Course 428

Elliptic Curves

Dr Timothy Murphy

Maxwell Theatre   Friday, 21 January 2004   12:00–15:00

Attempt 7 questions. (If you attempt more, only the best 7 will be counted.) All questions carry the same number of marks.

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

   Outline the proof that this operation is associative.

   Answer:

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

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 - x^2 + x.$$

   Determine the orders of P and Q.

   Answer:

   (a) *Let PQ be the line*

$$y = mx + c.$$

   Then

$$m = \frac{1 - 0}{1 - 0} = 1.$$

   This meets the curve where

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

   Thus if $P * Q = R = (x_2, y_2)$ *then*

$$0 + 1 + x_2 = 1 + m^2 = 2,$$

ie
$$x_2 = 1.$$
Thus $R = Q$. *Hence*
$$\begin{aligned} P + Q &= -Q \\ &= (1, -1). \end{aligned}$$

(b) P *is of order 2, since*
$$-(x, y) = (x, -y)$$
and so
$$-(0, 0) = (0, 0).$$
From above,
$$P + Q = -Q \implies 2Q = -P = P.$$
Hence Q *is of order 4.*

3. What is meant by saying that p is a *good prime* for an elliptic curve?

   Show that $3, 5$ and 7 are good primes for the elliptic curve
   $$\mathcal{E} : y^2 = x^3 - 2x,$$
   and determine the corresponding groups over the finite fields $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_7$.

   What can you deduce about the group of points of finite order on $\mathcal{E}(\mathbb{Q})$?

   Answer:

   (a) *Suppose*
   $$\mathcal{E}(\mathbb{Q}) : y^2 + a_1xy + a_3y = x * 3 + a_2x^2 + a_4x + a_6,$$
   where $a_i \in \mathbb{Z}$. *Then* p *is a* good prime *if the curve*
   $$\mathcal{E}(\mathbb{F}_p) : y^2 + a_1xy + a_3y = x * 3 + a_2x^2 + a_4x + a_6$$
   is elliptic, ie non-singular.

(b) *If p is an odd prime then it is good if and only if*

$$p \nmid D,$$

where D is the discriminant of the cubic.
In this case

$$\begin{aligned} D &= -(4b^3 + 27c^2) \\ &= -4 \cdot 2^3. \end{aligned}$$

Hence all odd primes are good.

(c) *Suppose $p = 3$. The quadratic residues* $\bmod 3$ *are* $0, 1$. *Thus we can draw up the table*

x	$x^3 - 2x$	*points*
0	0	$(0, 0)$
1	-1	
-1	1	$(-1, \pm 1)$

Thus $\mathcal{E}(\mathbb{F}_3)$ contains 4 points (including O), one of which, $(0, 0)$, *of order 2. Hence*

$$\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(4).$$

(d) *Suppose $p = 5$. The quadratic residues* $\bmod 3$ *are* $0, \pm 1$. *Thus we can draw up the table*

x	$x^3 - 2x$	*points*
0	0	$(0, 0)$
1	-1	$(1, \pm 2)$
2	-1	$(2, \pm 2)$
-2	1	$(-2, \pm 1)$
-1	1	$(-1, \pm 1)$

Thus $\mathcal{E}(\mathbb{F}_5)$ contains 10 points (including O), one of which, $(0, 0)$, *of order 2. Hence*

$$\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(10) = \mathbb{Z}/(2) \oplus \mathbb{Z}/(5).$$

(e) *Suppose $p = 7$. The quadratic residues* $\bmod 3$ *are* $0, 1, 2, -3$. *Thus we can draw up the table*

x	$x^3 - 2x$	*points*
0	0	$(0, 0)$
1	-1	
2	-3	$(2, \pm 2)$
3	0	$(3, 0)$
-3	0	$(3, 0)$
-2	3	
-1	1	$(-1, \pm 1)$

Thus $\mathcal{E}(\mathbb{F}_7)$ *contains 8 points (including* O*), three of which,* $(0,0), (3,0), (-3,0)$, *are of order 2. Hence*

$$\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(4) \oplus \mathbb{Z}/(2).$$

(f) *Since the torsion group*

$$T \subset \mathcal{E}(\mathbb{Q})$$

is isomorphic to a subgroup of $\mathcal{E}(\mathbb{F}_p)$ *for* $p = 3, 5, 7$ *it follows that*

$$T = \{0\} \text{ or } \mathbb{Z}/(2).$$

Since $(0,0) \in \mathcal{E}(\mathbb{Q})$, *it follows that*

$$T = \mathbb{Z}/(2).$$

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

$$1/3 = a_0 + a_1 2 + a_2 2^2 + \cdots,$$

where each a_i is 0 or 1.

