Course 428

Elliptic Curves I

Dr Timothy Murphy

Maxwell Theatre Friday, 21 January 2000 10:15–11:45

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 $P = (-2, 3),\ Q = (2, 5)$ on the curve

   $$y^2 = x^3 + 17$$

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

   Answer:

   (a) *Let the line PQ meets the curve again in the point R. Then*

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

   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*

   $$\det \begin{pmatrix} x & y & 1 \\ -2 & 3 & 1 \\ 2 & 5 & 1 \end{pmatrix} = 0,$$

   ie

   $$-2x + 4y - 16 = 0,$$

   ie

   $$y = \frac{1}{2}x + 4.$$

This meets the curve where

$$(\frac{1}{2}x+4)^2 = x^3+17.$$

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

$$-2+2+x = \frac{1}{4},$$

ie

$$x = \frac{1}{4}.$$

From the equation of the line

$$y = \frac{1}{8}+4 = \frac{33}{8}.$$

Thus

$$\begin{aligned} P+Q &= -(\frac{1}{4}, \frac{33}{8}) \\ &= (\frac{1}{4}, -\frac{33}{8}). \end{aligned}$$

(c) We have

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

ie

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

Thus the tangent at P *has slope*

$$m = \frac{12}{6} = 2.$$

Hence the tangent is

$$y-3 = 2(x+2),$$

ie

$$y = 2x + 7.$$

This meets the curve where

$$(2x + 7)^2 = x^3 + 17.$$

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

$$2 + 2 + x = 4$$

ie

$$x = 0.$$

From the equation of the tangent,

$$y = 7.$$

Thus

$$\begin{aligned} 2P &= -(0, 7) \\ &= (0, -7). \end{aligned}$$

2. Express the 5-adic integer $2/3 \in \mathbb{Z}_5$ in standard form

$$1/3 = a_0 + a_1 5 + a_2 5^2 + \cdots \qquad (0 \leq a_i < 5).$$

Does there exist a 5-adic integer x such that $x^2 = 6$?

Answer:

(a) *We have*

$$\frac{2}{3} \equiv 4 \bmod 5$$

since $3 \cdot 4 \equiv 2 \bmod 5$.

Now

$$\frac{2}{3} - 4 = \frac{-10}{3} = 5\frac{-2}{3},$$

while

$$\frac{-2}{3} \equiv 1 \bmod 5.$$

Thus
$$\frac{2}{3} \equiv 4 + 1 \cdot 5 \bmod 5^2.$$
Furthermore,
$$\frac{-2}{3} - 1 = \frac{-5}{3} = 5\frac{-1}{3},$$
while
$$\frac{-1}{3} \equiv 3 \bmod 5.$$
Thus
$$\frac{2}{3} \equiv 4 + 1 \cdot 5 + 3 \cdot 5^2 \bmod 5^3.$$
Continuing,
$$\frac{-1}{3} - 3 = \frac{-10}{3} = 5\frac{-2}{3}.$$
We have been here before;
$$\frac{-2}{3} \equiv 1 \bmod 5.$$
Thus
$$\frac{2}{3} \equiv 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 \bmod 5^4.$$
We have entered a loop; and the pattern will repeat itself indefinitely. We conclude that
$$\frac{2}{3} = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + 1 \cdot 5^5 + 3 \cdot 5^6 + \cdots .$$
Let us verify this; the sum on the right is
$$\begin{aligned} 4 + \frac{5}{1-5^2} + \frac{3 \cdot 5^2}{1-5^2} &= 4 + 5\frac{1+15}{-24} \\ &= 4 - 5\frac{2}{3} \\ &= \frac{2}{3}. \end{aligned}$$

(b) *The equation*
$$x^2 = 6 = 1 + 5$$
has just two solutions $\pm x$ *in* Z_5.
Note first what this means: we can find a sequence $x_0, x_1, \cdots \in \mathbb{Z}$ *such that*
$$x_n^2 \equiv 6 \bmod 5^n;$$

while if $m \leq n$ *then*

$$x_m \equiv x_n \bmod 5^m.$$

We shall show that if we have a solution x_n *we can always extend it to a solution* x_{n+1}.

