching in our table is in time complexity of $\mathcal{O}(\log a)$. So we have 3 steps:

(1) $\forall 0 \leq s < a$, computing $h \cdot (g^{-1})^s$. Time-complexity: $\mathcal{O}(a)$.

(2) $\forall 0 \leq t < b$, computing $(g^a)^t$. Time-complexity: $\mathcal{O}(b)$.

(3) Searching $(g^a)^t$ in our table. Time-complexity: $\mathcal{O}(b \log a)$.

There are $a + b$ multiplications and $b \log a$ searches. Thus, we want to find a and b s.t $a = b$ so if we know that $x < N$, a and b holds $a = b = \sqrt{N}$. Therefore, the time-complexity is $\mathcal{O}(\sqrt{N})$.
The algorithm is useful for 2 things:
• If $N = \mathrm{ord}(g)$, there is solution for the equation $g^x = h$ for $0 \leq x < N$.
• Suppose we know that $m \leq x < M$. Then: $0 \leq x' < M - m$ for $x' = x - m$ and the equation is: $g^{m+x'} = h$ or $g^{x'} = h \cdot g^{-m} = h'$. when $0 \leq x' < M - m = N$ we do it as above.

3.7 Karatsuba

Suppose that we have two polynomials $f(x) = \sum\limits_{i=0}^{2n-1} a_i x^i$ and $g(x) = \sum\limits_{i=0}^{2n-1} b_i x^i$ of length of $2n$. It is easy to add or extract (and is of $\mathcal{O}(n)$) but multiplication is of $\mathcal{O}(n^2)$. Karatsuba algorithm might simplifies it to $\mathcal{O}(n^{\log_2 3})$. When we multiply $f \cdot g$ we get a polynomial of length of about $4n$. So first we want to write: $f \cdot g = (f_0 + x^n f_1)(g_0 + x^n g_1) = f_0 \cdot g_0 + (f_0 \cdot g_1 + f_1 \cdot g_0)x^n + f_1 \cdot g_1 x^{2n}$.
In fact, we inverted a multiplication of 2 polynomials of length of $2n$ to 4 multiplications of polynomials of length of n. But, we may also write:
$f_0 \cdot g_1 + f_1 \cdot g_0 = (f_0 + f_1)(g_0 + g_1) - f_0 \cdot g_0 - f_1 \cdot g_1$ that gives us 3 multiplications instead of 4. The ideal is when $n = 2^k$. The multiplication is performed in k steps, every step takes 3 multiplications and 3^k multiplications in total ($3^k = (2^k)^{\log_2 3} = n^{\log_2 3}$).

3.8 Montgomery Modular Multiplication

Some mathematicians likely to say that adding 1 and extracting 1 (that is equivalent to add 0) is one of the oldest tricks , for example: $\int \frac{x^{n+1}}{x-1}\ dx\ = \int \frac{x^{n+1}-1+1}{x-1}\ dx = \int x^n + x^{n-1} + ... + 1 + \frac{1}{x-1}\ dx$ that is easy to solve now. Montgomery modular multiplication does not solve any integral but I would say that it follows the trick above.
Let's say that $\mathbb{F} = \mathbb{Z}_{97}$, $\frac{40}{2} = 20$ (that was easy to compute). What about $\frac{13}{2}$?
Intuition: let n be a positive integer. Under the quotient ring $\mathbb{Z}/_{n\mathbb{Z}}$, for every $0 \leq a < n$, all the numbers in the following set are equals to a: $\{a + kn \mid k \in \mathbb{Z}\}$.
We can use Euclid's algorithm to find 2^{-1} but we can simplify it by adding 97 (which equals 0),

$\dfrac{13}{2} = \dfrac{13+97}{2} = \dfrac{110}{2} = 55 \pmod{97}$.
Generally, we wish to compute $\dfrac{n}{R} \pmod{p}$.
Computing x s.t $R \mid n + px$, then $\dfrac{n}{R} = \dfrac{n+px}{R} \pmod{p}$. The equation is: $n + px \equiv 0 \pmod{R}$.
$\Rightarrow \; x = -n \cdot p^{-1} \pmod{R}$.

3.8.1 Montgomery Reduction

Represent every $a \in \mathbb{Z}_p$ by $a_R = a \cdot R \pmod{p}$ (that is called **Montgomery form**), choosing R greater than p. When we run the algorithm on computer, we'd choose R to be power of 2 and when we want to write it on paper, we'd choose R to be power of 10. Arithmetic:
• Adding: $X_R + Y_R = X \cdot R + Y \cdot R = (X+Y)R = (X+Y)_R = X_R +_R Y_R$.
• Multiplication:$\dfrac{X_R \cdot Y_R}{R} = \dfrac{(X \cdot R) \cdot (Y \cdot R)}{R} = (X \cdot Y)R = (X \cdot Y)_R = X_R \cdot_R Y_R$.
• "Regular" multiplication: $z = x_R \cdot y_R$, doing Montgomery reduction: searching u s.t $R \mid z + u \cdot p$, $u = -z \cdot p^{-1} \pmod{R}$.

$$x_R \cdot y_R = \begin{cases} \frac{z+u \cdot p}{R} & , x_R \cdot y_R < p \\ \\ \frac{z+u \cdot p}{R} - p & , \; x_R \cdot y_R \geq p \end{cases}$$

Example:
$p = 7$, $R = 10$, we compute $p^{-1} = 3 \pmod{R}$.
We wish to compute $6 \cdot 4 \pmod{7}$:

(a) Computing Montgomery forms:
$6 \cdot R = 6 \cdot 10 = 60 = 4 \pmod{7}$
$4 \cdot R = 4 \cdot 10 = 40 = 5 \pmod{7}$
Then, $6_R = 4$, $4_R = 5$.