Does there exist a 2-adic integer x such that $x^2 = -3$?

Answer:

(a) *We have*

$$1/3 \equiv 1 \bmod 2$$

since $1 \equiv 3 \bmod 2$. *Thus*

$$1/3 = 1 + O(2).$$

Now

$$1/3 - 1 = -2/3$$

Hence

$$\begin{aligned} 2^{-1}(1/3 - 1) &= -1/3 \\ &\equiv 1 \bmod 3. \end{aligned}$$

Thus

$$1/3 = 1 + 2 + O(2^2).$$

Now

$$-1/3 - 1 = -4/3$$

Hence

$$\begin{aligned} 2^{-2}(-1/3 - 1) &= -1/3 \\ &\equiv 1 \bmod 3. \end{aligned}$$

Thus

$$1/3 = 1 + 2 + 2^3 + O(2^4).$$

But now we have the same remainder $-1/3$*, so we have entered a cyle, and will get the series*

$$1/3 = 1 + 2 + 2^3 + 2^5 + 2^7 + \cdots.$$

To check that this is correct, note that

$$\begin{aligned} 1 + 2 + 2^3 + 2^5 + 2^7 + \cdots &= 1 + 2(1 + 2^2 + 2^4 + \cdots) \\ &= 1 + \frac{2}{1 - 2^2} \\ &= 1 - \frac{2}{3} \\ &= \frac{1}{3}. \end{aligned}$$

(b) *There does not exist a* 2*-adic integer*

$$x = a_0 + a_1 2 + a_2 2^2 + \cdots \quad (a_i \in \{0, 1\}$$

such that

$$x^2 = -3$$

since this would imply that

$$a = a_0 + a_1 2 + a_2 2^2$$

would satisfy

$$a^2 \equiv -3 \equiv 5 \bmod 8.$$

But the only quadratic residues $\bmod 8$ *are* $0, 1, 4$.

5. Prove that a point $P = (x, y)$ of finite order on the elliptic curve

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

necessarily has integral coordinates $x, y \in \mathbb{Z}$.

Answer: *It is sufficient to show that*

$$x, y \in \mathbb{Z}_p$$

for each prime p.

Let us fix the prime p, and write $\|\cdot\|$ for $\|\cdot\|_p$.

Note that

$$\|x\| > 1 \iff \|y\| > 1,$$

since otherwise x^3 or y^2 would dominate; and it this is so then

$$\|y\|^2 = \|x\|^3.$$

Suppose this is so. Let us change coordinates to X, Z where

$$(x, y) = [x, y, 1] = [X, 1, Z],$$

ie

$$X = x/y,\ Z = 1/y$$

or conversely

$$x = X/Z,\ y = 1/Z.$$

Suppose $\|x\|, \|y\| > 1$. Then

$$\|Z\| = 1/\|y\| < 1,$$

and

$$\|X\| = \|x\|/\|y\| = \|x\|^{-1/2} < 1.$$

The equation of the curve in X, Z coordinates is

$$Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

Substituting for Z in the right-hand side we get an expansion for Z as a power-series in X,

$$\begin{aligned} Z &= X^3 + aX^2(X^3 + \cdots) + bX(X^3 + \cdots)^2 + c(X^3 + \cdots)^3 \\ &= X^3 + aX^5 + O(X^7). \end{aligned}$$

In particular,

$$\|Z\| = \|X\|^3.$$

Let

$$\mathcal{E}_{(p^r)} = \{[X, 1, Z] \in \mathcal{E} : \|X\| \le p^{-r}, \|Z\| \le p^{-3r}\}.$$

