

## Number Theory: Elliptic Curves, Problem Sheet 4

1) One can explicitly work out the group  $E(k)$  if  $E$  is a given elliptic curve over a given finite field  $k$ —one can just count all the solutions and then add them to each other until one finds out what's going on. So, for the following equations, find all the solutions, and work out explicitly what the group is (in all cases, let the origin for the group law be  $[0 : 1 : 0]$  on the corresponding homogeneous cubic).

(i)  $Y^2 = X^3 + X$  over  $k = \mathbb{Z}/5\mathbb{Z}$ .

(ii)  $Y^2 = X^3 + 2X$  over  $k = \mathbb{Z}/5\mathbb{Z}$ .

(iii)  $Y^2 = X^3 + X$  over  $k = \mathbb{Z}/3\mathbb{Z}$ .

(iv)  $Y^2 + Y = X^3 + X^2$  over  $k = \mathbb{Z}/2\mathbb{Z}$  (note the non-standard form because we are in characteristic two so we can't complete the square; it's still an elliptic curve though (one can verify this by checking that there are no singular points). Note however that in this setting the inverse of  $(x, y)$  isn't  $(x, -y)$ ; this formula only works for cubics of the form  $y^2 = f(x)$ ).

and so on and so on. Which groups show up? Why can't an arbitrary abelian group show up? [Hint: what can you say about points of order 2?].

2) Consider the curve given by the equation  $Y^2 = X^3 + 81X$ . For which primes  $p$  does the resulting equation not give an elliptic curve mod  $p$ ? We say the equation has “bad reduction” for these primes. But can you find a change of variables defined over  $\mathbb{Q}$  such that the resulting equation has bad reduction for a strictly smaller set of primes? (hint:  $81 = 3^4$ ).

3) By using Hensel's lemma one can show that the reduction map on an elliptic curve will hit every non-singular point. We'll prove something a little more general.

(i) Say  $f \in \mathbb{Z}_p[x_1, x_2, \dots, x_n]$  and  $\bar{f} \in (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$  is its reduction mod  $p$ . Say  $\bar{f} \neq 0$  and  $\bar{P} = (a_1, a_2, \dots, a_n) \in (\mathbb{Z}/p\mathbb{Z})^n$  is a non-singular point on  $\bar{f} = 0$ . Prove that there exists  $P \in (\mathbb{Z}_p)^n \subset (\mathbb{Q}_p)^n$  such that  $P$  is on  $f = 0$  and the reduction of  $P$  is  $\bar{P}$ . Hint: say  $\partial \bar{f} / \partial x_i$  is non-zero at  $\bar{P}$ . Lift all the  $a_j$  arbitrarily for  $j \neq i$  and then lift  $a_i$  to make it all work.

(ii) Show that the non-singularity assumption is essential in the previous part by considering the equation  $f = y^2 - x^3 - p \in \mathbb{Z}_p[x, y]$ .

(iii) Prove the analogue of (i) in the homogeneous case. That is, if  $F \in \mathbb{Z}_p[X_1, X_2, \dots, X_{n+1}]$  is a homogeneous equation whose reduction  $\bar{F}$  is non-zero, and if  $\bar{P}$  is a point in  $\mathbb{P}^n(\mathbb{Z}/p\mathbb{Z})$  which is a non-singular point of  $\bar{F} = 0$  then prove that  $\bar{P}$  lifts to  $P \in \mathbb{P}^n(\mathbb{Q}_p)$  on  $F = 0$ .

4) Invent some elliptic curves over  $\mathbb{Q}$  and compute their torsion subgroups. Here's some to start you off:

(i)  $Y^2 = X^3 + 4X$

(ii)  $Y^2 = X^3 - 9X$

(iii)  $Y^2 = X^3 - 43X + 166$

(iv)  $Y^2 = X^3 - 219X + 1654$

(the numbers can get a bit big here so you'll probably want to use a calculator or a computer; the point of the last two questions is that there are points of quite large order, relatively speaking).

