Elliptic Curves 1994 — Answers

Timothy Murphy

May 25, 2004

1. Show that the equation
$$x^4 + y^4 = z^4$$
has no solutions in non-zero integers x, y, z.

Answer. We prove the stronger result, that
$$x^4 + y^4 = z^2$$
has no non-trivial solutions.

Suppose x, y, z is such a solution. We may assume that $x, y, z \geq 0$ and that
$$\gcd(x, y, z) = 1.$$
It is clear that just one of x and y is even, and that the other is odd, as also is z. We may thus assume that y is even.

We use the following result: The general solution in non-negative integers of
$$x^2 + y^2 = z^2$$
with $\gcd(x, y, z) = 1$ and y even is
$$x = u^2 - v^2,\ y = 2uv,\ z = u^2 + v^2$$
with $u \geq v \geq 0$ and $\gcd(u, v) = 1$.

In our case, we deduce that
$$x^2 = u^2 - v^2,\ y^2 = 2uv,\ z = u^2 + v^2,$$
with $\gcd(u, v) = 1$. Since x is odd we have $x^2 \equiv 1 \bmod 4$. It follows that u is odd, and v is even. From $y^2 = 2uv$ we deduce that
$$u = r^2,\ v = 2s^2.$$

Thus
$$x^2 = r^4 - 4s^4,\ y^2 = 4r^2s^2,\ z = r^4 + s^4.$$
If we set $t = x$ we see that from the solution (x, y, z) of our original equation
$$x^4 + y^4 = z^2$$
we have derived a solution (r, s, t) of the equation
$$r^4 - 4s^4 = t^2.$$
Concretely,
$$x = t,\ y = 2rs,\ z = r^4 + s^4.$$
Now we repeat the process, starting with the equation
$$r^4 - 4s^4 = t^2,$$
where $\gcd(r, 2s, t) = 1$*. From our lemma, we have*
$$r^2 = a^2 + b^2,\ 2s^2 = 2ab, t = a^2 - b^2,$$
with $\gcd(a, b) = 1$*.*
But this implies that
$$a = X^2,\ b = Y^2,$$
where $\gcd(X, Y) = 1$*; and so if we set $Z = r$ we have*
$$X^4 + Y^4 = Z^2,$$
with
$$r = Z,\ s = XY,\ t = X^4 - Y^4.$$
Thus from our original solution (x, y, z) of the equation
$$x^4 + y^4 = z^2$$
we have derived a second solution (X, Y, Z). We must show that this second solution is in some sense 'smaller'. In fact we have
$$z = r^4 + s^4 = X^4Y^4 + Z^4.$$
In particular
$$z \geq Z^4,$$
with equality possible only if $X = 0$ or $Y = 0$.

We can repeat this process to obtain a third solution of the equation, and then a fourth, and so on. We must end up with one of the solutions $(1, 0, 1),\ (0, 0, 0)$.

Since

$$(X, Y, Z) = (0, 0, 0) \implies (r, s, t) = (0, 0, 0) \implies (x, y, z) = (0, 0, 0),$$

the latter is impossible. On the other hand

$$(X, Y, Z) = (1, 0, 1) \implies (r, s, t) = (1, 0, 1) \implies (x, y, z) = (1, 0, 1);$$

so this case too cannot arise from a non-trivial solution.

We conclude that there cannot exist any solution with $x, y, z \neq 0$..

2. Show that the equation
$$x^3 + y^3 = z^3$$
has no solutions in non-zero integers x, y, z. (You may assume unique factorisation in the number ring $\mathbb{Z}[e^{2\pi i/3}]$).

Answer. Let us briefly recall the results we assume from algebraic number theory.

(a) *The ring*
$$I = \mathbb{Z}[\omega] = \{m + n\omega : m, n \in \mathbb{Z}\}$$
is the ring of algebraic integers in the number field
$$K = \mathbb{Q}(\omega),$$
where $\omega = e^{2\pi i/3}$.

(b) *The* norm *of* $z = m + n\omega$ *is the rational integer*
$$N(z) = z\bar{z} = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2.$$

(c) *The norm is multiplicative:*
$$N(wz) = N(w)N(z).$$

(d) *A number* $u \in I$ *is a unit if and only if* $N(u) = 1$.

(e) *The units in* I *are the numbers* $\pm 1, \pm\omega, \pm\omega^2$.

(f) *We say that* $x \in I$ *is* prime *if* $x \neq 0$, x *is not a unit, and* $x = yz$ *implies that* y *or* z *is a unit.*

(g) *We say that 2 primes x, y are equivalent, and we write $x \sim y$, if $y = ux$ for some unit u. In general we do not distinguish between equivalent primes.*

(h) *A number $x \in I$ is a prime if (but not only if) $N(u)$ is a rational prime.*

(i) *The number*

$$\pi = 1 - \omega$$

is a prime, with $N(\pi) = 3$.