(b) Computing:
$(6 \cdot 4)_R = 6_R \cdot_R 4_R = 4 \cdot_R 5$
$z = 4 \cdot 5 = 20$
$u = -z \cdot 3 \pmod{10} = 0 \implies \frac{z+u \cdot p}{R} = \frac{20+0 \cdot 7}{10} = \frac{20}{10} = 2$ (there will never be a remainder)
$2 < 7$, so $6_R \cdot_R 4_R = 2$

(c) For getting $6 \cdot 4$ we want to compute $2 \cdot R^{-1} \pmod{p}$:
reducing: $z = 2$, $u = -2 \cdot 3 = 4 \pmod{10}$
$10 \mid z + 4 \cdot 7 = 2 + 28 = 30$
$6 \cdot 4 = \frac{30}{10} = 3$ and it does hold $6 \cdot 4 = 3 \pmod{7}$

4 Elliptic Curves

4.1 Intro

<u>Definition</u>: Let $\mathbb{F}$ be a field. An **elliptic curve** is the equation $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{F}$.
The group of an elliptic curve is $E(F) := \{(x, y) \in \mathbb{F}^2 \mid y^2 = x^3 + ax + b, \; a, b \in \mathbb{F}\} \cup \{\infty\}$ (usually denoted E).
The set E has a structure of an abelian group:

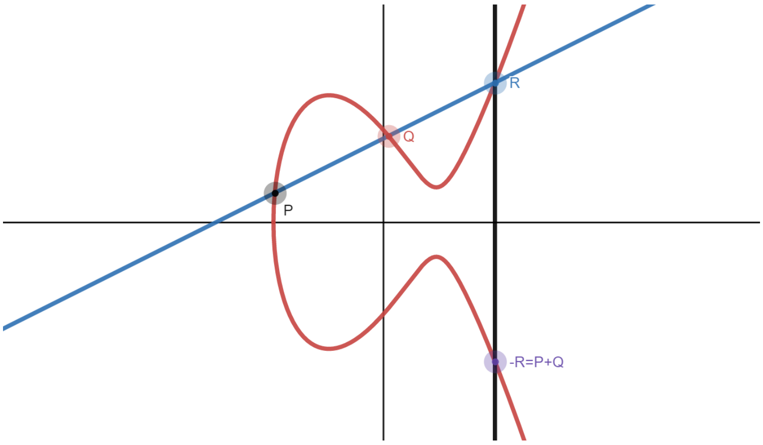

Figure 1: elliptic curve

- A binary operation is denoted by "+".
- ∞ is the identity element.
- $-(\alpha, \beta) = (\alpha, -\beta)$.
- If P $= (\alpha_1, \beta_1)$ and Q $= (\alpha_2, \beta_2)$ are points in E:
  Case (a): $\alpha_1 = \alpha_2$, $\beta_1 = -\beta_2$. Then, P + Q $= \infty$ (actually, if $\alpha_1 = \alpha_2$, β_1 must be equal to β_2).
  Case (b): $\alpha_1 \neq \alpha_2$. Then, P + Q $=$ −R (as we can see in figure 1).
  Case (c): P = Q. Then, P + Q = 2P = −R.

How practically we sum 2 points on elliptic curve:
Let E : $y^2 = f(x)$ be an elliptic curve over field $\mathbb{F}$ and let $P = (\alpha_1, \beta_1)$, $Q = (\alpha_2, \beta_2)$ be points on E. We wish to compute $-R = P + Q$. Denote the line that goes through P and Q by $y = \lambda x + \mu$. The incline is $\lambda = \frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1} \in \mathbb{F}$, then $\mu = \beta_1 - \lambda\alpha_1 \in \mathbb{F}$.
So far we have an elliptic curve $y^2 = f(x)$ and a line $y = \lambda x + \mu$ that what they have in common is our 2 points that we know (P and Q) and the point the we wish to find, R. So we want to solve the equation $f(x) - (\lambda x + \mu)^2 = 0$. The roots of the equation are $\alpha_1, \alpha_2, \alpha_3$ where $\alpha_1, \alpha_2 \in \mathbb{F}$ and $-R = (\alpha_3, -\beta_3)$.
$\Rightarrow f(x) - (\lambda x + \mu)^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$
$\Rightarrow \alpha_1 + \alpha_2 + \alpha_3 = -(\text{the coefficient of } x^2) = \lambda^2$
$\Rightarrow \alpha_3 = \lambda^2 - \alpha_1 - \alpha_2, \quad \beta_3 = \lambda \cdot \alpha_3 + \mu.$
$\Rightarrow (\alpha_3, \beta_3) = \big(\lambda^2 - \alpha_1 - \alpha_2, \lambda(\lambda^2 - \alpha_1 - \alpha_2) + \mu\big)$
Don't forget that y-coordinate is $(-\beta_3)$.
$\Rightarrow -R = P + Q = \big(\lambda^2 - \alpha_1 - \alpha_2, -\lambda(\lambda^2 - \alpha_1 - \alpha_2) - \mu\big)$

Example:
Let $\mathbb{F}_{11}$ be a field, $y^2 = x^3 - x + 1$ be an elliptic curve E and $P = (2, 5)$, $Q = (1, 10)$ be points on E. We wish to find a point R on E s.t $-R = P + Q$.
The line that goes through P and Q is $y = \lambda x + \mu$, so $\lambda = \frac{10-5}{1-2} = \frac{1}{2} = 6$ and then $5 = 6 \cdot 2 + \mu \Rightarrow \mu = -7 \Rightarrow \mu = 4$.
$\Rightarrow -R = \big(6^2 - 2 - 3, -3(6^2 - 2 - 3) - 4\big) = (9, -9)$
$\Rightarrow -R = (9, 2)$

4.2 Algebraic Geometry

Definition: Let $\mathbb{F}$ be a field. The n-dimensional **projective space** is $\mathbb{P}^n(\mathbb{F}) = \frac{\mathbb{F}^{n+1}\setminus\{0\}}{\sim}$ where $\sim$ is the equivalent relation - $v \sim u \iff v = \alpha \cdot w$ for some $0 \neq \alpha \in \mathbb{F}$.
Under the map $v \longmapsto \text{span}(v)$, $\mathbb{P}^n(\mathbb{F}) = \{l \mid l$ is a line that goes through 0 in $\mathbb{F}^{n+1}\}$.

