Course 428
Elliptic Curves II

Dr Timothy Murphy

Joly Theatre Friday, 5 April 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. Prove Fermat's Last Theorem *either* for $n = 3$ *or* for $n = 4$.

Answer:

$n = 3$ *We work in the field*

$$K = \mathbb{Q}(\omega),$$

where $\omega = e^{2\pi/3}$, *so that* $\omega^3 = 1$ *and* $1 + \omega + \omega^2 = 0$.
The integers in this field are the numbers

$$a + b\omega \quad (a, b \in \mathbb{Z}),$$

and the units are $\pm 1, \pm\omega, \pm\omega^2$. *The ring of integers* $A = \mathbb{Z}[\omega]$, *is a unique factorisation domain.*
Each number

$$\alpha = x + y\omega \in K$$

has conjugate

$$\bar{\alpha} = x + y\omega^2,$$

and

$$N(\alpha) = \alpha\bar{\alpha} = x^2 - xy + y^2.$$

Let

$$\pi = 1 - \omega.$$

Then

$$\bar{\pi} = 1 - \omega^2 = -\omega^2 \pi.$$

Since

$$N(\pi) = 3,$$

it follows that 3 ramifies:

$$3 = \epsilon \pi^2,$$

where $\epsilon = -\omega^2$.

The residues $\bmod \pi$ *are represented by* $0, \pm 1$.

Lemma 1. *If*

$$\alpha \equiv \pm 1 \bmod \pi$$

then

$$\alpha^3 \equiv \pm 1 \bmod \pi^3.$$

Proof. It is sufficient to prove the result if $\alpha \equiv 1 \bmod \pi$, ie

$$\alpha = 1 + \pi\beta.$$

Then

$$\alpha^3 \equiv 1 + 3\pi\beta + 3\pi^2\beta^2 \bmod \pi^3.$$

Since

$$\pi^2 \mid 3$$

the result follows. □

We want to show that

$$x^3 + y^3 + z^3 = 0$$

has no solution with $x, y, z \in \mathbb{Z}$ *and* $xyz \neq 0$. *We shall prove the more general result that for any unit* $\epsilon \in A$ *the equation*

$$x^3 + y^3 + \epsilon z^3 = 0$$

has no solution in A *with* $xyz \neq 0$.

Suppose we have such a solution. We may assume that $\gcd(x, y, z) = 1$. *Then*

$$(x + y)(x + \omega y)(x + \omega^2 y) = -\epsilon z^3.$$

$n = 4$ *We have to show that the equation*

$$x^4 + y^4 = z^4$$

has no non-trivial solution in $\mathbb{Z}$ *(ie with* $xyz \neq 0$*). In fact we prove the stronger result that*

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

has no non-trivial solution. We may assume without loss of generality that $x, y, z > 0$ *and that*

$$\gcd(x, y, z) = 1.$$

Recall that the integers $x, y, z > 0$ *are said to form a* Pythagorean triple *if* $\gcd(x, y, z) = 1$ *and*

$$x^2 + y^2 = z^2.$$

Lemma 2. *If* x, y, z *is Pythagorean triple then one of* x, y *is even and one is odd. The general Pythagorean triple with* y *even takes the form*

$$x = u^2 - v^2,\ y = 2uv,\ z = u^2 + v^2,$$

with $u, v \geq 0$ *and* $\gcd(u, v) = 1$.

In our case x^2, y^2, z *is a Pythagorean triple. If* y *is even then*

$$x^2 = u^2 - v^2,\ y^2 = 2uv,\ z = u^2 + v^2.$$

Since x *is odd, one of* u, v *is odd and one is even. If* u *were even and* v *were odd then*

$$x^2 = u^2 - v^2 \equiv -1 \mod 4,$$

which is impossible. Hence u *is odd and* v *is even.*
Since $y^2 = 2uv$ *and* $\gcd(u, v) = 1$ *it follows that*

