ELLIPTIC CURVES

CONTENTS

1. AFFINE CURVES

Let $\mathbf{K}$ be a field. The affine plane $\mathbf{A}^2(\mathbf{K})$ is the set $\mathbf{K}^2$ of pairs (u, v) for u, v in $\mathbf{K}$. Such a pair (u, v) is called an affine point.

Let $E(x, y) \in \mathbf{K}[x, y]$ be a non-constant polynomial in two indeterminates. The set

$$C = \{(u, v) \in \mathbf{K}^2 \mid E(u, v) = 0\}.$$

of affine points (u, v) in $\mathbf{A}^2(\mathbf{K})$ such that $E(u, v) = 0$ is called the plane affine curve with equation E.

If $\mathbf{L} \supset \mathbf{K}$ is an extension field of $\mathbf{K}$ we write

$$C(\mathbf{L}) = \{(u, v) \in \mathbf{L}^2 \mid E(u, v) = 0\}$$

for the set of $\mathbf{L}$-points on the curve C.

For example if $\mathbf{K} = \mathbf{R}$ and $E(x, y) = x + y + 1$ the set $C(\mathbf{K})$ is a line.

If $\mathbf{K} = \mathbf{R}$ and $E(x, y) = x^2 + y^2 - 1$ the set $C(\mathbf{K})$ is a circle.

If $\mathbf{K} = \mathbf{R}$ and $E(x, y) = x^2 + y^2 + 1$ the set $C(\mathbf{R})$ is empty but $C(\mathbf{C})$ is not.

2. SMOOTH POINT ON A CURVE

Let C be a plane affine curve with equation $E(x, y)$. Let $P = (u, v)$ be a point on C. The Taylor expansion of E at P starts like

$$E(x, y) = E(u, v) + \frac{\partial E}{\partial x}(u, v) \times (x - u) + \frac{\partial E}{\partial y}(u, v) \times (y - v) + \text{higher order terms.}$$

Since $E(u,v)=0$ we deduce that if the partial derivatives $\frac{\partial E}{\partial x}(u,v)$ and $\frac{\partial E}{\partial y}(u,v)$ are not both zero the first significant term in the Taylor expansion is the equation of a line called the tangent to C at P. In this situation P is said to be smooth.

For example if $E(x,y)=x^2+y^2-1$ and $P=(1,0)$ the equation of the tangent at P is $x-1=0$.

If $E(x,y)=y^2-x^3$ then the point $P=(0,0)$ is not smooth. One says that P is singular, or that C is singular at P.

We say that a plane curve C is smooth if and only if C is smooth at every point in $C(\bar{\mathbf{K}})$ where $\bar{\mathbf{K}}$ is an algebraic closure of $\mathbf{K}$.

3. The projective plane

Let $\mathbf{K}$ be a field. Let $\mathcal{T}$ be the set of triples (U,V,W) in $\mathbf{K}^3$ such that $(U,V,W)\neq(0,0,0)$. We define an equivalence relation $\mathcal{R}$ on $\mathcal{T}$. We write $(U,V,W)\mathcal{R}(U',V',W')$ if and only if there exists a non-zero λ in $\mathbf{K}$ such that $U'=\lambda U$, $V'=\lambda V$, $W'=\lambda W$. The set of equivalence classes for $\mathcal{R}$ is called the projective plane over $\mathbf{K}$ and denoted $\mathbb{P}^2(\mathbf{K})$. A class in $\mathbb{P}^2(\mathbf{K})$ is represented by any triple in it.

We note that if $W\neq 0$ then $(U,V,W)\mathcal{R}(u,v,1)$ with $u=U/W$ and $v=V/W$. So $\mathbb{P}^2(\mathbf{K})$ contains $\mathbf{A}^2(\mathbf{K})$. The points $(U,V,0)$ in $\mathbb{P}^2(\mathbf{K})$ are called the points at infinity. They correspond to asymptotic directions in the affine plane. Indeed the limit of $(tU,tV,1)$ when t tends to infinity is $(U,V,0)$ because $(tU,tV,1)\mathcal{R}(U,V,1/t)$.