(j) *Since*

$$\pi^2 = 1 - 2\omega + \omega^2 = -3\omega,$$

and $-\omega$ is a unit,

$$\pi^2 \sim 3.$$

(k) *We assume that there is unique factorisation into primes in I, up to multiplication by units.*

Lemma. If $x, y \in I$ then

$$x \equiv y \bmod \pi \implies x^3 \equiv y^3 \bmod \pi^3.$$

Proof. If

$$y = x + z\pi$$

then

$$\begin{aligned} y^3 - x^3 &= 3x^2 z\pi + 3xz^2\pi^2 \\ &\equiv 0 \bmod \pi^3. \end{aligned}$$

□

There are just 3 remainders modulo π, namely $0, \pm 1$. By the Lemma,

$$x \equiv \pm 1 \bmod \pi \implies x^3 \equiv \pm 1 \bmod \pi^3.$$

It follows that one of x, y, z is divisible by π. For otherwise

$$\begin{aligned} x^3 + y^3 + z^3 &\equiv \pm 1 \pm 1 \pm 1 \bmod \pi^3 \\ &\not\equiv 0 \bmod \pi^3. \end{aligned}$$

Two of x, y, z cannot be divisible by π, or the third would be also. Thus just one is divisible by π. We may assume (permuting x, y, z if necessary) that

$$\pi \nmid x, y, \ \pi \mid z$$

say

$$z = \pi z'.$$

Thus

$$x^3 + y^3 = \pi^3 (-z')^3.$$

We are going to prove the more general result:

Theorem. There do not exist $x, y, z \in \mathbb{Z}[\omega]$ satisfying

$$x^3 + y^3 = \epsilon \pi^3 z^3,$$

where ϵ is a unit, with

$$\pi \nmid x, y$$

and $z \neq 0$.

Proof. We can factorise the left-hand side:

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

Now

$$(x+y) - (x+\omega y) = \pi y,$$

and similarly

$$(x+\omega y) - (x+\omega^2 y) = \omega \pi y,$$

Hence

$$\pi \mid (x+y), (x+\omega y), (x+\omega^2 y).$$

[For if π didn't divide one of these, it would not divide any, and so it would not divide the product.]

It follows that

$$\gcd(x+y, x+\omega y) = \gcd(x+y, x+\omega^2 y) = \gcd(x+\omega y, x+\omega^2 y) = \pi.$$

Let

$$p = \frac{(x+y) - (x+\omega y)}{\pi} = y,$$
$$q = \frac{(x+y) - (x+\omega^2 y)}{\pi} = -\omega^2 y \equiv -y \bmod \pi.$$

Then
$$\frac{x+y}{\pi},\ \frac{x+\omega y}{\pi},\ \frac{x+\omega^2 y}{\pi}$$
are not congruent to each other modπ, and so must be congruent to $0.\pm 1$ in some order. In particular, just one of $(x+y),\ (x+\omega y),\ (x+\omega^2 y)$ must be divisible by π^2.

[This was shown in a different way in the answer to sample-428-2004 question 10b.]

Replacing y by ωy or $\omega^2 y$, if necessary, we may assume that
$$\pi^2 \mid (x+y).$$

But then
$$\begin{aligned}\pi^4 \mid \pi^3 z^3 &\implies \pi \mid z\\ &\implies \pi^6 \mid \epsilon\pi^3 z^3\\ &\implies \pi^4 \mid (x+y).\end{aligned}$$

Thus
$$x+\omega y = u\pi X^3,\ x+\omega^2 y = v\pi Y^3,\ x+y = w\pi^4 Z^3.$$
where u, v, w are units, $\pi \nmid X, Y$ and $Z \neq 0$.

Now
$$(x+y)+\omega(x+\omega y)+\omega^2(x+\omega^2 y) = 0.$$
Thus
$$u'X^3 + v'Y^3 + w'\pi^3 Z^3 = 0,$$
where u', v', w' are units, and $\pi \nmid X, Y$,

We may assume that $u' = 1$ (on dividing by u'). Thus
$$X^3 + v'Y^3 = w'\pi^3(-Z)^3.$$

Since
$$X^3, Y^3 \equiv \pm 1 \bmod \pi^3.$$
it follows that
$$1 \pm v' \equiv 0 \bmod \pi^3.$$
But this implies that
$$v' = \pm 1$$
[since eg $1+\omega = -\omega^2 \not\equiv 0 \bmod \pi$ while $1-\omega = \pi \not\equiv 0 \bmod \pi^2$].

If $v' = -1$ we can absorb the factor in Y^3 (taking $-Y$ in place of Y). Thus

$$X^3 + Y^3 = w'\pi^3 Z^3;$$

and the solution (x, y, z) of our original equation has led to the solution (X, Y, Z) of an equation of the same form. which in turn leads to a further solution, and so on.

[It's clear that the new solution is smaller in some sense than the original one, since it involves taking cube roots, so the result will follow by Fermat's 'Method of Infinite Descent'. We need to make this precise.]

Since

$$w\pi^4 Z^3 = x + y,$$

while

$$(x + y)(x + \omega y)(x + \omega^2 y) = \epsilon\pi^3 z^3,$$

it follows on taking norms that

$$\begin{aligned} 3^4 N(z)^3 &= N(x + y) \\ &\le 3^3 N(z)^3, \end{aligned}$$

Hence

$$0 < N(Z) < N(z).$$

Thus we get a strictly decreasing sequence of positive integers, which is impossible □

3. What is meant by saying that a point on the curve

$$y^2 = x^3 + ax^2 + bx + c$$

is *singular*? What are the points at infinity on this curve? Are any of them singular?

Show that there is a singular point on the curve if and only if

$$a^2b^2 + 18abc - 4a^3c - 4b^3 - 27c^2 = 0.$$

Answer.