$$u = s^2,\ v = 2t^2,$$

with $\gcd(s, t) = 1$.
Thus

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

ie

$$x^2 + 4t^4 = s^4.$$

Now $x, 2t^2, s^2$ is a Pythagorean triple. It follows that

$$x = a^2 - b^2,\ 2t^2 = 2ab,\ s^2 = a^2 + b^2,$$

with $\gcd(a, b) = 1$.
Since $t^2 = ab$ and $\gcd(a, b) = 1$, *it follows that*

$$a = X^2,\ b = Y^2,$$

with $\gcd(X, Y) = 1$.
If we set $s = Z$ then

$$X^4 + Y^4 = Z^2.$$

Thus one solution x, y, z of our equation leads to a second solution X, Y, Z. Also

$$Z^4 = s^4 = u^2 < z,$$

since $v \neq 0$.
Thus each solution gives rise to a new solution with strictly smaller z, which is evidently impossible.

2. (a) Solve the equation

$$x^3 + 3x - 1 = 0.$$

(b) Solve the equation

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

Answer:

(a) Set

$$x = u + v.$$

Then

$$x^3 = u^3 + v^3 + 3uv(u + v).$$

Thus

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

Let

$$uv + 1 = 0.$$

Then

$$u^3 + v^3 = -1,$$

while

$$uv = -1 \implies u^3v^3 = -1.$$

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

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

Hence

$$u^3, v^3 = \frac{-1 \pm \sqrt{5}}{2}.$$

We conclude that the equation has the real solution

$$x = \left(\frac{-1+\sqrt{5}}{2}\right)^{1/3} + \left(\frac{-1-\sqrt{5}}{2}\right)^{1/3},$$

together with the complex solutions

$$x = \left(\frac{-1+\sqrt{5}}{2}\right)^{1/3} \omega + \left(\frac{-1-\sqrt{5}}{2}\right)^{1/3} \omega^2,$$

$$x = \left(\frac{-1+\sqrt{5}}{2}\right)^{1/3} \omega^2 + \left(\frac{-1-\sqrt{5}}{2}\right)^{1/3} \omega.$$

(b) We can write

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

The quadratic on the right will be a perfect square if

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

ie

$$\lambda^3 + \lambda = 2.$$

One solution of this is $\lambda = 1$. Setting $\lambda = 1$, our equation reads:

$$(x^2 + 1)^2 = 2(x + 1)^2.$$

Thus

$$x^2 + 1 = \pm\sqrt{2}(x + 1),$$

ie

$$x^2 - \sqrt{2}x + (1 - \sqrt{2}),\ x^2 + \sqrt{2}x + (1 + \sqrt{2}).$$

Solving these two quadratic equations,

$$x = \frac{-\sqrt{2} \pm \sqrt{2}\sqrt{2\sqrt{2} - 1}}{2},$$

$$x = \frac{\sqrt{2} \pm i\sqrt{2}\sqrt{2\sqrt{2} + 1}}{2}.$$

3. Show that a torsion-free finitely-generated abelian group A is free, ie

$$A \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$

Find a Z-basis $e_1, \ldots, e_r$ for the group

$$A = \{(x, y, z) \in \mathbb{Z}^3 : x + 2y + 3z = 0\},$$

ie a set of elements such that each element $a \in A$ is uniquely expressible in the form

$$a = n_1 e_1 + \cdots + n_r e_r,$$

with $n_1, \ldots, n_r \in \mathbb{Z}$.

4. State Mordell's Theorem, and sketch its derivation from the Weak Mordell Theorem (which states that if $\mathcal{E} = \mathcal{E}(\mathbb{Q})$ is an elliptic curve over the rationals then the quotient-group $\mathcal{E}/2\mathcal{E}$ is finite).