4. Projective curves

Let $d\geqslant 1$ be an integer. Let $E(X,Y,Z)\in\mathbf{K}[X,Y,Z]$ be a non-zero homogeneous polynomial of degree d. All the non-zero monomials in E have total degree d.

If $(U,V,W)\mathcal{R}(U',V',W')$ then there exists a non-zero λ in $\mathbf{K}$ such that $U'=\lambda U$, $V'=\lambda V$, $W'=\lambda W$. So $E(U',V',W')=\lambda^d E(U,V,W)$ so $E(U,V,W)=0$ if and only if $E(U',V',W')=0$. We thus can define the set C of points $P=(U,V,W)$ in $\mathbb{P}^2(\mathbf{K})$ such that E vanishes at P. This set is called the projective plane curve with equation E.

For example if $d=1$ and $E=X+Y-Z$ then C is the set of points (U,V,W) in $\mathbb{P}^2(\mathbf{K})$ such that $U+V-W=0$. This is the projective line with equation $X+Y-Z$. In case W is not zero we have $(U,V,W)\mathcal{R}(u,v,1)$ with $u=U/W$ and $v=V/W$. And $u+v-1=0$. So the curve $C(\mathbf{K})$ contains the affine curve C_{aff} with equations $x+y-1$. If $(U,V,0)$ is on C then $V=-U$ and $(U,V,0)\mathcal{R}(1,-1,0)$. We say that C has a unique point at infinity, namely $(1,-1,0)$.

Now if $d=2$ and $E=X^2-Y^2-Z^2$ then C is an hyperbola. Its affine part is the curve C_{aff} with equations x^2-y^2-1. There are two points at infinity, namely $(1,1,0)$ and $(1,-1,0)$.

An important theorem attributed to Bézout states that if $\mathbf{K}$ is algebraically closed and C_1 and C_2 are plane projective curves with respective degrees d_1 and d_2 such that the intersection $C_1\cap C_2$ is finite then this intersection consists of d_1d_2 points provided one counts multiplicities.

5. Elliptic curves

Let $\mathbf{K}$ be a field with characteristic p different from 2 and 3. A Weierstrass curve is by definition a smooth plane projective curve with equation $Y^2Z-X^3-aXZ^2-bZ^3$ where a and

b are in $\mathbf{K}$. The smoothness condition is easily seen to be equivalent to $27b^2 + 4a^3 \neq 0$. The quantity $-16(27b^2 + 4a^3)$ is called the discriminant of the Weierstrass curve. Weierstrass curves are special cases of elliptic curves.

If C is a Weierstrass curve there is an involution

$$w : C \to C$$

mapping (U, V, W) onto $(U, -V, W)$.

The affine part of C is the affine curve with equation $y^2 - x^3 - ax - b$. There is a unique point at infinity, namely $\mathcal{O} = (0, 1, 0)$. We call it the origin of C.

One can define a commutative group law $\oplus$ on $C(\mathbf{K})$ such that $\mathcal{O}$ is the neutral element, the opposite $\ominus P$ of $P = (U, V, W)$ is $w(P) = (U, -V, W)$, and three points P, Q, R on C are colinear if and only if $P \oplus Q \oplus R = \mathcal{O}$.