Since

$$x^2 \equiv 1 \bmod 5 \implies x \equiv \pm 1 \bmod 5,$$

any solution must be $\equiv \pm 1 \bmod 5$. *If* x *is a solution so is* $-x$, *so we may assume that* $x \equiv 1 \mod 5$.

By hypothesis,

$$x_n^2 \equiv 6 \bmod 5^n,$$

ie

$$x_n^2 = 6 + a5^n,$$

for some $a \in \mathbb{Z}$.

Now set

$$x_{n+1} = x_n + z5^n.$$

Then

$$\begin{aligned} x_{n+1}^2 &= x_n^2 + 2zx_n5^n + z^2 5^{2n} \\ &= 6 + (a + 2zx_n)5^n + z^2 5^{2n} \\ &\equiv 6 + (a + 2zx_n)5^n \bmod 5^{n+1}, \end{aligned}$$

assuming $n \geq 1$.

Thus

$$x_{n+1}^2 \equiv 6 \bmod 5^{n+1}$$

if z *satisfies the equation*

$$a + 2zx_n \equiv 0 \bmod 5.$$

But this equation has a unique solution, since $x_n \equiv 1 \bmod 5$, *namely*

$$\begin{aligned} z &= -2^{-1}a \bmod 5 \\ &= 2a \bmod 5. \end{aligned}$$

We conclude that we can always extend our solution to an arbitrarily high power $\bmod 5^n$*, and so construct a solution in* $\mathbb{Z}_5$*.*

This argument is a standard one in p-adic theory. There may or may not be solutions to an equation $\bmod p, \bmod p^2, \ldots$*. But at a certain point one finds that a solution* $\bmod p^n$ *can be extended uniquely to a solution* $\bmod p^{n+1}$*, and then to a solution* $\bmod p^{n+2}$*, and so on.*

This is expressed formally in Hensel's Lemma, a simple form of which states that if we are given a polynomial $f(x) \in \mathbb{Z}[x]$ *then any solution*

$$f(x_0) \equiv 0 \bmod p$$

for which

$$f'(x_0) \not\equiv 0 \bmod p$$

(where $f'(x)$ *is the derivative of* $f(x)$*) extends uniquely to a solution* $x \in \mathbb{Z}_p$ *of the p-adic equation*

$$f(x) = 0.$$

This follows on considering the binomial expansion

$$f(x_n + zp^n) \equiv f(x_n) + zf'(x_n)p^n \bmod p^{n+1}.$$

An alternative way of solving the original equation is to imitate real analysis, using the binomial expansion of $(1+x)^{1/2}$*. Thus*

$$\begin{aligned} 6^{1/2} &= (1+5)^{1/2} \\ &= 1 + \frac{1}{2}5 + \frac{\frac{1}{2}\cdot -\frac{1}{2}}{1\cdot 2}5^2 + + \frac{\frac{1}{2}\cdot -\frac{1}{2}\cdot -\frac{3}{2}}{1\cdot 2\cdot 3}5^3 + \cdots \\ &= 1 + 2^{-1}5 + \frac{1}{1\cdot 2}2^{-2}5^2 + \frac{1\cdot 3}{1\cdot 2\cdot 3}2^{-3}5^3 + \cdots \end{aligned}$$

To show that this series converges in $\mathbb{Z}_5$*, we need to show that the coefficients do not get large (in p-adic terms) quicker than the powers* 5^n *get small.*