(a) A point on the projective curve

$$F(x, y, z) = 0$$

(where $F(x, y, z)$ is a homogeneous polynomial) is said to be singular if

$$\frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = \frac{\partial F}{\partial z} = 0.$$

The given curve Γ takes the homogeneous form

$$F(x, y, z) \equiv y^2 z - x^3 - ax^2 z - bxz^2 - cz^3 = 0.$$

It follows that the point $P = (x, y) \in \Gamma$ is singular if

$$3x^2 + 2axz + bz^2 = 0,\ 2yz = 0,\ y^2 - ax^2 - 2bxz - 3cz^2 = 0.$$

If $z = 0$ then $x = 0$ from the first equation and so $y = 0$ from the third equation. This is impossible. Hence $y = 0$, and so

$$3x^2 + 2axz + bz^2 = 0,\ ax^2 + 2bxz + 3cz^2 = 0.$$

Reverting to non-homogeneous notation,

$$3x^2 + 2ax + b = 0,\ ax^2 + 2bx + 3c = 0.$$

If

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

then first equation can be written $f'(x) = 0$, while x times the first plus the second is just $3f(x) = 0$.

It follows that the point $P = (x, y)$ on Γ is singular if and only if $y = 0$ and

$$f(x) = f'(x) = 0,$$

in other words x is a double root of $f(x)$.

(b) The point $[x, y, z]$ is 'at infinity' if $z = 0$. The point $[x, y, 0]$ is on Γ if

$$x^3 = 0.$$

Thus Γ has just one point at infinity, $[0, 1, 0]$.

(c) This point is not singular, since

$$y^2 - ax^2 - 2bxz - cz^2 = y^2 \neq 0.$$

(d) *As we have seen, there is a singular point on Γ if and only if $f(x)$ has a double root, ie $f(x)$ and $f'(x)$ have a root in common.*

Two polynomials $f(x)$ and $g(x)$ have a root in common if and only if their resultant *$R(f,g)$ vanishes.*

The resultant of $f(x)$ and $f'(x)$ is

$$R(f,f') = \det \begin{pmatrix} 1 & a & b & c & 0 \\ 0 & 1 & a & b & c \\ 3 & 2a & b & 0 & 0 \\ 0 & 3 & 2a & b & 0 \\ 0 & 0 & 3 & 2a & b \end{pmatrix}.$$

Thus we have to compute this determinant. Expanding with respect to the first column,

$$\begin{aligned} R(f,f') &= \det \begin{pmatrix} 1 & a & b & c \\ 2a & b & 0 & 0 \\ 3 & 2a & b & 0 \\ 0 & 3 & 2a & b \end{pmatrix} + 3\det \begin{pmatrix} a & b & c & 0 \\ 1 & a & b & c \\ 3 & 2a & b & 0 \\ 0 & 3 & 2a & b \end{pmatrix} \\ &= 1(b^3) - a(2ab^2) + b(4a^2b - 3b^2) - c(8a^3 - 12ab) \\ &\quad +3a(-ab^2 + 4a^2c - 3bc) - 3b(-2b^2 + 6ac) + 3c(-ab + 9c) \\ &= -a^2b^2 - 18abc + 4a^3C + 4b^3 + 27c^2, \end{aligned}$$

which is just the given expression, multiplied by -1.

4. Show that there an abelian group can be defined on the elliptic curve

$$y^2 = x^3 + ax^2 + bc + c$$

such that $P + Q + R = 0$ if and only if P, Q, R are collinear.

Does this condition determine the group uniquely?

Answer.

(a) *We denote the elliptic curve by $\mathcal{E}$.*

Given $P, Q \in \mathcal{E}$ let $P * Q$ denote the point where the line PQ (or the tangent at P if $P = Q$) meets $\mathcal{E}$ again.

The binary operation $*$ on $\mathcal{E}$ is evidently commutative:

$$Q * P = P * Q.$$

Also, from the symmetry of the relation between $P, Q, P * Q$,

$$P * (P * Q) = Q.$$

Let $O = [0, 1, 0]$. This is a point of inflexion on $\mathcal{E}$, ie the tangent $z = 0$ at O meets $\mathcal{E}$ thrice at O. Thus

$$O * O = O.$$

We define the binary operation $+$ on $\mathcal{E}$ by

$$P + Q = O * (P * Q).$$

i. *The operation is commutative:*

$$Q + P = P + Q,$$

since $Q * P = P * Q$.

ii. *The element O is neutral, ie*

$$O + P = P$$

for all P. For

$$O + P = O * (O * P) = P$$

from above.

iii. *The point P has additive inverse $O * P$, since*

$$P * (O * P) = O \implies P + (O * P) = O * O = O.$$

iv. *It remains to prove that the operation is associative, ie*

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

It is sufficient to show that

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

By a cubic *in the projective plane $\mathbb{P}^2(\mathbb{Q})$ we mean any curve*

$$\begin{aligned} \Gamma : \quad & c_1x^3 + c + 2x^2y + c_3x^2z + c_4xy^2 + c_5xyz \\ & +c_6xz^2 + c_7y^3 + c_8y^2z + c_9yz^2 + c_{10}z^3 = 0 \end{aligned}$$

of degree 3.