Lemma 1. *$\mathcal{E}_{(p^r)}$ is a subgroup for each $r \geq 1$.*

Proof. Suppose

$$P_1 = [X_1, 1, Z_1],\ P_2 = [X_2, 1, Z_2] \in \mathcal{E}_{(p^r)}.$$

Let

$$P_3 = [X_3, 1, Z_3] = P_1 + P_2.$$

Suppose P_1P_2 is the line

$$Z = mX + d.$$

Then

$$m = \frac{Z_2 - Z_1}{X_2 - X_1}$$

But

$$\begin{aligned} Z_2 - Z_1 &= (X_2^3 + aX_2^5 + \cdots) - (X_1^3 + aX_1^5 + \cdots) \\ &= (X_2^3 - X_1^3) + a(X_2^5 - X_1^5) + \cdots \end{aligned}$$

Thus

$$m = X_1^2 + X_1X_2 + X_2^2 + O((X_1 + X_2)^4)$$

Hence

$$m \equiv 0 \bmod p^{2r},$$

ie

$$\|m\| \leq p^{-2r}.$$

Moreover, since $d = Z_1 - mX_1$,

$$\|d\| \leq p^{-3r}.$$

Since $-(x, y) = (x, -y)$ it follows that

$$-[X, 1, Z] = -[X/Z, 1/Z, 1] = [X/Z, -1/Z, 1] = [-X, 1, -Z].$$

In particular,

$$-P_3 = [-X_3, 1, -Z_3].$$

Thus $X_1, X_2, -X_3$ are the roots of

$$mX + d = X^3 + aX^2(mX + d) + bX(mX + d)^2 + c(mX + d)^3.$$

Hence

$$X_1 + X_2 - X_3 = -\frac{ad + 2bmd + 3cm^2 d}{1 + am + bm^2 + cm^3}.$$

Hence

$$X_3 \equiv X_1 + X_2 \bmod p^{3r}.$$

□

Lemma 2. *There is no point $P \neq O$ of finite order in $\mathcal{E}_{(p)}$.*

Proof. It is sufficient to show there is no point of prime order q.

□

6. Find all points of finite order on the elliptic curve

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + 17.$$

Answer: *According to the Nagell-Lütz theorem, a point $P = (x, y)$ of finite order must have $x, y \in \mathbb{Z}$ with $y = 0$ or $y^2 | D$, where D is the discriminant of the cubic.*

In this case

$$\begin{aligned} D &= -(4b^2 + 27c^2) \\ &= -27 \cdot 17^2. \end{aligned}$$

Thus $y = 0$ or

$$y = 3^a 17^b$$

where $a, b \in \{0, 1\}$. In other words,

$$y \in \{0, \pm 1, \pm 3, \pm 17, \pm 3 \cdot 17\}.$$

There is no integer solution with $y = 0$.

If $y = \pm 1$ then

$$x^3 = 1 - 17 = -16$$

which again has no integer solution.

If $y = \pm 3$ then

$$x^3 = 9 - 17 = -8 \implies x = -2.$$

If $y = \pm 17$ then

$$x^3 = 17^2 - 17 = 17 \cdot 16,$$

with no integer solution.

Finally, if $y = \pm 3 \cdot 17$ then

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

with no integer solution.

Hence the only possible points of finite order are $(-2, \pm 3)$. [Recall that Nagell-Lütz gives a necessary but not sufficient condition for a point to be of finite order.] Let $P = (-2, 3)$.

The tangent at P has slope

$$\begin{aligned} m &= \frac{3x^2}{2y} \\ &= \frac{12}{6} \\ &= 2. \end{aligned}$$

If the tangent at P meets the curve again at $-2P = (x_2, y_2)$ then

$$-2 - 2 + x_2 = m^2 = 4,$$

ie

$$x_2 = -8.$$

Since we have seen that there is no point of finite order with $x_2 = -8$ it follows that $-2P$ is of infinite order, and so therefore is P.

Hence the only point of finite order on $\mathcal{E}$ is $O = [0, 1, 0]$.