Notations:
The equivalent class of $(x_1, x_2, ..., x_n) \in \mathbb{F}^{n+1}$ is denoted $[x_1 : x_2 : ... : x_n]$.
Let A= $\{(x_1 : x_2 : ... : x_n) \mid x_n \neq 0\}$ and let B= $\{(x_1, x_2, ..., x_n) \mid x_n = 0\}$. Therefore, we generally write $\mathbb{P}^n(\mathbb{F}) = A\dot{\cup}B$.
$V(f) = \{f(x_0, ...x_{n-1}) = 0 \mid x_0, ...x_{n-1} \in \mathbb{F}$, f is a polynom$\}$.

Proposition:

(a) There exists a bijection map, $\mathbb{F}^n \longmapsto A$, $(x_1, x_2, ..., x_{n-1}) \longmapsto (x_1 : x_2 : ... : x_{n-1} : 1)$.

(b) There exists a bijection map, $\mathbb{P}^{n-1} \longmapsto B$, $(x_1, x_2, ..., x_{n-1}) \longmapsto (x_1 : x_2 : ... : x_{n-1} : 0)$.
Therefore, $\mathbb{P}^n(\mathbb{F}) = \mathbb{F}^n \cup \mathbb{P}^{n-1}(\mathbb{F})$.

Definition: Let $f \in \mathbb{F}[x_0, ..., x_n]$. f is said to be **homogeneous** of degree r if $f(\alpha v) = \alpha^r f(v)$.
Corollary: $f(x_0, ..., x_n) = 0 \iff f(\alpha x_0, ..., \alpha x_n) = 0$, $\alpha \neq 0$. Thus, for homogeneous function f, it is well defined, $V(f) = \{(x_0 : ... : x_n) \in \mathbb{P}^n(\mathbb{F}) \mid f(x_0, ..., x_n) = 0\}$.

Let $f \in \mathbb{F}[x_0, ..., x_{n-1}]$, $V(f) \subseteq \mathbb{F}^n \subseteq \mathbb{P}^n(\mathbb{F})$. We wish to find homogeneous function g s.t $V(g) \cap \mathbb{F}^n = V(f)$. Solution: **homogenization**.
$g(x_0, ..., x_n) = f(\frac{x_0}{x_n}, ..., \frac{x_{n-1}}{x_n}) \cdot x_n^r$ where r is big enough so that all the denominator will be disappeared.
Example:
Let $f(x, y) = y^2 - (x^3 + ax + b)$. Adding z follows to: $g(x, y, z) = [(\frac{y}{z})^2 - ((\frac{x}{z})^3 + a \cdot \frac{x}{z} + b)] \cdot z^3 \Longrightarrow g(x, y, z) = y^2 z - (x^3 + axz^2 + bz^3)$.
Remark: $f(x_0, ..., x_{n-1}) = g(x_0, ..., x_{n-1}, 1)$. A point in $V(g) \cap \mathbb{F}^n$ is $(x_0, ..., x_{n-1}, 1)$ s.t $f(x_0, ..., x_{n-1}) = g(x_0, ..., x_{n-1}, 1) = 0$ that is to say $x_0, ..., x_{n-1} \in V(f)$.

Definition: $V(g)$ is said to be the **projection** of $V(f)$ and $V(g) \setminus V(f)$ are the points at ∞ of $V(f)$.
The points in ∞ of an elliptic curve are the points that given by setting $z = 0$:
$f(x, y) = y^2 - (x^3 + ax + b)$, $g(x, y, z) = y^2 x - (x^3 + axz^2 + bz^3)$.
$g(x, y, 0) = -x^3$.
Then the point at ∞ is $(0 : y : 0) = (0 : 1 : 0)$.

4.2.1 Clearing Denominators in Projective Coordinate

We saw that for polynomial $p(x) = \sum\limits_{i=0}^{n} a_i x^i$ the homogenization of $p(x)$ is $g(x, y) = \sum\limits_{i=0}^{n} a_i x^i y^{n-i}$.

Now we want to describe the homogenization of rational function: let $f(x) = \dfrac{P(x)}{Q(x)} = \dfrac{\sum\limits_{i=0}^{n} a_i x^i}{\sum\limits_{j=0}^{m} b_j x^j}$ be a rational function. The homogenization of degree $\max\{n, m\}$ (without loss of generality $n \geq m$) is:

$h(x,y) = \dfrac{\sum\limits_{i=0}^{n} a_i x^i y^{n-i}}{\sum\limits_{j=0}^{m} b_j x^j y^{n-j}}$. It is well-define on $\mathbb{P}^1(\mathbb{F})$ because it is homogeneous of degree 0,
$h : \mathbb{P}^1(\mathbb{F}) \to \mathbb{F} \subseteq \mathbb{P}^1(\mathbb{F})$.