Assume $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are two affine points on C. Assume $x_P \neq x_Q$. We want to compute $P \oplus Q$. The line (PQ) has equation

$$(y - y_P) = \lambda(x - x_P)$$

where

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}.$$

We substitute y by $y_P + \lambda(x - x_P)$ in the affine equation $-y^2 + x^3 + ax + b$ and find the degree 3 equation in x

$$x^3 - \lambda^2 x^2 + \text{ terms of smaller degree.}$$

This equation has three solutions : x_P, x_Q and x_R where R is the third intersection point in $C \cap (PQ)$. The sum of the roots of a degree d unitary polynomial is the opposite of the coefficient of x^{d-1}. So

$$x_P + x_Q + x_R = \lambda^2.$$

We deduce that

$$x_R = \lambda^2 - x_P - x_Q$$

and $y_R = y_P + \lambda(x_R - x_P)$. And $P \oplus Q = \ominus R = (x_R, -y_R)$.

Assume now that $x_P = x_Q$. If $y_P = -y_Q$ then $Q = \ominus P$ and $P \oplus Q = \mathcal{O}$. If $y_P = y_Q$ then $P = Q$. We look for some point R such that $P \oplus P \oplus R = \mathcal{O}$. There is a line that intersects C at P with multiplicity two and at R with multiplicity one. This line is the tangent to C at P. Its equation is

$$\frac{\partial E}{\partial x}(x_P, y_P) \times (x - x_P) + \frac{\partial E}{\partial y}(x_P, y_P) \times (y - y_P)$$

where

$$E(x, y) = x^3 + ax + b - y^2$$

is the equation of the affine part of C.

We find

$$\frac{\partial E}{\partial x}(x_P, y_P) = 3x_P^2 + a \text{ and } \frac{\partial E}{\partial y}(x_P, y_P) = -2y_P.$$

The slope of the tangent at P is thus

$$\lambda = \frac{3x_P^2 + a}{2y_P}.$$

We substitute y by $y_P + \lambda(x - x_P)$ in the affine equation $-y^2 + x^3 + ax + b$ and find the degree 3 equation in x

$$x^3 - \lambda^2 x^2 + \text{ terms of smaller degree.}$$

This equation has three solutions : x_P, x_P and x_R. The sum of the roots of a degree d unitary polynomial is the opposite of the coefficient of x^{d-1}. So

$$2x_P + x_R = \lambda^2.$$

We deduce that

$$x_R = \lambda^2 - 2x_P$$

and $y_R = y_P + \lambda(x_R - x_P)$. And $P \oplus P = \ominus R = (x_R, -y_R)$.

6. Elliptic curves over finite fields

Let $\mathbf{K}$ be a finite field with cardinality q. Let a and b in $\mathbf{K}$ such that $27b^2 + 4a^3$ is not 0. Let C be the Weierstrass curve with equation $Y^2Z - X^3 - aXZ^2 - bZ^3$. The set $C(\mathbf{K})$ is a finite commutative group. According to a famous theorem due to Hasse, the order of this group belongs to the interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$. There exists a deterministic polynomial time algorithm that on input a and b returns the order of this group. This algorithm is due to René Schoof.

Exercise 1. *Let* $\mathbf{K}$ *be the field* $\mathbf{Z}/5\mathbf{Z}$*. Let* C *be the affine curve with equation*

$$y^2 = x^3 - x + 2$$

over $\mathbf{K}$.

1. Prove that C is smooth.
2. Compute all the points on C with coordinates in $\mathbf{K}$.
3. Let E be the projective (elliptic) curve with homogeneous equation
$$Y^2Z = X^3 - XZ^2 + 2Z^3.$$
Let $P \in E(\mathbf{K})$ be the point with coordinates $(3 : 1 : 1)$. Let $\mathcal{O} = (0 : 1 : 0)$. Prove that
$$[3]P = P \oplus P \oplus P = O.$$
4. Compute $[10000000001]P$.

Exercise 2. *Let* $\mathbf{K}$ *be the field* $\mathbf{Z}/5\mathbf{Z}$*. Let* C *be the affine curve with equation*

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

over $\mathbf{K}$.

