Course 428

Elliptic Curves I

Dr Timothy Murphy

Joly Theatre Friday, 11 January 2002 16:15–17:45

Attempt 5 questions. (If you attempt more, only the best 5 will be counted.) All questions carry the same number of marks.

1. Explain informally how two points on an elliptic curve are added.

   Find the sum $P+Q$ of the points $P=(-1,0),\ Q=(2,3)$ on the curve

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

   over the rationals $\mathbb{Q}$. What are $2P$ and $2Q$?

   Answer:

   (a) *The line PQ meets the curve again in a point R. We have*

$$R = -(P+Q).$$

   Let OR meet the curve again in the point S. Then

$$S = -R = P+Q.$$

   If $P=Q$ then we take the tangent at P in place of the line PQ.

   (b) *The line PQ is given by*

$$\det\begin{pmatrix} x & y & 1 \\ 0 & -1 & 1 \\ 2 & 3 & 1 \end{pmatrix} = 0,$$

   ie

$$-4x + 2y + 2 = 0,$$

ie

$$y = 2x - 1.$$

This meets the curve where

$$(2x-1)^2 = x^3 + 17.$$

We know that two of the roots of this equation are $0, 2$*; hence the third is given by*

$$0 + 2 + x = 4$$

ie

$$x = 2.$$

From the equation of the line,

$$y = 3.$$

In other words, this line touches the curve at Q*. Thus*

$$\begin{aligned} P + Q &= -Q \\ &= (2, -3). \end{aligned}$$

To compute $2P$ *we must find the tangent at* P*. Differentiating the equation of the curve,*

$$2y\frac{dy}{dx} = 3x^2,$$

ie

$$\frac{dy}{dx} = \frac{3x^2}{2y}.$$

2. Define the discriminant Δ of a monic polynomial

$$f(x) = x^n + c_1 x^{n-1} + \cdots + c_n,$$

and show that $f(x)$ has a multiple root if and only if $\Delta = 0$.

Determine the discriminant of the polynomial

$$p(x) = x^3 + ax^2 + c.$$

Show that the curve

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

over the rationals $\mathbb{Q}$ is non-singular.

Answer:

3. Express the 2-adic integer $1/3 \in \mathbb{Z}_2$ in standard form

$$1/3 = a_0 + a_1 2 + a_2 2^2 + \cdots \qquad (a_i \in \{0, 1\}).$$

Does there exist a 2-adic integer x such that $x^2 = -1$?

Answer: *We have*

$$\frac{1}{3} \equiv 1 \bmod 2$$

since $3 \cdot 1 \equiv 1 \bmod 2$.

Now

$$\frac{1}{3} - 1 = \frac{-2}{3} = 2\frac{-1}{3}.$$

But

$$\frac{-1}{3} \equiv 1 \bmod 2.$$

Thus

$$\frac{1}{3} \equiv 1 + 1 \cdot 2 \bmod 2^2.$$

Furthermore,

$$\frac{-1}{3} - 1 = \frac{-4}{3} = 2^2\frac{-1}{3}.$$

Thus

$$\begin{aligned} \frac{-1}{3} &= 1 + 2^2\frac{-1}{3} \\ &= 1 + 2^2 + 2^4\frac{-1}{3} \\ &= 1 + 2^2 + 2^4 + 2^6 + \cdots \end{aligned}$$

and so

$$\begin{aligned} \frac{1}{3} &= 1 + 2 \cdot \frac{-1}{3} \\ \frac{-1}{3} &= 1 + 2 + 2^3 + 2^5 + 2^7 + \cdots \end{aligned}$$

There does not exist a 2-adic integer x such that $x^2 = -1$? For there is no integer n such that

$$n^2 \equiv -1 \bmod 4.$$

[If

$$x = a_0 + a_1 2 + a_2 2^2 + \cdots$$

satisfied $x^2 = -1$ then

$$n = a_0 + a_1 2$$

would satisfy $n^2 \equiv -1 \bmod 2^2$.]

4. Find the order of the point $(0,0)$ on the elliptic curve

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

over the rationals $\mathbb{Q}$.