$$(x : y) \to h(x,y) \to \big(h(x,y) : 1\big) = \left(h(x,y) = \frac{\sum\limits_{i=0}^{n} a_i x^i y^{n-i}}{\sum\limits_{j=0}^{m} b_j x^j y^{n-j}}\right) = \Big(\sum_{i=0}^{n} a_i x^i y^{n-i} : \sum_{j=0}^{m} b_j x^j y^{n-j}\Big).$$

Example:
$f(x) = \frac{x^2+1}{x-1} \implies h(x,y) = \frac{x^2+y^2}{xy-y^2}$,
$\mathbb{P}^1 \xrightarrow{h} \mathbb{P}^1$, $(x : y) \xrightarrow{h} (x^2+y^2 : xy - y^2)$
$1 \to (1:1) \to (1^2+1^2 : 1 \cdot 1 - 1^2) = (2:0) = \infty$

4.3 Zeros and Poles

Definition: Let $f(x)$ be a rational function (can be polynomial as well). A root α of f is called **zero of order n** if $f(\alpha) = f^{(1)}(\alpha) = ... = f^{(n-1)}(\alpha) = 0$ and $f^{(n)}(\alpha) \neq 0$.
Definition: Let $f(x)$ be a rational function. α is called **pole of order n** if $\lim\limits_{x\to\alpha} f(x) = \infty$ and n is the minimal which $\lim\limits_{x\to\alpha} (x-\alpha)^n f(x)$ exists.
Definition: $(x-\alpha)$ is called **uniformizing parameter**.
Remark: Every $f(x) \in F[x]$ can be written by $f(x) = (x-\alpha)^n \cdot f_0(x)$ where $f_0 \neq 0$ is well-defined. When f_0 is defined and $f_0 \neq 0$, $n \in \mathbb{Z}$ is unique.
The order of f at α is denoted $\text{ord}_\alpha(f) = n$.
- If $n > 0$, then α is zero.
- If $n < 0$, then α is a pole.

Example:
For $\alpha = 2$, $f(x) = \frac{(x-2)^2(x-1)}{x-7} = (x-2)^2 \cdot \dfrac{x-1}{x-7}$, $f_0(x) = \dfrac{x-1}{x-7}$.

4.4 Hyper-Elliptic Curves

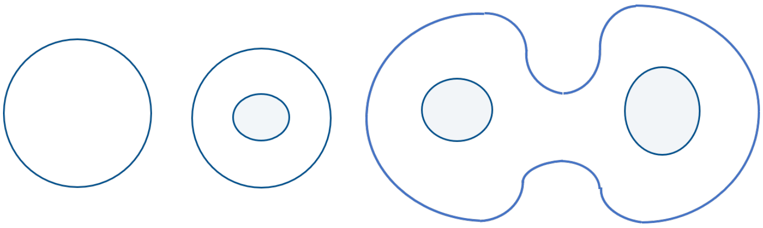

Figure 2: 0 genus, 1 genus and 2 genus

‘ Definition: The **genus** of a surface is the number of ”holes” it has (see figure 2).
Definition: Let $\mathbb{F}$ be an algebraically closed field, $f \in \mathbb{F}$. E: $y^2 = f(x)$ is called an **hyper-elliptic curve** where $3 \leq \deg(f) = 2g+1$ and f is monic-polynomial.
Definition: **Polynomial function** on E is a polynomial $p(x,y) \in \mathbb{F}[x]$ reduced to E.

Proposition: Every polynomial function $p(x,y)$ can be written by $p(x,y)=a(x)+b(x)y$ where $a(x),b(x)\in\mathbb{F}[x]$.
Definition: **Rational function on E** is a quotient of two polynomial functions, $a=\frac{P}{Q}$, $Q\neq 0$.
Remark: A polynomial function a on E is defined on (α,β) if it has representation of $u=\frac{P}{Q}$ s.t $Q(\alpha,\beta)\neq 0$.
Defintion: Let $P=a(x)+b(x)y$ be a rational function on some E. The **conjugate of P** is $\overline{P}=a(x)-b(x)y$, the **norm** of P is $N(P):=P\cdot\overline{P}=a^2-b^2y^2=a^2-b^2f\in\mathbb{F}[x]$ and the **conjugate point** to $(\alpha,\beta)\in E(F)$ is $-(\alpha,\beta)=(\alpha,-\beta)$.
Proposition: If P is polynomial function then $\overline{P}(\alpha,\beta)=P(-(\alpha,\beta))$.
Theorem: For all $(\alpha,\beta)\in E(F)$ there exists uniformizing parameter $u=u_{(\alpha,\beta)}$ s.t for all polynomial function P, exists one and only $s=\text{ord}_{(\alpha,\beta)}(P)$ s.t $P=u^s\cdot h$, h is rational function defined at (α,β) and is not zeroed there.
Notation: **F[E]** is a set of all polynomials function over E.
F(E) is a set of all rational functions over E.
Definition: A function e_v (sometimes it is denoted V) is called **evaluation** if it holds:

(a) $e_v(x+y)\geq\min\{e_v(x),e_v(y)\}$.

(b) $e_v(xy)=e_v(x)+e_v(y)$

Proposition: If V is an evaluation and $V(P)\neq V(Q)$ then $V(P+Q)=\min\big(V(P),V(Q)\big)$.
Theorem: The function $e_v=\text{ord}_{(\alpha,\beta)}:F[E]\to\mathbb{Z}\cup\{\infty\}$ where $\text{ord}_{(\alpha,\beta)}(0)=\infty$ is evaluation.

4.5 Orders and Divisors

Definitions: Let E be an elliptic curve over algebraically closed field $\mathbb{F}$.