Lemma. Suppose $P_1, \ldots, P_8$ are 8 points in the projective plane $\mathbb{P}^2(\mathbb{Q})$ such that no 6 points lie on a conic. Then there are an infinity of cubics passing through these 8 points; and all of them pass through a 9th point P_9.

To see that there are an infinity of curves, we note that each point imposes a homogeneous linear condition on $c_1, \dots, c_{10}$. Thus we have 8 homogeneous linear equations in 10 unknowns. These necessarily have an infinity of solutions (regarding scalar multiples as the same solution).
In general the vector space formed by the solutions $(c_1, \dots, c_{10})$ has dimension 2, ie the solutions form a pencil

$$\Gamma \equiv u\Gamma_1 + v\Gamma_2,$$

The cubics Γ_1, Γ_2 have the 8 points $P_1, \dots, P_8$ in common. But 2 cubics have at most 9 points in common; and if they 8 rational points in common, then they have a 9th rational point in common. In particular Γ_1, Γ_2 have a 9th point P_9 in common. This will also lie on every curve Γ in the pencil.
If the dimension of the solution space is greater than 2 then we can find a cubic curve in the pencil passing through $P_1, \dots, P_8$ and 2 further points A, B on P_1P_2 (say). But then this cubic must degenerate into the line P_1P_2 and a conic containing the other 6 points, contrary to our assumption that no 6 of the given 8 points lie on a conic.
We apply this Lemma to the configuration formed by the 10 points

$$P_1 = 0,\ P_2 = P,\ P_3 = Q,\ P_4 = R,\ P_5 = P * Q,$$
$$P_6 = P + Q,\ P_7 = Q * R,\ P_8 = Q + R,\ P_9 = (P + Q) * R,\ P_{10} = P * (Q + R).$$

We consider the curve $\mathcal{E}$, together with the 2 degenerate cubics formed by the sets of 3 lines

$$\{P_1P_5P_6, P_3P_4P_7, P_2P_8P_9\},\ \{P_1P_7P_8, P_2P_3P_5, P_4P_6P_{10}\}.$$

These 3 cubics go through the 8 points $P_1, \dots, P_8$. Hence by the Lemma they have a 9th point in common. But the first degenerate cubic meets $\mathcal{E}$ again at P_9, while the second one meets $\mathcal{E}$ again at P_{10}. It follows that $P_9 = P_{10}$, ie

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

(b) *We could choose any point of inflexion O' in place of O, giving the binary operation*

$$P \circ Q = O' * (P * Q).$$

In effect

$$P \circ Q = P + Q - O'.$$

It is readily verified that this does define an abelian group with neutral element O', since

$$P \circ O' = P + O' - O' = P.$$

The negative of P is now $-P - O'$, since

$$P \circ (-P - O') = P - P - O' - O' = -2O' = O'.$$

The associative law holds, since

$$(P \circ Q) \circ R = P + Q + R - 2O' = P + Q + R + O' = P \circ (Q \circ R).$$

This is the only way to define a group on $\mathcal{E}$ with the stated property. For if O is the neutral element of the group we must have

$$O + O + O = 0,$$

which implies that O is a point of involution. If now $-P$ is the negative of P then

$$O + P + (-P) = 0,$$

which implies that

$$-P = O * P.$$

Finally, if $P + Q = R$ then

$$P+Q+(-R) = 0 \implies -R = (P*Q) \implies R = -(P*Q) = O*(P*Q).$$

5. Find the order of the points $P = (0, 0),\ Q = (1, 1)$ on the elliptic curve

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

Determine the points $P \pm Q$.

Answer.

(a) *The point P has order 2, since the tangent at P is $x = 0$, which meets the curve again at $0 = [0, 1, 0]$.*

(b) Let the tangent at Q be

$$y = mx + d.$$

Since

$$2y\left(\frac{dy}{dx}\right) = 3x^2 + 2x - 1,$$

we have

$$m = \frac{4}{2} = 2.$$

Thus the tangent is

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

ie

$$y = 2x - 1.$$

This line meets the curve where

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

Thus if the tangent at Q meets the curve again at $R = (X, Y)$, so that $2Q + R = 0$, then

$$1 + 1 + X = m^2 - 1 = 3.$$

Hence $X = 1$ and so $Y = 1$, ie $R = Q$. Thus

$$3Q = 0,$$

and so Q has order 3.

(c) The slope of PQ is

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

Thus PQ is the line

$$y = x.$$

This meets the curve again at (X, Y), where

$$0 + 1 + X = m^2 - 1 = 0,$$

ie at $(-1, -1)$. Hence

$$P + Q = -(-1, -1) = (-1, 1).$$

Similarly, if $Q' = -Q = (1, -1)$, the slope of PQ' is

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

Thus PQ is the line

$$y = -x.$$

This meets the curve again at (X, Y), where

$$0 + 1 + X = m^2 - 1 = 0,$$

ie at $(-1, 1)$. Hence

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

6. Sketch the proof of the Nagell-Lutz Theorem, that a point $P = (x, y)$ of finite order on the elliptic curve

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + ax^2 + bx + x,$$

where $a, b, c \in \mathbb{Z}$, necessarily has integral coordinates $x, y \in \mathbb{Z}$.

Show also that for such a point either $y = 0$ or

$$y \mid 2\Delta,$$

where Δ is the discriminant of $x^3 + ax^2 + bx + c$.