(v) and so on and so on.

5) (from Cassels' book, and he attributes it to Nagell) Let  $A \in \mathbb{Q}$  be non-zero. We will compute the torsion subgroup of the curve  $Y^2 = X(X^2 + A)$ .

Firstly, show that by a suitable linear change of coordinates, we may assume that  $A$  is an integer, and such that there is no prime  $p$  with  $p^4 | A$ .

I claim that now the torsion is as follows:

(I)  $(0, 0)$  always has order 2.

(II) If  $A = 4$  then  $(2, \pm 4)$  have order 4.

(III) If  $A = -C^2$  for some integer  $C$ , then  $(\pm C, 0)$  have order 2.

And that's it. Fill in the details of the following sketch proof:

(i) Check that if  $(a, b)$  is on the curve and  $b \neq 0$  then  $2(a, b) := (a, b) \oplus (a, b) = (x, y)$ , with  $x = (a^2 - A)^2/4b^2$ .

(ii) Check that the points of order 2 are as in (I) and (III) above.

(iii) Check that  $(0, 0) = 2(a, b)$  for some rational point  $(a, b)$  iff  $A = 4$ , and that  $(\pm C, 0)$  is never of the form  $2(a, b)$  if  $A = -C^2$ .

(iv) It suffices to prove that there are no points of odd order other than the identity. So let  $(a, b)$  be a point of odd order, and we seek a contradiction. Firstly, check  $a$  is a square. (Hint: use (i)).

(v) If  $d = \text{hcf}(a, A)$  and  $a = da_1$ ,  $A = dA_1$ , then  $b = db_1$  where  $b_1^2 = a_1(da_1^2 + A_1)$ .

(vi) There exist integers  $f, g, h$  with  $\text{hcf}(f, g) = 1$  and  $a_1 = \pm f^2$ ,  $da_1^2 + A_1 = \pm g^2$ ,  $b_1 = fg$ ,  $d = h^2$  (with all choices of sign the same).

(vii)  $a^2 - A = 2h^4f^4 \mp h^2g^2$ , and  $b = h^2fg$ .

(viii)  $a^2 - A \equiv 0 \pmod{2b}$ . (Hint: use (i)).

(ix)  $f|g^2$ .

(x) Hence  $f = 1$  or  $f = -1$ , and  $g \equiv 0 \pmod{2}$ ,  $h \equiv 0 \pmod{2}$ .

(xi) Hence  $2^4|A$ , contradiction.

6(a) Show that any elliptic curve with a point of order 4 over  $\mathbb{Q}$  can be put into the form  $Y^2 + XY + vY = X^3 + vX^2$ . Hint: don't get hung up with general equations of the form  $Y^2 = X^3 + AX + B$ ; start with an equation of this form, but then write down a linear transformation taking the point of order 4 to the origin, and then draw lines to work out the relationships amongst the coefficients.

(b) Show that any elliptic curve with a point of order 5 over  $\mathbb{Q}$  can be put into the form  $Y^2 + (1+v)XY + vY = X^3 + vX^2$ .

7) Work out  $G/2G$ , where  $G = E(\mathbb{Q})$ , and  $E$  runs through the following curves:

(i)  $Y^2 = X(X+1)(X-14)$

(ii)  $Y^2 = X(X^2 + 3X + 5)$

(iii)  $Y^2 = X(X^2 + 2X + 9)$

(iv)  $Y^2 = X(X^2 - 2X + 9)$

(v)  $Y^2 = X(X^2 + 17)$

You shouldn't expect to be able to do this question in all cases, as there is a part of the procedure that we didn't automate. In fact probably you should have got stuck on one of the above questions! Which one?

(vi) etc etc etc.

8) For each of the curves in Q7 for which you managed to compute  $G/2G$ , compute the rank of the curve.