5. Determine the rank of the elliptic curve

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

Answer: *Since the cubic $p(x) = x^3 - x$ has 3 rational roots, we have two methods of attacking the problem.*

Method 1 *The associated elliptic curve is*

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

Let the associated homomorphisms be

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

Since $p(x)$ has 3 rational roots, and $\tilde{b} = 4$ is a perfect square, the rank r is given by

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

Since $b = -1,\ \tilde{b} = 4$,

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

Also

$$\chi(0,0) = b = -1,\ \tilde{\chi}(0,0) = \tilde{b} = 4.$$

It follows that

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

If $d \in \operatorname{im}\tilde{\chi}$ and $dd' = \tilde{b} = 4$ then the equation

$$du^4 + d't^4 = v^2$$

has a solution with $\gcd u, t = 1 = \gcd v, t$. If $d < 0$ then $d' < 0$ and the equation evidently has no solution. Hence

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

It follows that

$$2^{r+2} \leq 2 \cdot 2,$$

ie

$$r = 0.$$

Method 2 *Let*

$$\chi_0, \chi_1, \chi_{-1} : \mathscr{E} \to \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$$

be the associated homomorphisms. Thus

$$\begin{aligned}\chi_0(x, y) &= x \bmod \mathbb{Q}^{\times 2},\\ \chi_1(x, y) &= x - 1 \bmod \mathbb{Q}^{\times 2},\\ \chi_0(x, y) &= x + 1 \bmod \mathbb{Q}^{\times 2},\end{aligned}$$

except that

$$\begin{aligned}\chi_0(0, 0) &= p'(0) = -1,\\ \chi_1(1, 0) &= p'(1) = 2,\\ \chi_{-1}(-1, 0) &= p'(-1) = 2.\end{aligned}$$

By Mordell's Lemma,

$$2\mathscr{E} = \ker(\chi_0 \times \chi_1 \times \chi_{-1}),$$

and so

$$\mathscr{E}/2\mathscr{E} = \mathrm{im}(\chi_0 \times \chi_1 \times \chi_{-1}),$$

Moreover, since $p(x)$ has 3 rational roots,

$$2^{r+2} = |\mathscr{E}/2\mathscr{E}|.$$

If $(x, y) \in \mathscr{E}$ then

$$x = \frac{du^2}{t^2},\ y = \frac{v^2}{t^2}$$

where d is square-free. Thus

$$\begin{aligned}x - 1 &= \frac{du^2 - t^2}{t^2} = \frac{ev^2}{t^2},\\ x + 1 &= \frac{du^2 + t^2}{t^2} = \frac{fw^2}{t^2},\end{aligned}$$

where e, f are square-free; and

$$(\chi_0 \times \chi_1 \times \chi_{-1})(x, y) = (d, e, f),$$

if $x \neq 0, \pm 1$. *Moreover* def *is a perfect square, since*

$$y^2 = \frac{defu^2v^2w^2}{t^6}.$$

From above,

$$ev^2 = du^2 - t^2, \ fw^2 = du^2 + t^2.$$

It follows from this that

$$\begin{aligned} d > 0 &\implies f > 0 \implies e > 0, \\ d < 0 &\implies e < 0 \implies f > 0. \end{aligned}$$

In particular $f > 0$ *in all cases.*

Also

$$d \mid 1, \ e \mid 2, \ f \mid 2.$$

It follows that

$$\operatorname{im}(\chi_0 \times \chi_1 \times \chi_{-1}) \subset \{(1,1,1), (-1,-1,1), (1,2,2), (-1,-2,2)\}.$$

Hence

$$2^{r+2} \leq 4 \implies r = 0.$$

6. Determine the group (ie the torsion group and rank) of the elliptic curve

$$\mathscr{E}(\mathbb{Q}) : y^2 = x^3 - 1.$$

Answer: *First we make the constant term vanish by setting* $x = x' + 1$. *The equation becomes*

$$\mathscr{E} : y^2 = x'^3 + 3x'^2 + 3x'.$$

The associated elliptic curve is given by

$$\tilde{a} = -2a, \ \tilde{b} = a^2 - 4b.$$

Thus the associated curve is

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

If the associated homomorphisms are

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

then the rank r *is given by*

$$2^{r+1} = \frac{|\operatorname{im}\chi||\operatorname{im}\tilde{\chi}|}{2},$$

since $\tilde{b} = -3$ *is not a perfect square.*

We have

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

Also

$$\chi(0,0) = 3,\ \tilde{\chi}(0,0) = -3.$$

If $d \mid 3$ *and* $dd' = 3$ *then* $d \in \operatorname{im}\chi$ *if and only if the equation*