Answer: *Let $P = (0,0)$. The tangent at the point (x,y) has slope*

$$m = \frac{3x^2 - 1}{2y - 1}.$$

In particular, the tangent at P has slope 1. Hence the tangent is

$$y = x.$$

This meets the curve again where

$$x^2 - x = x^3 - x$$

ie where

$$x = 1,$$

and therefore

$$y = 1.$$

Thus

$$2P = -(1,1) = Q,$$

say. The line OQ (where O is the neutral element $[0,1,0]$) is $x = 1$. This meets the curve again where

$$y^2 - y = 0,$$

ie where

$$y = 0.$$

Thus

$$2P = (1,0) = R,$$

say.

The slope at R is

$$m = \frac{2}{-1} = -2.$$

Thus the tangent is

$$y = -2(x-1),$$

ie

$$y + 2x - 2 = 0.$$

This meets the curve again where

$$4(x-1)^2 - 2(x-1) = x^3 - x,$$

ie

$$x^3 - 4x^2 + 9x - 6.$$

We know that this has roots $1, 1$. *Hence the third root is given by*

$$1 + 1 + x = 4,$$

ie

$$x = 2.$$

Thus the tangent meets the curve again at the point

$$S = (2, -2).$$

The line OS, *ie* $x = 2$, *meets the curve again where*

$$y^2 - y = 6.$$

One solution is $y = -2$; *so the other is given by*

$$-2 + y = 1,$$

ie

$$y = 3.$$

Thus

$$2R = (2, 3) = T,$$

say.

The slope at T *is*

$$m = \frac{11}{5}.$$

Let the tangent at T be

$$y = mx + c.$$

This meets the curve where

$$(mx + c)^2 - (mx + c) = x^3 - x.$$

Thus the tangent meets the curve again where

$$2 + 2 + x = m^2.$$

Evidently x is not integral. Hence T is of infinite order, and so therefore is $P = (0, 0)$, since $T = 4P$.

5. Show that the curve

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

over the finite field $\mathbb{F}_2$ is elliptic, and determine its group.

Hence or otherwise, find all points of finite order on the curve

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

over the rationals $\mathbb{Q}$.

Answer:

(a) *In homogeneous coordinates the curve takes the form*

$$F(X, Y, Z) \equiv Y^2Z + XYZ + X^3 + XZ^2 = 0$$

(since $2 = 0$).
At a singular point,

$$\begin{aligned}
\frac{\partial F}{\partial X} &= YZ + X^2 + Z^2 = 0,\\
\frac{\partial F}{\partial Y} &= XZ = 0,\\
\frac{\partial F}{\partial X} &= Y^2 + XY = 0.
\end{aligned}$$

From the second equation, $X = 0$ or $Z = 0$. If $X = 0$ then $Y = 0$ from the third equation, and $Z = 0$ from the first. If $Z = 0$ then $X = 0$ from the first equation, and $Y = 0$ from the third. Thus in either case $X = Y = Z = 0$. Since this does not define a point in the projective plane, the curve is non-singular, ie elliptic.
If $x = 0$ then $y^2 = 0$ and so $y = 0$. If $x = 1$ then $y^2 + y = 0$ and so $y = 0$ or $y = 1$. We conclude that there are just 4 points on $\mathcal{E}(\mathbb{F}_2)$, namely $(0, 0), (1, 0), (1, 1)$ and $O = [0, 1, 0]$.

It follows that the group is either $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ *or* $\mathbb{Z}/(4)$.
If $P + Q = 0$ *then the line* PQ *goes through* $O = [0, 1, 0]$*, and so is of the form* $x = c$*. Thus*

$$-(0,0) = (0,0),$$
$$-(1,0) = (1,1).$$

Since there is just one point of order 2, the group must be $\mathbb{Z}/(4)$.

(b) *Reduction modulo 2 defines a homomorphism*

$$\mathscr{E}(\mathbb{Q}) \to \mathscr{E}(\mathbb{F}_2),$$

which is injective on the torsion group

$$T \subset \mathscr{E}(\mathbb{Q}).$$

It follows that in this case $T \subset \mathbb{Z}/(4)$*, ie* $T = \{0\}$, $\mathbb{Z}/(2)$ *or* $\mathbb{Z}/(4)$.
Since

$$x = 0 \implies y = 0$$

there is just one point on the line $x = 0$*, and so*

$$-(0,0) = (0,0),$$

ie $P = (0, 0$ *is of order 2. Thus* $T = \mathbb{Z}/(2)$ *or* $\mathbb{Z}/(4)$.
If there are any more points of finite order, they must be two points $\pm Q$ *of order 4, with*