Answer.

(a) *Suppose $P = [x, y, z]$ is a point of finite order on*

$$\mathcal{E}(\mathbb{Q}) : y^2 z = x^3 + ax^2 z + bxz^2 + cz^3,$$

where $a, b, c \in \mathbb{Z}$. We may suppose that $x, y, z \in \mathbb{Z}$ and that $\gcd(x, y, z) = 1$.

We want to show that $z = \pm 1$, so that $P = (x/z, y/z)$ is integral.
We prove this by showing that for each prime p that $p \nmid z$.
Suppose in fact that $p \mid z$. Then $p \mid x$, and so $p \nmid y$.
We consider the curve $\mathcal{E}(\mathbb{Q}_p)$ over the p-adic field $\mathbb{Q}_p$. If we set

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

then X and Z are p-integral, and in fact

$$p \mid X, Z.$$

We take X, Z as our coordinates, writing $P = (X, Z)$.
In these coordinates the curve takes the form

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

We can express Z as a power-series in X, by recursion:

$$Z = X^3 + aX^5 + (a^2 + b)X^7 + \cdots .$$

In particular the curve in this p-adic neighbourhood of $0 = [0, 1, 0]$ can be parametrised by $X(P) = X$.
Our argument depends on the following result.

Lemma. For each $e > 0$ let

$$\mathcal{E}_{p^e} = \{P \in \mathcal{E}(\mathbb{Q}_p) : p^e \mid X(P)\}.$$

Then $\mathcal{E}_{p^e}$ is a subgroup, and

$$P, Q \in \mathcal{E}_{p^e} \implies X(P + Q) \equiv X(P) + X(Q) \bmod p^{3e}.$$

Suppose

$$P = (X, Z),\ Q = (X', Z'),$$

where $p^e \mid X, X'$. Then $p^{3e} \mid Z, Z'$. Also

$$\begin{aligned} Z &= X^3 + aX^2Z + bXZ^2 + cZ^3, \\ Z' &= X'^3 + aX'^2Z' + bX'Z'^2 + cZ'^3. \end{aligned}$$

Subtracting,

$$\begin{aligned} Z - Z' &= X^3 - X'^3 + a(X^2Z - X'^2Z') + b(XZ^2 - X'Z'^2) + c(Z^3 - Z'^3) \\ &= (X - X')\left[X^2 + XX' + X'^2 + a(X + X')Z + bZ^2\right] \\ &\quad +(Z - Z')\left[aX'^2 + bX'(Z + Z') + c(Z^2 + ZZ' + Z'^2\right]. \end{aligned}$$

Thus

$$(1 + u)(Z - Z') = (X^2 + XX' + X'2 + v)(X - X'),$$

where $p^{2e} \mid u$ and $p^{4e} \mid v$. It follows that

$$M = \frac{Z - Z'}{X - X'} \equiv X^2 + XX' + X'^2 \bmod p^{4e}.$$

In particular

$$p^{2e} \mid M.$$

Let the line PQ be
$$Z = MX + D.$$
Since $p^e \mid X,\ p^{2e} \mid M,\ p^{3e} \mid Z$ it follows that
$$p^{3e} \mid D.$$
This line meets $\mathcal{E}$ where
$$MX + D = X^3 + aX^2(MX + D) + bX(MX + D)^2 + c(MX + D)^3.$$
Suppose the line meets $\mathcal{E}$ in P, Q, R, where $R = (X'', Z'')$. Then
$$X + X' + X'' = \frac{aD + 2bMD + 3cM^2D}{1 + aM + bM^2 + cM^3}$$
We conclude that
$$X + X' + X'' \equiv 0 \bmod p^{3e}.$$
The result follows, since
$$-(X, Z) = (-X, -Z).$$
Corollary. Every point in $\mathcal{E}_p$ except $0 = [0, 1, 0]$ is of infinite order.
For suppose P has finite order n. We may suppose n is prime; for if $n = de$ we can take dP in place of P.
It follows from the Lemma that if $p^e \,||\, X(P)$ then
$$p^e \,||\, X(P) \implies X(nP) \equiv nX(P) \bmod p^{3e}.$$
This leads to a contradiction whether $n = p$ or not.
It follows therefore that
$$P \notin \mathcal{E}_p.$$
In other words,
$$p \not| z.$$
Since this is true for all primes p,
$$z = \pm 1,$$
and so $P = (x/z, y/z)$ is integral.

(b) *Suppose $P = (x, y)$ has finite order. Then so has $2P = (X, Y)$, say. Hence $x, y, X, Y \in \mathbb{Z}$, by the first part.*

The tangent at P has slope given by

$$2y\frac{dy}{dx} = 3x^2 + 2ax + b = f'(x),$$

where

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

Thus if the tangent is

$$y = mx + d,$$

then

$$m = \frac{f'(x)}{2y}.$$

This tangent cuts $\mathcal{E}$ where

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

The roots of this are x, x, X. Thus

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

In particular $m \in \mathbb{Z}$, ie

$$2y \mid f'(x).$$

On the other hand

$$y \mid f(x)$$

since $y^2 = f(x)$. It follows that

$$y \mid \gcd(f(x), f'(x)).$$

But

$$\gcd(f(x), f'(x)) = \Delta,$$

where Δ is the discriminant of $f(x)$. Hence

$$y \mid \Delta$$

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

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

Answer. *The discriminant is given by*

$$\Delta = a^2b^2 - 4b^3 = 1 - 4 = 3.$$

Thus by the Nagell-Lutz theorem, if $P = (x, y)$ *is a point of finite order then* $x, y \in \mathbb{Z}$ *and* $y = 0$ *or* $y \mid \Delta$. *In other words,*

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

If $y = 0$ *then* $x = 0$ *or* $x^2 - x + 1 = 0$. *The last equation has no rational solution. Thus there is just one point of order 2, namely* $(0, 0)$.