$$du^4 + 3u^2t^2 + d't^4 = v^2$$

has a solution with $\gcd(u,t) = 1 = \gcd(v,t)$*.*

If $d = -1$ *then* $d' = 3$*, and the equation is*

$$-u^4 + 3u^2t^2 + 3t^4 = v^2.$$

Thus

$$-u^4 \equiv v^2 \bmod 3 \implies u \equiv v \equiv 0 \bmod 3.$$

Hence

$$9 \mid 3t^4 \implies 3 \mid t,$$

so that $\gcd(t,u) > 1$*, contrary to hypothesis. It follows that*

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

Similarly, if $d \mid 3$ *and* $dd' = 3$ *then* $d \in \operatorname{im}\tilde{\chi}$ *if and only if the equation*

$$du^4 - 6u^2t^2 + d't^4 = v^2$$

has a solution with $\gcd(u,t) = 1 = \gcd(v,t)$*. If* $d = -1$ *then* $d' = 3$*, and the equation is*

$$-u^4 - 6u^2t^2 + 3t^4 = v^2.$$

As before this implies that $3 \mid u, t$*, contrary to hypothesis. Hence*

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

It follows that

$$2^{r+2} = 2 \cdot 2 \implies r = 0.$$

It remains to determine the torsion subgroup of $\mathscr{E}$*. If* $(x,y) \in \mathscr{E}$ *then* $x, y \in \mathbb{Z}$*, and by Nagell-Lutz*

$$y = 0 \text{ or } y^2 \mid \Delta = -4b^3 - 27c^2 = -27.$$

Thus $y = 0, \pm 1, \pm 3$.

If $y = 0$ *then*

$$x^3 = 1 \implies x = 1.$$

If $y = \pm 1$ *then*

$$x^3 = 2,$$

which has no rational solution.

If $y = \pm 3$ *then*

$$x^3 = 10,$$

which also has no rational solution.

We conclude that

$$\mathscr{E} = \{0, (1, 0)\} \cong \mathbb{Z}/(2).$$

7. Determine the rank of the elliptic curve

$$\mathscr{E}(\mathbb{Q}) : y^2 = x^3 - 5x.$$

Answer: *We observe that*

$$P = (-1, 2) \in \mathscr{E}.$$

Let the tangent at P *be*

$$y = mx + c.$$

Then

$$m = \frac{3x^2 - 5}{2y} = -\frac{1}{2}.$$

The tangent meets the curve where

$$(mx + c)^2 = x^3 - 5x.$$

Thus if the tangent meets the curve again at $Q = (x, y)$ *then (by considering the coefficient of* x^2*)*

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

Thus x *is non-integral, and so* Q *is of infinite order. Hence* P *is also of infinite order. In particular the rank*

$$r \geq 1.$$

The associated elliptic curve is

$$\tilde{\mathscr{E}} : y^2 = x^3 + 20x.$$

Since $p(x) = x^3 - 5x$ *has just one rational root, and* 20 *is not a perfect square,*

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

where

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

are the auxiliary homomorphisms.

We have

$$\operatorname{im}\chi \subset \{\pm 1, \pm 5\},\ \operatorname{im}\tilde{\chi} \subset \{\pm 1, \pm 2, \pm 5, \pm 10\}.$$

Since

$$\chi(0,0) = -5,\ \chi(-1,2) = -1,$$

we have

$$\operatorname{im}\chi = \{\pm 1, \pm 5\}.$$

If $d \mid 20$ *and* $dd' = 20$ *then* $d \in \operatorname{im}\tilde{\chi}$ *if and only if the equation*

$$du^4 + d't^4 = v^2$$

has a solution with $t > 0$ *and* $\gcd(u,t) = 1 = \gcd(v,t)$*. If* $d < 0$ *then* $d' < 0$ *and this equation evidently has no solution. Hence*

$$\operatorname{im}\tilde{\chi} \subset \{1, 2, 5, 10\}.$$

Thus

$$2^{r+2} \leq 2 \cdot 2^2,$$

ie

$$r \leq 1.$$

Hence

$$r = 1.$$