7. Define the Weierstrass elliptic function $\wp(z)$ with respect to a lattice $\Lambda \subset \mathbb{C}$, and establish the functional equation linking $\wp'(z)$ and $\wp(z)$.

   Show that any even function which is elliptic (doubly-periodic) with respect to Λ is expressible as a rational function in $\wp(z)$.

   Express the Weierstrass elliptic function $\wp_{2L}(z)$ with respect to the lattice $2\Lambda = \{2\omega : \omega \in \Lambda\}$ in terms of $\wp_\Lambda(z)$.

   Answer: *We define*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L,\ \omega \neq 0} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

8. Find the rank of the curve

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 - x.$$

Answer: *There are 3 points of order 2 on $\mathcal{E}$:*

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

The associated elliptic curve is

$$\tilde{\mathcal{E}}(\mathbb{Q}) : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x,$$

ie

$$\tilde{\mathcal{E}} : y^2 = x^3 + 4x.$$

Let the rank be r. Then

$$2^{r+2} = |im\,\chi| \cdot \left|im\,c\tilde{h}i\right|,$$

where

$$\chi : \mathcal{E} \to \mathbb{Q}^{\times 2}/\mathbb{Q}^{\times}, \quad \tilde{\chi} : \tilde{\mathcal{E}} \to \mathbb{Q}^{\times 2}/\mathbb{Q}^{\times}$$

are the auxiliary homomorphisms.
We have

$$im\,\chi \subset \{\pm 1\}.$$

Since $-1 \in im\,\chi$ [as $\chi(0,0) = -1$],

$$im\,\chi = \{\pm 1\}.$$

On the other hand,

$$im\,\tilde{\chi} \subset \{\pm 1, \pm 2\}.$$

[Recall that $e \in im\,\chi$ where $ef = b$ if and only if the auxiliary equation

$$u^2 = es^4 + as^2t^2 + ft^4$$

has a solution with $\gcd(s,t) = \gcd(u,t) = 1$.]
If $e = -1$ then $f = -4$, and $-1 \in im\,\tilde{\chi}$ if and only if

$$s^2 = -s^4 - 4t^4,$$

which is clearly impossible.
It follows that

$$|im\,\tilde{\chi}| \le 2,$$

and so

$$2^{r+2} \le 2 \cdot 2.$$

Hence
$$r = 0.$$
[One might recall that the n is a congruent number — ie there exists a right-angle triangle with rational sides and area n — if and only if the elliptic curve
$$y^2 = x^3 - n^2x$$
has rank > 0. Thus our result is equivalent to the well-known result that 1 is not a congruent number.]

9. Find all rational points on the curve
$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + 1.$$

Answer: *Let us first determine the points of finite order. By Nagell-Lütz, if $P = (x, y)$ is such a point then $x, y \in \mathbb{Z}$ and either $y = 0$ or*
$$y^2 \mid D,$$
where
$$D = -(4b^3 + 27c^2) = -3^3.$$
Hence
$$y \in \{0, \pm 1, \pm 3\}.$$
If $y = 0$ then $x = -1$, giving just one point $(-1, 0)$ of order 2.

If $y = \pm 1$ then $x^3 = 0$, giving the two points $(0, \pm 1)$.

If $y = \pm 3$ then $x^3 = -8$, giving the two points $(-2, \pm 3)$.

It remains to determine if these points are of finite order.

The slope at (x, y) is
$$m = \frac{3x^2}{2y},$$
and the tangent
$$y = mx + c$$
meets the curve again at (x_2, y_2), where
$$2x + x_2 = m^2.$$

Let
$$P = (0, 1).$$
The slope at P is $m = 0$, and the tangent
$$y = 1$$

meets the curve again where $x_2 = 0$, *ie* P *is a point of inflexion satisfying*

$$3P = 0.$$

Since there are points of orders 2 and 3, and there are ≤ 6 *points of finite order, the torsion group must be* $\mathbb{Z}/(6)$, *and the points* $(-2, \pm 3)$ *must be of order 6.*