- **Divisor over E** is the finite sum $D=\sum_{i=1}^{k}n_iP_i$ where $n_1,...,n_k\in\mathbb{Z}$ and $P_1,...,P_k\in E(\mathbb{F})$.
- The **degree of D**, denoted deg$D$ is the integer $\sum_{P\in E}n_P$.
- The **order of D** at a point P is the integer $n_P=\text{ord}_P(D)$.

Example:
$\mathbb{F}=\mathbb{C}$, E : $y^2=x^3+3x$ with points $P_1=(0,0)$, $P_2=(1,2)$, $P_3=(1,-2)$, $P_4=(\infty)$.
A divisor on E is:
$3P_1-2P_2+7P_3+6P_4=3\big((0,0)\big)-2\big((1,2)\big)+7\big((1,-2)\big)+6(\infty)$.
It is an additive group denoted $\mathbb{D}$.
$[2(0,0)+3(\infty)]+[5(1,2)-6(\infty)]=2(0,0)+5(1,2)-3(\infty)$.

Proposition: The set of all divisors on an elliptic curve E, denoted $\mathbb{D}$, forms an additive group under addition rule:
$\sum_{P\in E}m_PP+\sum_{P\in E}n_PP=\sum_{P\in E}(m_P+n_P)P$.
The set of all divisors of degree 0, denoted $\mathbb{D}^0$, is a subgroup of $\mathbb{D}$.
Definition: Let $g\in F(E)$. The divisor of g is defined by $(g)=\text{div}(g)=\sum_{P\in E}\text{ord}_P(g)\cdot(P)$.

Examples:

(a) E : $y^2=x^3+3x$
$(x)=\text{ord}_{(0,0)}x\cdot(0,0)+\text{ord}_\infty x\cdot(\infty)=2(0,0)-2(\infty)$.

Here $g := x$, thus g has one zero at $\alpha = 0$ and the point is $P = (0,0)$ that is to say, $P = -P$ so $\mathrm{ord}_P(0,0) = 2$ and we therefore reduce 2 times the point in infinity.

(b) $l(x,y) = y - (\lambda x + \mu)$
$(l) = (P) + (Q) + (R) - 3(\infty)$

Proposition: Let E be an elliptic curve over $\mathbb{F}$ and assume $g, h \in F(E)$ so $(g), (h)$ are divisors on E

(a) $(gh) = (g) + (h)$.

(b) if g is function of variable x only, $g = a \prod (x - \alpha_i)^{n_i}$ then
$(g) = \sum\limits_{i, f(\alpha) \neq 0} \big[n_i(\alpha_i, \beta_i) + n_i(\alpha_i, -\beta_i)\big] + \sum\limits_{i, f(\alpha_i) = 0} 2n_i(\alpha_i, 0) - 2\sum\limits_i n_i(\infty)$.

(c) $\deg\big((g) + (h)\big) = \deg(g) + \deg(h)$.

(d) if $g \neq 0$ then $\deg(g) = 0$.

4.6 Elliptic Curves over $\mathbb{C}$

Definition: **Lattice** over $\mathbb{C}$ is sub-group of the group over $\mathbb{C}$ with addition that generated by two elements, w_1, w_2 which are linear-independence in $\mathbb{C}$ as linear space over $\mathbb{R}$.
$\mathcal{L} = \{n \cdot w_1 + m \cdot w_2 \mid n, m \in \mathbb{Z}\}$. $\mathcal{L} \leq \mathbb{C}$ is sub-group and the quotient is $\mathbb{C}/\mathcal{L}$.
Theorem:
(1) For all lattice L, there exists functions $P, P' : \mathbb{C}/L \to \mathbb{C} \cup \{\infty\}$ s.t (P, P') is bijection from $\mathbb{C}/L$ to an elliptic curve.
(2) Under addition over E, it is isomorphism.
(3) Every elliptic curve is thus obtained.
E : $y^2 = 4x^3 - 6 \circ G_4 x - 14 \circ G_6$ where G_4, G_6 are constants which depends on L.
Definition: Let w_1, w_2 be complex numbers that are linear independent over $\mathbb{R}$ and let $\mathcal{L}$ be the lattice generated by w_1, w_2. Then, **Weierstrass $\mathcal{P}$-function** is defined by:
$\mathcal{P}_{\mathcal{L}}(z) = \dfrac{1}{z^2} + \sum\limits_{\substack{w \neq 0 \\ w \in \mathcal{L}}} \big(\dfrac{1}{z - w} - \dfrac{1}{w^2}\big)$.
Properties of Weierstrass $\mathcal{P}$-function:
Given a lattice $\mathcal{L}$ and Weierstrass $\mathcal{P}$-function, the following holds:
• The derivation is of P is: $P' = -2 \sum\limits_{w \in L} \frac{1}{(x-w)^3}$.
• P has a pole of order 2 at each lattice point (it followed by the construction).
• P is an even function.

Example:
Let $w_1 = 1$, $w_2 = i$. Then, $\mathcal{L} = \{n + mi \mid n, m \in \mathbb{Z}\}$.
$P'_L(z) = \sum\limits_{n,m \in \mathbb{Z}} \frac{1}{(z-n-mi)^3}$
For all $w' \in L$, it holds $P'_L(z + w') = P'_L(z)$ and actually $P_L(z + w') = P_L(z)$ as well.
$\Rightarrow (P')^2 = 4P^3 - 6 \cdot G_4 P - 14 \cdot G_6$
$\Rightarrow G_{2k} = G_{2k}(L) = \sum\limits_{0 \neq w \in L} \frac{1}{w^{2k}}$
It follows that the value of the functions P, P' is ∞ exactly at the points in L that is $0 \in \mathbb{C}/L$ goes to ∞.