1. Prove that C is smooth.
2. Compute all the points on C with coordinates in $\mathbf{K}$.

3. Let $C \cup \{\mathcal{O}\}$ be the elliptic curve obtained by adding the point $\mathcal{O} = (0 : 1 : 0)$ to the affine curve C. Recall the definition of the group law on $C(\mathbf{K}) \cup \{O\}$. What is the order of this group ?
4. Let Q be the point with coordinates $x_Q = 1$ et $y_Q = 2$. Compute $[321234567898765432123]Q$.

Exercise 3. *Let C be the affine curve with equation*

$$y^2 = x^3 + 2x + 1$$

over the field $\mathbb{F}_7$

1. Is C a smooth curve ?
2. Give the list of all points in $C(\mathbb{F}_7)$.
3. Let E be the elliptic curve obtained by adding to C the point $\mathcal{O} = (0, 1, 0)$. Let P be the point with affine coordinates $(0, 6)$. Check that $P \in E(\mathbb{F}_7)$. Compute $[2]P$.
4. Let Q be the point with affine coordinates $(1, 5)$. Check that $Q \in E(\mathbb{F}_7)$. Compute $P \oplus Q$.
5. Which is the structure of the group $E(\mathbb{F}_7)$?

Exercise 4. *Let $f(x)$ be the polynomial $x^2 + x + 1$ in $\mathbb{F}_5[x]$.*

1. Prove that $f(x)$ is irreducible.
2. Let $\mathbf{K} = \mathbb{F}_5[x]/f(x)$. Let $\alpha = x \bmod f(x) \in \mathbf{K}$. Prove that $\mathbf{K}$ is a field.
3. What is the cardinality of $\mathbf{K}$?
4. Let D be the affine curve with equation
$$y^2 = x^3 + x + 1$$
over $\mathbf{K}$. Prove that D is smooth.
5. We call F be the elliptic curve obtained by adding to D the point $\mathcal{O} = (0, 1, 0)$. Check that $P = (4, 3)$ is in $D(\mathbf{K})$.
6. Compute $[2]P$.
7. Check that $Q = (3\alpha + 1, 4\alpha + 2)$ is in $D(\mathbf{K})$.

7. The projective plane over the ring $\mathbf{Z}/n\mathbf{Z}$

Let $n \geqslant 2$ be an integer. Let $\mathcal{T}$ be the set of triples (U, V, W) in $(\mathbf{Z}/n\mathbf{Z})^3$ such that the ideal (U, V, W) is $\mathbf{Z}/n\mathbf{Z}$. Equivalently the greatest common divisor of n, U, V, and W is 1. We write $(U, V, W)\mathcal{R}(U', V', W')$ if and only if there exists a unit λ in $\mathbf{Z}/n\mathbf{Z}$ such that $U' = \lambda U$, $V' = \lambda V$, $W' = \lambda W$. The set of equivalence classes for $\mathcal{R}$ is called the projective plane over $\mathbf{Z}/n\mathbf{Z}$ and denoted $\mathbb{P}^2(\mathbf{Z}/n\mathbf{Z})$. A class in $\mathbb{P}^2(\mathbf{Z}/n\mathbf{Z})$ is represented by any triple in it.

Let $d \geqslant 1$ be an integer. Let $E(X, Y, Z) \in (\mathbf{Z}/n\mathbf{Z})[X, Y, Z]$ be an homogeneous polynomials of degree d. All the non-zero monomials in E have total degree d. We assume that the coefficients in E have no common factor.

If $(U, V, W)\mathcal{R}(U', V', W')$ then there exists a unit λ in $\mathbf{Z}/n\mathbf{Z}$ such that $U' = \lambda U$, $V' = \lambda V$, $W' = \lambda W$. So $E(U', V', W') = \lambda^d E(U, V, W)$. So $E(U, V, W) = 0$ if and only if $E(U', V', W') = 0$. We thus can define the set C of points $P = (U, V, W)$ in $\mathbb{P}^2(\mathbf{Z}/n\mathbf{Z})$ such that E vanishes at P. This set is called the projective plane curve with equation E.