If $y = \pm 1$ *then*

$$x^3 - x^2 + x - 1 = 0.$$

If this has a rational root it must be integral, and must divide 1. In other words it must be ± 1. *(If an equation*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \quad (a_1, \ldots, a_n \in \mathbb{Z})$$

has a rational root then it must be integral, and must divide a_n.*) By inspection* $x = 1$ *satisfies the equation but not* $x = -1$. *Thus we get 2 points* $(1, \pm 1)$ *on the curve.*

If $y = \pm 3$ *then*

$$x^3 - x^2 + x - 9 = 0.$$

As before, if this has a rational root then it is integral, and divides 9, *ie it is* $\pm 1, \pm 3, \pm 9$. *By inspection none of these satisfies the equation.*

We conclude that the torsion group F *of the curve has at most the 4 elements*

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

The slope at $P = (1, 1)$ *is given by*

$$2y \frac{dy}{dx} = 3x^2 - 2x + 1,$$

ie

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

Thus the tangent at P *is*

$$y = x.$$

This meets the curve again at $(0, 0)$. *Hence*

$$2(1, 1) + (0, 0) = 0,$$

ie

$$2(1,1) = -(0,0) = (0,0).$$

Thus the point $(1,1)$ *is of order 4, since* $(0,0)$ *is of order 2.*

It follows that

$$F = \mathbb{Z}/(4);$$

and in particular the point $(1,-1)$ *must be of order 4, with*

$$2(1,-1) = (0,0).$$

8. Determine the groups of the elliptic curve

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

over the finite fields $\mathbf{GF}(3)$, $\mathbf{GF}(5)$ and $\mathbf{GF}(7)$.

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

Answer.

GF(3) *The quadratic residues modulo 3 are:*

$$0, 1.$$

The values of x *for which* $x^3 + x$ *is in this set are*

$$x = 0, 2.$$

Hence the points on the curve are:

$$0 = [0,1,0], (0,0), (2,1), (2,2).$$

There is just one point of order 2, namely $(0,0)$*. (A point has order 2 if and only if* $y = 0$*.)*

The only groups of order 4 are $\mathbb{Z}/(4)$ *and* $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$*. The latter has 3 elements of order 2. Hence*

$$\mathcal{E}(\mathbf{GF}(3)) = \mathbb{Z}/(4).$$

GF(5) *The quadratic residues modulo 5 are:*

$$0, 1, 4.$$

The values of x *for which* $x^3 + x$ *is in this set are*

$$x = 0, 2, 3.$$

Hence the points on the curve are:

$$0 = [0, 1, 0], (0, 0), (2, 0), (3, 0).$$

There are 3 points of order 2. Hence

$$\mathcal{E}(\mathbf{GF}(3)) = \mathbb{Z}/(2) \oplus \mathbb{Z}/(2).$$

GF(7) *The quadratic residues modulo p are:*

$$0, 1, 2, 4.$$

The values of x for which $x^3 + x$ is in this set are

$$x = 0, 1, 3, 5.$$

Hence the points on the curve are:

$$0 = [0, 1, 0], (0, 0), (1, 3), (1, 4), (3, 3), (3, 4), (5, 2), (5, 5).$$

There is just one point of order 2, namely $(0, 0)$.
The only groups of order 8 are $\mathbb{Z}/(8)$, $\mathbb{Z}/(4) \oplus \mathbb{Z}/(2)$ and $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$. These have 1, 3 and 7 elements of order 2. Hence

$$\mathcal{E}(\mathbf{GF}(7)) = \mathbb{Z}/(8).$$

Let F be the group of points of finite order on $\mathcal{E}(Q)$. Then for each 'good' prime p, reduction modulo p defines an injective homomorphism

$$\Phi : F \to \mathcal{E}(\mathbf{GF}(p)).$$

In the present case, this means that F is isomorphic to subgroups of $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$, $\mathbb{Z}/(4)$ and $\mathbb{Z}/(8)$. We know that $\mathcal{E}(\mathbb{Q})$ contains just one element of order 2, namely $(0, 0)$. It follows that

$$F = \{0, (0, 0)\} = \mathbf{GF}(2).$$

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

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

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

   Answer.

(a) *The Weierstrass elliptic function $\wp(z) \equiv \wp_L(z)$ with respect to the lattice $L = \langle \omega_1, \omega_2 \rangle$ is defined by*

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

This function is elliptic with respect to L, ie

$$\wp(z+\omega) = \wp(z)$$

for each $\omega \in L$.

