

TD5 : ELLIPTIC CURVES

---

**Exercise 1 :**

Let  $C$  be the affine curve with equation

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

over the field  $\mathbb{F}_7$ .

Is  $C$  a smooth curve?

Give the list of all points in  $C(\mathbb{F}_7)$ .

We call  $E$  be the elliptic curve obtained by adding to  $C$  the point at infinity.

Let  $P$  be the point with affine coordinates  $(0, 6)$ . Check that  $P \in E(\mathbb{F}_7)$ . Compute  $2P$ .

Let  $Q$  be the point with affine coordinates  $(1, 5)$ . Check that  $Q \in E(\mathbb{F}_7)$ . Compute  $P + Q$ .

Which is the structure of the group  $E(\mathbb{F}_7)$ ?

---

**Exercise 2 :**

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

Prove that  $f(x)$  is irreducible.

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.

What is the cardinality of  $\mathbf{K}$ ?

Let  $D$  be the affine curve with equation

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

over  $\mathbf{K}$ .

Prove that  $D$  is smooth.

We call  $F$  be the elliptic curve obtained by adding to  $D$  the point at infinity.

Check that  $P = (4, 3)$  is in  $D(\mathbf{K})$ .

Compute  $2P$ .

Check that  $Q = (3\alpha + 1, 4\alpha + 2)$  is in  $D(\mathbf{K})$ .

Compute  $P + Q$ .

---

**Exercise 3 :**

We want to factor the integer  $n = 4223$ . Let  $R = \mathbb{Z}/n\mathbb{Z}$ . Let  $P$  be the affine point  $P = (0, 1) \in R^2$ . Let

$$C(R) = \{(x, y) \in R^2 \mid y^2 = x^3 + x + 1\}$$

be the affine curve over  $R$  with equation  $Y^2 = X^3 + X + 1$ .

Check that  $P$  is a point in  $C(R)$ .

We try to define a sequence  $(P_k)_{k \geq 1}$  by setting  $P_1 = P$  and  $P_{k+1} = [k+1]P_k$  for  $k \geq 0$ .

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

```
? 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  $R$  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  $(0, 1) \in \mathbb{Z}/p\mathbb{Z}$  has order dividing  $5!$  in the group  $E_p = C(\mathbb{Z}/p\mathbb{Z}) \cup O_p$ . But the point  $(0, 1) \in \mathbb{Z}/q\mathbb{Z}$  has order not dividing  $5!$  in the group  $E_q = C(\mathbb{Z}/q\mathbb{Z}) \cup O_q$ .

Indeed the group  $E_p = C(\mathbb{Z}/p\mathbb{Z}) \cup O_p$  is isomorphic to  $\mathbb{Z}/35\mathbb{Z}$  while the group  $E_q = C(\mathbb{Z}/q\mathbb{Z}) \cup O_q$  is isomorphic to  $\mathbb{Z}/87\mathbb{Z}$ .

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

Design and implement an integer factoring algorithm based on these observations and following the principles of Pollard's  $p - 1$  method.

Propose a heuristic estimate of the running time of this algorithm.

---