As it happens, in this case the coefficients do not get large at all, as they are all 5*-adic integers. For*

$$\begin{aligned} \frac{1\cdot 3\cdots(2n-1)}{1\cdot 2\cdots n} &= \frac{1\cdot 2\cdot 3\cdots 2n}{(2\cdot 4\cdots 2n)(1\cdot 2\cdots n)} \\ &= 2^{-n}\frac{(2n)!}{n!n!} \\ &= 2^{-n}\binom{2n}{n}, \end{aligned}$$

and we know of course that this binomial coefficient is an integer. Even if we weren't so fortunate, it is not hard to see that $n!$ *gets small (in p-adic terms) slower than* p^n*. For suppose*

$$p^e \parallel n,$$

ie $p^e \mid n$ *but* $p^{e+1} \nmid n$*. Then*

$$\begin{aligned} e &= [n/p] + [n/p^2] + \cdots \\ &< n/p + n/p^2 + \cdots \\ &= \frac{n}{p} \cdot \frac{1}{1 - 1/p} \\ &= \frac{n}{p-1} \end{aligned}$$

ie

$$\|n!\|_p > p^{-n/(p-1)} \geq p^{-n/2},$$

while

$$\|p^n\|_p = p^{-n},$$

3. Show that the group of the elliptic curve

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

over the finite field $\mathbb{F}_7$ is cyclic, and find a generator.

Answer: *Let us find the 'finite' points on the curve. The quadratic residues* mod7 *are:* $0, 1, 2, 4$*. The following table is more-or-less self-explanatory.*

x	y^2	y
0	1	± 1
1	1	± 1
2	5	X
3	5	X
$4 = -3$	0	0
$5 = -2$	3	X
$6 = -1$	6	X

Thus there are 5 finite points on the curve. Adding the point at infinity, we see that the curve is of order 6. But the only abelian group of order 6 is the cyclic group $\mathbb{Z}/(6)$*.*

There is just one element of order 2, namely $(4, 0)$. *There must be two elements of order 3, and two elements of order 6.*

Let $P = (0, 1)$. *The slope of the tangent at the point* (x, y) *is*

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

Thus the slope at P *is* $m = 0$, *and so the tangent is*

$$y = 1.$$

This meets the curve again at the point $(1, 1)$. *Hence*

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

Thus $2P \neq -P = (0, -1)$. *Hence* P *does not have order 3; so it must have order 6, ie* P *is a generator of the group.*

4. Outline the proof that a point $P = (x, y)$ of finite order on the elliptic curve

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

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

Answer: *[The proof below does not use p-adic numbers explicitly, as I do in my notes. However, the idea is the same. In particular, we prove the result by showing that* x, y *are p-adic integers for each prime p, ie p does not divide the denominators of* x *and* y.*]*

In homogeneous coordinates the curve has equation

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

We work in the affine patch $Y \neq 0$, *setting* $Y = 1$:

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

Lemma: *If* $\|Z\|_p < 1$ *(ie* $p \mid Z$*) then* $\|X\|_p < 1$, *and in fact*

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

Proof: *If* $\|X\|_p \geq 1$ *then* X^3 *dominates the equation, ie all other terms have smaller p-adic value, which is impossible.*

So $\|X\|_p < 1$; and then the terms aX^2Z, bXZ^2, cZ^3 all have p-adic value smaller then Z. Hence Z and X^3 must have the same p-adic value.

We set

$$\mathscr{E}_{p^e} = \{[X, 1, Z] : \|X\| \leq p^{-e}, \|Z\| < 1\}.$$

Lemma: *Suppose $P_1, P_2 \in \mathscr{E}_{p^e}$. Then $P_1 + P_2 \in \mathscr{E}_{p^e}$. Moreover, if $P_1 = [X_1, 1, Z_1], P_2 = [X_2, 1, Z_2], P + 1 + P_2 = [X_3, 1, Z_3]$ then*