(b) *In the neighbourhood of $z = 0$,*

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + \sum_{\omega \neq 0} \frac{1}{\omega^2} \left(\frac{1}{(1 - z/\omega)^2} - 1 \right) \\ &= \frac{1}{z^2} + \sum_{\omega \neq 0} \frac{1}{\omega^2} \left(2z\frac{1}{\omega} + 3z^2 \frac{1}{\omega^2} + \cdots \right) \\ &= \frac{1}{z^2} + 3g_2 z^2 + 5g_3 z^4 + O(z^6), \end{aligned}$$

where

$$g_r = \sum_{\omega \in L,\, \omega \neq 0} \frac{1}{\omega^{2r}}.$$

(The terms with odd powers of z vanish since

$$\sum \frac{1}{\omega^{2r+1}} = 0,$$

as the terms in ω and $-\omega$ cancel out.)

We see in particular that $\wp(z)$ is an even function of z. It follows that $\wp'(z)$ is an odd function, and so $\wp'(z)^2$ is again an even function.

We have

$$\wp'(z) = -\frac{2}{z^3} + 6g_2 z + 20 g_3 z^3 + O(z^5).$$

Hence

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24 g_2}{z^2} - 80 g_3 + O(z^2).$$

It is clear that we can find constants A, B such that

$$F(z) \equiv \wp'(z)^2 - 4\wp(z)^3 + A\wp(z) + B = O(z^2).$$

Since $F(z)$ is an elliptic function with no poles, it will follow that $F(z) \equiv 0$, ie

$$\varphi'(z)^2 = 4\varphi(z)^3 - A\varphi(z) - B.$$

We have

$$\varphi(z)^3 = \frac{1}{z^6} + \frac{9g_2}{z^2} + 15g_3 + O(z^2).$$

Thus

$$\varphi'(z)^2 - 4\varphi(z)^3 = -\frac{60g_2}{z^2} - 140g_3 + O(z^2).$$

Hence

$$\varphi'(z)^2 - 4\varphi(z)^3 + 60g_2\varphi(z) + 140g_3 = O(z^2).$$

Since this is an elliptic function without any poles, and vanishing at $z = 0$, it must vanish identically, ie

$$\varphi'(z)^2 = 4\varphi(z)^3 - 60g_2\varphi(z) - 140g_3,$$

which is the sought-for functional equation.

(c) *Suppose $f(z)$ is elliptic with respect to L and even. Let its zeroes in the fundamental parallelogram*

$$\Delta = \{x\omega_1 + y\omega_2 : 0 \le x, y < 1\}$$

be $a_1, \ldots, a_r$, and let its poles in Δ be $b_1, \ldots, b_s$.
In fact $r = s$; for

$$\frac{1}{2\pi} \int_\Delta \frac{f'(z)}{f(z)} = r - s = 0,$$

since the contributions to the integral from opposite sides of the parallelogram cancel out.
Furthermore, since $f(z)$ is even, if a is a zero then so is $-a \bmod L$; and similarly if b is a pole then so is $-b \bmod L$. Thus the zeroes and poles divide into pairs modulo L, say

$$\pm a_1, \pm a_2, \ldots,$$

This is true even for those zeroes and poles for which $-a \equiv a \bmod L$, ie $2a \in L$ For if $f(z)$ is even then $f'(z)$ is odd. Hence

$$f'(a) = f'(-a) = -f'(a) \implies f'(a) = 0$$

if $2a \in L$. Thus if a is a root of $f(z)$ then it is a double root. In fact the same argument shows that all the odd derivatives of $f(z)$ vanish at a:

$$f'(a) = f'''(a) = \cdots = 0.$$

Thus if $f(z)$ vanishes at a it has a zero there of even order.

The same is true of poles, as may be seen by considering $1/f(z)$ in place of $f(z)$, since $1/f(z)$ has zeroes where $f(z)$ has poles.

Thus $f(z)$ has zeroes at $\pm a_1, \dots, \pm a_{r'}$, and poles at $\pm b_1, \dots, \pm b_{r'}$.

But the function $\wp(z) - \wp(a)$ has a double pole at each point of L. Hence it has just 2 zeroes in the fundamental parallelogram. These must be $\pm a \bmod L$.

It follows that the function

$$F(z) = \frac{(\wp(z) - \wp(b_1)) \cdots (\wp(z) - \wp(b_{r'}))}{(\wp(z) - \wp(a_1)) \cdots (\wp(z) - \wp(a_{r'}))} f(z)$$

has no poles or zeroes, and so is constant. In other words

$$f(z) = C \frac{(\wp(z) - \wp(a_1)) \cdots (\wp(z) - \wp(a_{r'}))}{(\wp(z) - \wp(b_1)) \cdots (\wp(z) - \wp(b_{r'}))}$$

is a rational function of $\wp(z)$.

(d) *Consider the function $\wp_{2L}(2z)$. This has double poles at the points of L. In the neighbourhood of $z = 0$*

$$\wp_{2L}(2z) = \frac{1}{4z^2} + O(z^2).$$

It follows that

$$\wp_{2L}(2z) - \frac{1}{4}\wp_L(z)$$

has no poles, and is $O(z^2)$ in the neighbourhood of). Hence

$$\wp_{2L}(2z) = \frac{1}{4}\wp_L(z),$$

and so

$$\wp_{2L}(z) = \frac{1}{4}\wp_L(z/2).$$

10. State Mordell's Theorem on the group of rational points on an elliptic curve, and sketch the proof.

Answer. Mordell's Theorem states that the abelian group formed by the rational points on the curve

$$\mathcal{E} : y^2 = x^3 + ax^2 + bx + c$$

is finitely-generated.