$$2Q = P.$$

Thus the tangent at Q *must pass through* P*, and so is of the form*

$$y = tx$$

for some constant $t \in \mathbb{Q}$*. This line meets the curve where*

$$t^2x^2 + tx^2 = x^3 + x,$$

ie at $x = 0$ *and where*

$$x^2 - t(1 + t)x + 1 = 0.$$

If the line is a tangent this will have a double root, and so

$$t^2(t + 1)^2 = 4,$$

ie

$$t^4 + 2t^3 + t^2 - 4 = 0.$$

A rational solution must in fact be integral (since the equation is monic) and so $t \mid 4$, *ie*

$$t \in \{\pm 1, \pm 2, \pm 4\}.$$

Now we observe that $t = 1$ *is a solution. [We might have seen this earlier.] So the line* $y = x$ *is a tangent. This meets the curve where*

$$x^2 - 2x + 1 = 0,$$

ie at the point $Q = (1, 1)$. *Thus* $2Q = P$, *and* $T = \mathbb{Z}/(4)$, *with*

$$T = \{O, P, \pm Q\}.$$

Finally, $-Q$ *is the other point of the curve on the line* $x = 1$, *with*

$$y^2 + y = 2.$$

Thus $-Q = (1, -2)$, *and*

$$T = \{O, (0,0), (1,1), (1,-2)\}.$$

6. Suppose $P = (x, y)$ is a point of finite order on the elliptic curve

$$y^2 = x^3 + ax^2 + bx + c \qquad (a, b, c \in \mathbb{Z}).$$

Given that $x, y \in \mathbb{Z}$ show that

$$y = 0 \text{ or } y \mid \Delta,$$

where Δ is the discriminant of the polynomial

$$p(x) = x^3 + ax^2 + bx + c.$$

Find all points of finite order on the elliptic curve

$$y^2 = x^3 + 4x$$

over the rationals $\mathbb{Q}$.

Answer:

(a)

(b) *We have*

$$\Delta = -4(-2)^3 = 2^5.$$

By the (strong) Nagel-Lutz Theorem, a point (x, y) *on the curve of finite order has integer coordinates* x, y*, and either* $y = 0$ *or else*

$$y^2 \mid 2^5,$$

ie

$$y = 0, \pm 2, \pm 4.$$

There is no point with $y = 0$*, since 2 is not a cube.*
Suppose $y = \pm 2$*. Then*

$$x^3 - 2 = 4,$$

ie

$$x^3 = 6.$$

This has no rational solution.
Finally, suppose $y = \pm 4$*. Then*

$$x^3 - 2 = 16,$$

ie

$$x^3 = 18,$$

which again has no rational solution.
We conclude that the only point on the curve of finite order is the neutral element $0 = [0, 1, 0]$*, or order 1.*

7. Describe carefully (but without proof) the Structure Theorem for Finite Abelian Groups.

   How many abelian groups of order 24 (up to isomorphism) are there?

   Answer: *Every finitely-generated abelian group* A *is expressible as the direct sum of cyclic subgroups of infinite or prime-power order:*

$$A = \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}/(p_1^{e_1}) \oplus \mathbb{Z}/(p_2^{e_2}) \oplus \cdots \oplus \mathbb{Z}/(p_r^{e_r}).$$

   Moreover, the number of copies of $\mathbb{Z}$*, and the prime-powers* $p_1^{e_1}, \ldots, p_r^{e_r}$ *occuring in this direct sum are uniquely determined (up to order) by* A*.*

   Suppose

$$|A| = 36 = 2^2 \cdot 3^2.$$

Then the 2-component A_2 and the 3-component A_3 of A have orders 4 and 9. Thus
$$A_2 = \mathbb{Z}/(4) \text{ or } \mathbb{Z}/(2) \oplus \mathbb{Z}/(2),$$
and
$$A_2 = \mathbb{Z}/(9) \text{ or } \mathbb{Z}/(3) \oplus \mathbb{Z}/(3).$$
It follows that there are just 4 abelian groups of order 36, namely
$$\mathbb{Z}/(4) \oplus \mathbb{Z}/(9) = \mathbb{Z}/(36),$$
$$\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(9) = \mathbb{Z}/(18) \oplus \mathbb{Z}/(2),$$
$$\mathbb{Z}/(4) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(3) = \mathbb{Z}/(12) \oplus \mathbb{Z}/(3),$$
$$\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(3) = \mathbb{Z}/(6) \oplus \mathbb{Z}/(6).$$