Assume n is prime to 6. Assume $d = 3$ and $E(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$ where a and b are in $\mathbf{Z}/n\mathbf{Z}$ and $27b^2 + 4a^3$ is a unit. We denote $C(\mathbf{Z}/n\mathbf{Z})$ the set of points (U, V, W) in $\mathbb{P}^2(\mathbf{Z}/n\mathbf{Z})$ such that $E(U, V, W) = 0$. This is the elliptic curve over $\mathbf{Z}/n\mathbf{Z}$ with equation E.

It is possible to define a commutative group law on this set. This is theoretically a bite delicate but in practice we most of the time will simply use the same formulae as in the case of elliptic curves over fields. This may lead us to divide by an element in $\mathbf{Z}/n\mathbf{Z}$ that is neither 0 nor invertible. In such a situation we cannot use the usual addition formulae but we don't really mind because we have found a non-trivial factor of n, which is a nice counterpart.

8. Elliptic curves and Chinese remainder theorem

Let $n \geqslant 2$ be an integer. Assume n is prime to 6. Let a and b in $\mathbf{Z}/n\mathbf{Z}$ such that $27b^2 + 4a^3$ is a unit. Let $C(\mathbf{Z}/n\mathbf{Z})$ be the elliptic curve with equation $E(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$.

Let $m \geqslant 2$ be a divisor of n. By reducing the coefficients in $E(X, Y, Z)$ modulo m we define an elliptic curve over $\mathbf{Z}/m\mathbf{Z}$ which we denote $C(\mathbf{Z}/m\mathbf{Z})$.

The reduction map modulo m is compatible with addition on either sides because the sum $P \oplus Q$ is defined by polynomial expressions in the coordinates of P and Q. We denote

$$\rho_m : C(\mathbf{Z}/n\mathbf{Z}) \to C(\mathbf{Z}/m\mathbf{Z})$$

this group homomorphism.

In case $n = n_1n_2$ with $\gcd(n_1, n_2) = 1$ the map

$$\begin{aligned} \rho_{n_1} \times \rho_{n_2} : \qquad & C(\mathbf{Z}/n\mathbf{Z}) \longrightarrow C(\mathbf{Z}/n_1\mathbf{Z}) \times C(\mathbf{Z}/n_2\mathbf{Z}) \\ & P \longmapsto (P \bmod n_1, P \bmod n_2). \end{aligned}$$

is a bijection according to the Chinese remainder theorem.

9. Introduction to the elliptic curve factoring method

In view of the Chinese isomorphism above one is lead to adapt Pollard's $p - 1$ method to the context of elliptic curves. This leads to Lenstra's elliptic curve factoring method. The idea is to pick a random point P on a random elliptic curve C over $\mathbf{Z}/n\mathbf{Z}$ then define a sequence of points by setting $P_1 = P$, $P_2 = [2]P_1$, $P_3 = [3]P_2$,..., $P_{k+1} = [k + 1]P_k$, etc. At some point we hope that some P_k will be equal to the origin $(0, 1, 0)$ modulo some prime divisor p of n. As in the Pollard's $p-1$ algorithm this should result in a non-trivial gcd between n and the third projective coordinate of P_k. The condition for this to happen is that the cardinality of $C(\mathbf{Z}/p\mathbf{Z})$ be a divisor of $k!$ In other words the method succeeds when $\#C(\mathbf{Z}/p\mathbf{Z})$ is smooth. So we don't need $p-1$ to be smooth. We rather need some random integer in the Hasse interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ to be smooth. This makes this algorithm a good general purpose factoring algorithm while the $p - 1$ method only works when n has a prime divisor p such that $p - 1$ is smooth.