To prove this we show first that $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$ is finite.

For this we have to go to an algebraic number field K containing the roots α, β, γ of

$$f(x) = x^3 + ax^2 + bx + c,$$

and show that $\mathcal{E}(K)/\mathcal{E}(K)$ is finite.

Since $\mathcal{E}(\mathbb{Q}) \subset \mathcal{E}(K)$, it will follow that $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$ is finite.

The proof is based on the following Lemmas.

Lemma. The point $P = (x, y) \in \mathcal{E}(\mathbb{Q})$ is of the form $P = 2Q$ with $Q \in \mathcal{E}(\mathbb{Q})$ if and only if $x - \alpha, x - \beta, x - \gamma$ are all perfect squares:

$$x - \alpha = \alpha'^2,\ x - \beta = \beta'^2,\ x - \gamma = \gamma'^2.$$

Lemma. Suppose $c = 0$. Then the map

$$\Phi : \mathcal{E}(\mathbb{Q}) \to K^\times/(K^\times)^2$$

under which

$$P \mapsto \begin{cases} 1 & \text{if } P = 0 = [0, 1, 0] \\ b & \text{if } P = (0, 0) \\ x & \text{if } P = (x, y) \neq (0, 0) \end{cases}$$

is a homomorphism.

For each of the roots $\theta = \alpha, \beta, \gamma$ we obtain a corresponding homomorphism

$$\Phi_\theta : \mathcal{E}(\mathbb{Q}) \to K^\times/(K^\times)^2$$

by making the coordinate-change $x \mapsto x - \theta$ (bringing $(\theta, 0)$ to $(0, 0)$).

Lemma. $P = 2Q$ if and only if

$$P \in \ker \Theta_\alpha \cap \ker \Theta_\beta \cap \ker \Theta_\gamma.$$

Lemma. $\mathcal{E}/2\mathcal{E}$ is finite if and only if $\mathrm{im}\Theta_\alpha$, $\mathrm{im}\Theta_\beta$, $\mathrm{im}\Theta_\gamma$ are all finite.

To prove $\mathrm{im}\Theta_\alpha$ *finite, we may again suppose $c = 0$, so that the curve takes the form*

$$\mathcal{E} : y^2 = x(x^2 + ax + b).$$

Lemma. Suppose $(x, y) \in \mathcal{E}(K)$; and suppose $\mathfrak{p}$ is a prime ideal. Then

$$\mathfrak{p}^{2e} \mid\mid x$$

(ie $\mathfrak{p}$ occurs to an even power in x) unless

$$\mathfrak{p} \mid \Delta.$$

Corollary. Let $S \subset K^\times$ be the subgroup

$$S = \{x \in K^\times : \langle x \rangle = a^2\}.$$

Then

$$(K^\times)^2 \subset S;$$

and we can find a finite number of points $P_1, \ldots, P_d \in \mathcal{E}$ such that for any point $P \in \mathcal{E}$,

$$\operatorname{im}(P - P_i) \in S/(K^\times)^2$$

for some i.

This reduces the proof that $\mathcal{E}/2\mathcal{E}$ is finite to the following result from algebraic number theory.

Lemma. The quotient-group $S/(K^\times)^2$ is finite.

This follows from 2 standard theorems: firstly, the finiteness of the ideal class group; and secondly, Dirichlet's Units Theorem which asserts that the group of units in a number field K is finitely-generated.

We have shown therefore that $\mathcal{E}(K)/2\mathcal{E}(K)$ is finite, from which it follows that $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(Q)$ is finite. It remains to deduce that $\mathcal{E}(\mathbb{Q})$ is finitely-generated.

Let $P_1, \ldots, P_r$ be representatives of $\mathcal{E}/2\mathcal{E}$ (where $\mathcal{E} = \mathcal{E}(\mathbb{Q})$). Suppose $P \in \mathcal{E}$. Then

$$P - P_i \in 2\mathcal{E}$$

for some i, say

$$P - P_{i_0} = 2P_1.$$

Similarly

$$\begin{aligned} P_1 - P_{i_1} &= 2P_2, \\ P_2 - P_{i_2} &= 2P_3, \end{aligned}$$

and so on.

We want to show that this recursion

$$P \mapsto P_1 \mapsto P_2 \mapsto \cdots$$

represents in some sense an 'infinite descent'. To this end we define the height *of a point $P \in \mathcal{E}$ as follows.*

Suppose $x \in \mathbb{Q}$. Let $x = m/n$ in its lowest terms. Then we set

$$H(x) = \max(|m|, |n|),\ h(x) = \log H(x).$$

If now $P = (x, y) \in \mathcal{E}$ we set

$$H(P = H(x),\ h(P) = h(x).$$

Mordell's Theorem is now a consequence of the following 3 Lemmas.

Lemma. There are only a finite number of points $P \in \mathcal{E}$ such that

$$h(P) \le C$$

for any constant C.

Lemma. There is a constant C such that

$$h(2P) \ge 4h(P) - C$$

for all $P \in \mathcal{E}$.

Lemma. For any point $P_0 \in \mathcal{E}$ there is a constant $C = C(P_0)$ such that

$$h(P - P_0) \le 2h(P) + C$$

for all $P \in \mathcal{E}$.