4.7 Number of Points on Elliptic Curve

Suppose $\mathbb{F}_q$ be a finite field with $q = p^r$ elements where p is prime. We wish to find the order of E: $|E(\mathbb{F}_q)| = |\{(x, y) \in \mathbb{F}_q^2 : y^2 = x^3 + ax + b,\ a, b \in \mathbb{F}_q\}| + |\{\infty\}| = ?$
Any $x \in \mathbb{F}_q$ there is q possibilities. Every x has one possibility for y "in average", rather half of the elements in $\mathbb{F}_q$ has a root for $x^3 + ax + b$ and every such a root contribute 2 points. In average, there are $q + 1$ points.
Hasse Theorem: Let $E(\mathbb{F}_q)$ be an elliptic curve over a finite field $\mathbb{F}_q$ $(q = p^r)$. Then $|E(\mathbb{F}_q)| = q+1-a$ where $|a| \leq 2\sqrt{q}$.

4.7.1 Zeta Function

Let E be an elliptic curve over a finite field $\mathbb{F}_q$, $N_q = |E(\mathbb{F}_q)|$, for all $r \geq 1$, $\mathbb{F}_q \subset \mathbb{F}_{q^r}$. Then we may define **zeta function** to be $\zeta(E/\mathbb{F}_q : T) = \exp(\sum\limits_{r=1}^{\infty} \frac{N_{q^r} T^r}{r})$.
Similarly, it is possible to define it for all projective variety, that is for all set in $\mathbb{P}^n$ that is defined by equations.
Example:
$Z(\mathbb{P}^n/\mathbb{F}_q : T)$
$N_q = |\mathbb{P}^n(\mathbb{F}_q)| = |\frac{\mathbb{F}_q^{n+1} \backslash \{0\}}{\sim}| = \frac{q^{n+1}-1}{q-1} = \sum\limits_{i=0}^{n} q^i$ (the second equations is because of multiplying $\mathbb{F}_q^{\times}$).
Computing:
$\sum\limits_{r=1}^{\infty} \frac{N_{q^r} T^r}{r} = \sum\limits_{r=1}^{\infty} \frac{T^r}{r} \sum\limits_{i=0}^{n} q^{ri} = \sum\limits_{i=0}^{n} \sum\limits_{r=1}^{\infty} \frac{(q^i T)^r}{r} = \sum\limits_{i=0}^{n} -\log(1 - q^i T)$
Then,
$\zeta(\mathbb{P}^n/\mathbb{F}_q : T) = \exp\big(\sum\limits_{i=0}^{n} -log(1 - q^i T)\big) = \prod\limits_{i=0}^{r} \frac{1}{1-q^i T} = \frac{1}{(1-T)(1-qT)...(1-q^n T)}$

4.7.2 Weil Conjecture

(a) V is an N-dimensional projective space.

(b) $Z\big(V/\mathbb{F}_q, T\big)$ is rational function of T.

(c) Rational equation: there exists $\varepsilon \in \mathbb{Z}$ that is called **Euler's characteristic** of V that holds:
$Z\big(V/\mathbb{F}_q, \frac{1}{q^N}\big) = \pm q^{\frac{\varepsilon}{2} \cdot N} Z\big(V/\mathbb{F}_q, T\big)$.

(d) there exists polynomials $P_i(T) \in \mathbb{Z}(T)$ for $q \leq i \leq 2N$ that holds:
$Z\big(V/\mathbb{F}_q, T\big) = \dfrac{P_1(T)P_3(T)...P_{2N-1}(T)}{P_2(T)P_4(T)...P_{2N}(T)}$ and P_i can be composite over $\mathbb{C}$, $P_i(T) = \prod\limits_{j=1}^{b_i} (1-\alpha_{ij}T)$, $|\alpha_{ij}| = q^{\frac{i}{2}}$.

Remark: b_i is called **Betti number** of V.

4.7.3 Finite Extension of of Finite Field

Here we wish to compute the number of points of an elliptic curve over large finite field according to small field.
Let E be an elliptic curve over a small field $\mathbb{F}_q$ where we can easily compute the number of points of E (denoted N_q). Let $t = 1 + q - N_q$ and write $x^2 - tx + q = (x - \alpha)(x - \beta)$. Then, for every r,

$|E(\mathbb{F}_{q^r})| = (1-\alpha^r)(1-\beta^r)$.

Example:
Let $\mathbb{F} = \mathbb{F}_7$ be field of 7 elements and let $E: y^2 = x^3 + 2x + 3$. We wish to find the number of points of E over $\mathbb{F}_{49}$, N_{7^2}.
$N_7 = 6$ so $t = 1 + 7 - 6 = 2$.
Then, $x^2 - 2x + 7 = (x-\alpha)(x-\beta) \Rightarrow -2x + 7 = -(\alpha+\beta) + \alpha\beta$
$\Rightarrow \alpha + \beta = 2$
$\alpha\beta = 7$
Now we can compute $N_{49} = |E(\mathbb{F}_{49})| = (1-\alpha^2)(1-\beta^2)$
$\Rightarrow N_{49} = 1 - (\alpha^2 + \beta^2) + \alpha^2\beta^2$
But, $\alpha^2\beta^2 = 49$ and $\alpha^2 + \beta^2 = (\alpha+\beta)^2 - 2\alpha\beta = -10$
So we got that $N_{49} = 1 + 10 + 49 = 60$.