Assume for example that we want to factor the integer $n = 4223$. Let P be the point

$$P = (0, 1, 1) \in \mathbb{P}^2(\mathbf{Z}/n\mathbf{Z}).$$

Let C be the plane projective curve with equation

$$E(X,Y,Z) = Y^2Z - X^3 - XZ^2 - Z^3.$$

We check that P is a point in $C(\mathbf{Z}/n\mathbf{Z})$.

We try to define a sequence $(P_k)_{k\geqslant 1}$ by setting $P_1 = P$ and $P_{k+1} = [k+1]P_k$ for $k \geqslant 1$.

We find $P_2 = (1056, 3694, 1)$, $P_3 = (4182, 2994, 1)$, $P_4 = (3567, 2664, 1)$, ...

```
? n=4223;
? P=[0,1]*Mod(1,n);
? E=ellinit([1,1]*Mod(1,n));
? P1=P
%4 = [Mod(0, 4223), Mod(1, 4223)]
? P2=ellmul(E,P1,2)
%5 = [Mod(1056, 4223), Mod(3694, 4223)]
? P3=ellmul(E,P2,3)
%6 = [Mod(4182, 4223), Mod(2994, 4223)]
? P4=ellmul(E,P3,4)
%7 = [Mod(3567, 4223), Mod(2664, 4223)]
? P5=ellmul(E,P4,5)
  ***   at top-level: P5=ellmul(E,P4,5)
  ***                     ^--------------
  *** ellmul: impossible inverse in Fp_inv: Mod(41, 4223).
  ***   Break loop: type 'break' to go back to GP prompt
```

We fail to compute $P_5 = [5]P_4$ because at some point in the calculation we find a non-zero scalar $41 \bmod n$ in $\mathbf{Z}/n\mathbf{Z}$ which is not invertible. This exhibits a factor $p = 41$ of n. The cofactor is $q = n/p = 103$. We check that p and q are prime.

To understand what is happening we redo the computation modulo p then modulo q.

```
? p=41;
? P=[0,1]*Mod(1,p);
? E=ellinit([1,1]*Mod(1,p));
? P1=P
%11 = [Mod(0, 41), Mod(1, 41)]
? P2=ellmul(E,P1,2)
%12 = [Mod(31, 41), Mod(4, 41)]
? P3=ellmul(E,P2,3)
%13 = [Mod(0, 41), Mod(1, 41)]
? P4=ellmul(E,P3,4)
%14 = [Mod(0, 41), Mod(40, 41)]
? P5=ellmul(E,P4,5)
%15 = [0]
?
?
? q=103;
```

```
? P=[0,1]*Mod(1,q);
? E=ellinit([1,1]*Mod(1,q));
? P1=P
%19 = [Mod(0, 103), Mod(1, 103)]
? P2=ellmul(E,P1,2)
%20 = [Mod(26, 103), Mod(89, 103)]
? P3=ellmul(E,P2,3)
%21 = [Mod(62, 103), Mod(7, 103)]
? P4=ellmul(E,P3,4)
%22 = [Mod(65, 103), Mod(89, 103)]
? P5=ellmul(E,P4,5)
%23 = [Mod(29, 103), Mod(27, 103)]
```

We see that the point $(0,1) \in \mathbf{Z}/p\mathbf{Z}$ has order dividing $5!$ in the group $C(\mathbf{Z}/p\mathbf{Z})$. But the point $(0,1) \in \mathbf{Z}/q\mathbf{Z}$ has order not dividing $5!$ in the group $C(\mathbf{Z}/q\mathbf{Z})$.

Indeed the group $C(\mathbf{Z}/p\mathbf{Z})$ is isomorphic to $\mathbf{Z}/35\mathbf{Z}$ while the group $C(\mathbf{Z}/q\mathbf{Z})$ is isomorphic to $\mathbf{Z}/87\mathbf{Z}$.

```
? ellgroup(ellinit([1,1]*Mod(1,p)))
%24 = [35]
?
? ellgroup(ellinit([1,1]*Mod(1,q)))
%25 = [87]
```