Now we must determine the rank of the curve. First we bring the root $x = -1$ *of the cubic to 0, by the transformation* $x' = x + 1$. *Dropping the* $'$*ss the curve is now*

$$\mathcal{E} = \mathcal{E}(\mathbb{Q}) : y^2 = x^3 - 3x^2 + 3x.$$

The associated curve is

$$\tilde{\mathcal{E}} : y^2 = x^3 + 6x^2 - 3x.$$

The rank r *is given by*

$$2^{r+2} = |im\,\chi| \cdot |im\,\tilde{\chi}|\,,$$

where

$$\chi : \mathcal{E} \to \mathbb{Q}^{\times 2}/\mathbb{Q}^{\times}, \quad \tilde{\chi} : \tilde{\mathcal{E}} \to \mathbb{Q}^{\times 2}/\mathbb{Q}^{\times}$$

are the auxiliary homomorphisms.

We have

$$\{1, 3\} \subset im\,\chi \subset \{\pm 1, \pm 3\}$$

(working always $\bmod \mathbb{Q}^{\times 2}$*).*

If $e = -1$ *then* $ef = b = 3 \implies f = -3$; *and* $e \in im\,\chi$ *if and only if the auxiliary equation*

$$u^2 = es^4 + ft^4$$

has a solution with $\gcd(s, t) = \gcd(u, t) = 1$. *This is evidenly impossible with* $e, f < 0$. *Hence* $-1 \notin im\,\chi$, *and so*

$$im\,\chi = \{1, 3\}.$$

Turning to the $\tilde{\chi}$,

$$\{1, -3\} \subset im\,\tilde{\chi} \subset \{\pm 1, \pm 3\}.$$

If $e = -1$ *then* $ef = \tilde{b} = -3 \implies f = 3$. *Thus* $-1 \in im\,\tilde{\chi}$ *if and only if the auxiliary equation*

$$u^2 = -s^4 + 3t^4$$

has a solution with $\gcd(s,t) = \gcd(u,t) = 1$*. If* s, t *are both odd then*

$$u^2 \equiv -1 + 3 = 2 \bmod 8,$$

which is impossible. If s *is even and* t *is odd then*

$$u^2 \equiv 3 \bmod 8,$$

which is again impossible. Finally, if s *is odd and* t *is even then*

$$u^2 \equiv -1 \bmod 8,$$

which is still impossible.

We conclude that

$$-1 \notin im\, \tilde{\chi}.$$

Hence

$$im\, \tilde{\chi} = \{1, -3\},$$

and so

$$r = 0.$$

Hence the only rational points on the curve are the points of finite order: $(-1, 0), (0, \pm 1), (2, \pm 3)$*.*

10. Solve the equation

$$x^4 + 4x + 1 = 0.$$

Answer: *We can write the equation as*

$$(x^2 + \lambda)^2 = 2\lambda x^2 - 4x + (\lambda^2 - 1).$$

The right-hand side will be a perfect square if

$$2^2 = 2\lambda(\lambda^2 - 1),$$

ie

$$\lambda^3 - \lambda - 2 = 0.$$

To solve this equation, let

$$\lambda = u + v.$$

Then

$$u^3 + v^3 + (u + v)(3uv - 1) - 2 = 0.$$

Let us choose u, v so that

$$3uv = 1.$$

Then

$$u^3 + v^3 = 2.$$

On the other hand,

$$u^3 v^3 = 1/27.$$

Thus u^3, v^3 are the roots of

$$t^2 - 2t + 1/27 = 0.$$

Hence

$$u^3, v^3 = 1 \pm \sqrt{1 - 1/27} = 1 \pm \sqrt{26/27}.$$

Thus

$$u, v = \sqrt[3]{1 \pm \sqrt{26/27}},$$

and so

$$\lambda = \sqrt[3]{1 + \sqrt{26/27}} + \sqrt[3]{1 - \sqrt{26/27}}.$$

With this value of λ the original equation reduces to

$$x^2 + \lambda = \pm\sqrt{2\lambda}(x - \sqrt{2}/\lambda),$$

ie

$$x^2 \mp \sqrt{2/\lambda}x + (\lambda \pm 1/\sqrt{\lambda}).$$

The solutions of these 2 quadratics give the 4 roots of the original polynomial.