4.7.4 The "Super Naive" Algorithm

Let $E: y^2 = f(x)$ be an elliptic curve over $\mathbb{F}_q$. For all $x \in \mathbb{F}_q$, we compute $\big(f(x)\big)^{\frac{q-1}{2}} = \pm 1$. Hence, $|E(\mathbb{F}_q)| = 1 + \sum\limits_{x \in \mathbb{F}_q} \big(1 + f(x)^{\frac{q-1}{2}}\big)$.
Time complexity is greater than q.

4.7.5 The "Naive" Algorithm

Here we simplify it by baby step - giant step algorithm.
According to Hasse theorem holds $|E(\mathbb{F}_q)| = q + 1 - a$ and $|a| \le 2\sqrt{q}$.
• Find a point on E, $P \in E(\mathbb{F}_q)$ (randomly choose $x \in \mathbb{F}_q$ and compute $f(x)^{\frac{q-1}{2}}$ until we get 1, then compute $\sqrt{f(x)}$ by Tonelli-Shanks).
• Search $q + 1 - 2\sqrt{q} \le n \le q + 1 + 2\sqrt{q}$ s.t $nP = 0$.
If there is one n and only, then $|E(\mathbb{F}_q)| = n$.
Else, find another point, P' and compute nP'. If there is only one n from all the n we have already found, we've done. Else, we try again with another point with all the n from the last iteration.
• Finding n: $n = q + 1 - a$, $|a| \le 2\sqrt{q}$.
$nP = 0 \iff (q+1)P = aP$.
This is discrete log problem which $-2\sqrt{q} \le a \le 2\sqrt{q}$ is known. Thus, baby step - giant step allows to solve it in time complexity of $\mathcal{O}\big(2\sqrt[4]{q} \cdot (\log q)^r\big)$.

4.7.6 Schoof

Schoof's algorithm is based on properties of Frobenius on elliptic curves. Reminder: If $\mathbb{F}$ is field of characteristic p, there is homomorphism $\mathrm{Fr}: \mathbb{F} \to \mathbb{F}$ defined by $\mathrm{Fr}(x) = x^p$. Similarly, if $q = p^r$, $\mathrm{Fr} = (\mathrm{Fr})^r$ is well defined and homomorphism which we denote $\mathrm{Fr}_q = x^q$. It holds $\mathrm{Fr}(x) = x \iff x \in \mathbb{F}_q$.
Corollary: Let $E/\mathbb{F}_q$, E: $y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_q$ and suppose $\mathbb{F}_q \subset L$, $P = (\alpha, \beta) \in E(L)$. Then $\mathrm{Fr}_q(P) = (\alpha^q, \beta^q) \in E(L)$.
Generally, if $g \in \mathbb{F}_q[x]$, then for all $\gamma \in L$, $\mathrm{Fr}_q(g(\gamma)) = g(\mathrm{Fr}(\gamma))$.
Corollary: If $P_1, P_2 \in E(L)$ (where $E/\mathbb{F}_q$) then $\mathrm{Fr}_q(P_1 + P_2) = \mathrm{Fr}_q(P_1) + \mathrm{Fr}_q(P_2)$ where $\mathrm{Fr}_q(\infty) = \infty$.
Theorem: If $E/\mathbb{F}_q$ is en elliptic curve and $|E(\mathbb{F}_q)| = q + 1 - a$, then for all $P \in E(L)$ and for all $\mathbb{F}_q \subset L$ holds $\mathrm{Fr}_q^2(P) - a\mathrm{Fr}_q(P) + q \cdot P = 0$ (*).

Remark: For $P \in E(\mathbb{F}_q)$ it is clear that $\mathrm{Fr}_q(P) = P$ so the the theorem says that $P - a \cdot P + q \cdot P = 0$ i.e $(1 + q - a)P = 0$ and it is known that $|E(\mathbb{F}_q)| = 1 + q - a$.

Schoof's idea:
(1) For all $P \in E(L)$, (*) gives an equation on a and it allows to find a and hence to find $|E(\mathbb{F}_q)|$.
(2) It is better to check (*) even for P that holds $l \cdot P = 0$ where l is prime.
Remark: if $l \cdot P = 0$ then $l \cdot \mathrm{Fr}_q(P) = 0$ as well. Therefore, (*) determine a only in modulo l, but by checking l options only.
(3) Doing it for many such small l's - $l_1, l_2, ...l_k$.
Chinese remainders theorem gives us $a \pmod{l_1 \cdot l_2 \cdot ... \cdot l_k}$. If $4\sqrt{q} < l_1 \cdot ... \cdot l_k$, $a \pmod{l_1 \cdot ... \cdot l_k}$ and $|a| \leq 2\sqrt{q}$ then it is allowed to find a singly.
Time complexity: $\overset{\sim}{\mathcal{O}}(\log^5 n)$.

4.8 Torsion points

Definition: Let E elliptic curve over a field $\mathbb{F}$. The **division polynomial** of order n is a polynomial $f_n(x)$ that its roots are all the x coordinate of all the points of order n where n is odd.
Remark: The points of order 2 are obtained where y=0.
What is the degree of f_n?
Depends on the order of $E[n] = \{R \in E(L) \mid n \cdot R = 0, F \subset L\}$.
Proposition: Let $\mathbb{F} = \mathbb{C}$. Then, $E[n] \cong \mathbb{Z}_n^2$.