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

Proof: *Let the line P_1P_2 be*

$$Z = MX + C.$$

Then

$$M = \frac{Z_2 - Z_1}{X_2 - X_1}.$$

Subtracting the equation for the two points,

$$Z_2 - Z_1 = (X_2^3 - X_1^3) + a(X_2^2Z_2 - X_1^2Z_1) + b(X_2Z_2^2 - X_1Z_1^2) + c(Z_2^3 - Z_1^3).$$

Writing

$$X_2^2Z_2 - X_1^2Z_1 = (X_2^2 - X_1^2)Z_2 + X_1^2(Z_2 - Z_1), \quad X_2Z_2^2 - X_1Z_1^2 = (X_2 - X_1)Z_2^2 + X_1(Z_2^2 - Z_1^2),$$

we derive

$$\begin{aligned} \frac{Z_2 - Z_1}{X_2 - X_1} &= \frac{(X_1^2 + X_1X_2 + X_2^2) + a(X_1 + X_2)Z_2 + bZ_2^2}{1 - aX_1^2 - bX_1(Z_1 + Z_2) - c(Z_1^2 + Z_1Z_2 + Z_2^2)} \\ &= \frac{N}{D}, \end{aligned}$$

say. Evidently

$$\|N\|_p \leq p^{-2e}, \quad \|D\|_p = 1.$$

Thus

$$\|M\|_p \leq p^{-2e}.$$

Since

$$C = Z_1 - MX_1,$$

it follows that

$$\|C\|_p \leq p^{-3e}.$$

The line P_1P_2 meets the curve where

$$MX + C = X^3 + aX^2(MX + C) + bX(MX + C)^2 + c(MX + C)^3.$$

Since $-[X, 1, Z] = [-X, 1, -Z]$, the roots of this equation are $X_1, X_2, -X_3$. Thus

$$X_1 + X_2 - X_3 = \frac{a + 2bM + 3cM^2}{1 + aM + bM^2 + cM^3} C.$$

We conclude that

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

Corollary: *If $P \in \mathscr{E}_{p^e}$ then*

$$X(nP) \equiv nX(P) \bmod p^{3e}.$$

Lemma: *The only point of finite order in $\mathscr{E}_p$ is $O = [0, 1, 0]$.*

Proof: *Suppose P is of order n, and suppose q is a prime factor of n. Then $(n/q)P$ is of order q. Hence we may suppose that P is of prime order q.*

But

$$X(qP) \equiv qX(P) \bmod p^{3e}$$

It follows that

$$\|X(qP)\|_p = p^e$$

if $q \neq p$, while

$$\|X(pP)\|_p = p^{e+1}.$$

if $q = p$. In either case $qP \neq 0$.

Lemma: *If (x, y) is of finite order then*

$$\|x\|_p \leq 1, \quad \|y\|_p \leq 1.$$

Proof: *Conversion from X, Z coordinates to x, y coordinates is given by*

$$[X, 1, Z] = [X/Z, 1/Z, 1] = [x, 1, y].$$

Thus

$$y = \frac{1}{Z}.$$

Since $P \notin \mathscr{E}_p$,

$$\|Z\|_p \geq 1.$$

Thus

$$\|y\|_p \leq 1.$$

If $\|x\|_p > 1$ *then* x^3 *dominates the equation. Hence*

$$\|x\|_p \leq 1.$$

Since this is true for all primes p, we conclude that

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

5. 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

$$2R = 4P = (2, 3) = T,$$

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 $T = 4P$.

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

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

over the rationals $\mathbb{Q}$.

Answer: *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, with 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 finitely-generated abelian groups.

How many abelian groups of order 36 (up to isomorphism) are there?

Answer:

(a) *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.

(b) *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

$$A_3 = \mathbb{Z}/(9) \text{ or } \mathbb{Z}/(3) \oplus \mathbb{Z}/(3).$$

It follows that there are just 4 abelian groups of order 36, namely

$$\begin{gathered}
\mathbb{Z}/(4) \oplus \mathbb{Z}/(9) = \mathbb{Z}/(36),\\
\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(9) = \mathbb{Z}/(18) \oplus \mathbb{Z}/(2),\\
\mathbb{Z}/(4) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(3) = \mathbb{Z}/(12) \oplus \mathbb{Z}/(3),\\
\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(3) = \mathbb{Z}/(6) \oplus \mathbb{Z}/(6).
\end{gathered}$$