Corollary: $\big|E(\mathbb{C})[n]\big| = n^2$ and $\deg(f_n) = \begin{cases} \dfrac{n^2-1}{2} & , n \in 2\mathbb{N}+1 \\ \dfrac{n^2-4}{2} & , n \in 2\mathbb{N} \end{cases}$ $\qquad mm$

4.8.1 Recursion Formulas of Division Polynomials

$$\mathrm{char}(\mathbb{F}) > 3, \quad y^2 = x^3 + ax + b, \quad F(x) = 4(x^3 + ax + b)$$

$$f_0 = 0, \qquad f_1 = 1, \qquad f_2 = 1, \qquad f_3 = 3x^4 + 6ax^2 + 12bx - a^2$$

$$f_4 = 2(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$$

$$f_{2m} = (f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2)f_m, \quad m > 2$$

$$f_{2m+1} = \begin{cases} f_{n+1}f_m^2 - F^2 f_{m-1}f_{m+1}^3, & 2 \not| \, m \geq 3 \\ F^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3, & 2|m \geq 2 \end{cases}$$

5 Primes

Given a number $p \in \mathbb{N}$ we want to know whether p is prime or composite number in order to choose group with order that is not composite. In this section we wish to describe some primality tests.

5.1 Fermat Test

As we have seen before Fermat's little theorem says: if p is prime, then for all $a \in \mathbb{Z}_p$ holds $a^{p-1} \equiv 1 \pmod{p}$. So Fermat test is a corollary of that theorem that can determine that a number is composite:
Let $p \in \mathbb{N}$, if there exists $a \in \mathbb{N}$ s.t $a^{N-1} \not\equiv 1 \pmod{p}$ then p is composite.

5.2 Miller - Rabin Primality Test

Miller-Rabin primality test is a probabilistic algorithm to determine whether a given number is likely to be prime.
Definition: A number N is called **pseudo prime** under base a if $\gcd(a, N) = 1$ and $a^{N-1} \equiv \pmod{N}$.
Remark: If N is prime then N is pseudo prime under every base a that holds $\gcd(a, N) = 1$.
Definition: Suppose a number N is composite to different primes $N = p_1 \cdot p_2 \cdot ... \cdot p_k$ where $k \geq 2$. N is called **Carmichael number** if for all $1 \leq i \leq k$, $p_i - 1 \Big| N - 1$ and $p_i \neq 2$.
Example for Carmichael number: $561 = 3 \cdot 11 \cdot 17$.
Definition: If N is Carmichael number, then N is pseudo prime for all base a s.t $\gcd(a, N) = 1$.

Suppose $2 \not| \; r$, $p - 1 = 2^t \cdot r$ where p is odd and let an integer a s.t $p \not| \; a$. Let's look about the following finite sequence modulo p:
$a_0 = a^r, a^{2r}, a^{4r}, ..., a^{2^t r} = a_t = 1$, $(a_i = a^{2^i r})$.
If a_i is the first element in the sequence that equals 1, then $a_{i-1}^2 = 1$ and $a_{i-1} \neq 1$ so $a_{i-1} = -1$.

Definition: A number N is called **absolutely pseudo-prime** under a base a where $N - 1 = 2^t \cdot r$ (and r is odd) if $a^r \equiv 1 \pmod{N}$ or one of the elements in the sequence $a^r, a^{2r}, ..., a^{2^t r}$ is equal -1.
Theorem: If a number N is composite, then N is absolutely pseudo-prime in relate to at most a quarter of $a \in \mathbb{Z}_N^{\mathrm{x}}$.
corollary: If N is absolutely pseudo-prime relative to m random bases, then the probability that N is composite is 4^{-m}.

The algorithm:
Let N be an odd number.
(1) Write $N - 1 = 2^t r$ where r is odd.
(2) Randomize base a s.t $2 \leq a \leq N - 1$
(3) If $a^r \not\equiv 1 \pmod{N}$ **and** $\forall 0 \leq i \leq t-1$ holds $a^{2^i \cdot r} \not\equiv -1 \pmod{N}$, it results that N is composite.
(4) Else, randomize another base and go to step (3).

5.3 Elliptic Curves Modulo N

Here N is not necessarily prime so there is not ”truly” an elliptic curve modulo N but it is possible to ”add” according to projective coordinate formulas. If a prime p holds $p \not| \; N$, E is an elliptic curve modulo N and $Q_1, Q_2 \in E(\mathbb{Z}_N)$. Then the reduction of Q_1, Q_2 modulo p is $(Q_1)_p$ and $(Q_2)_p$ and $(Q_1 + Q_2)_p = (Q_1)_p + (Q_2)_p$.

5.3.1 Pocklington Elliptic Test

Proposition: Suppose that $N \in \mathbb{N}$, E is an elliptic curve modulo N, $R \in E(\mathbb{Z}_N)$ and $m \in \mathbb{Z}$ s.t:

(a) m has a prime divisor q s.t $(\sqrt[4]{N} + 1)^2 < q$.

(b) $m \cdot R = 0$.

(c) $(\frac{m}{q}) \cdot R \neq 0$ (i.e the "z-coordinate" is disjoint to N).

Then N is prime.

5.3.2 Goldwasser - Kilian Algorithm

Given a number N that passed many Miller - Rabin tests.

(a) Choose an elliptic curve modulo N.

(b) Compute $m = |E(\mathbb{Z}_N)|$ (Schoof).

(c) Examine that m has a divisor $(\sqrt[4]{N} + 1)^2 < q < m$ that is prime is high probability (Miller - Rabin). If it doesn't, choose another elliptic curve.

(d) Find $R \in E(\mathbb{Z}_N)$.

(e) Examine that $m \cdot R = 0$ (it is true because m is the order of the group) and $(\frac{m}{q}) \cdot R \neq 0$. If it doesn't, choose another R.

According to Elliptic Pocklington, N is prime if q is prime. The process goes back to prove primality of q. Eventually, we may get a "certificate of primality": N, E, m, R, q (and so on...).

References

Arithmetic Methods in Cryptography (201.1.3121) by Prof. Amnon Besser, Ben-Gurion University.
Algebraic Aspects of Cryptography, Neal Koblitz (1998).