Course 428 — Sample Paper

Timothy Murphy

13 April 2004

Attempt 7 questions. All carry the same mark. The word 'curve' always means projective curve.

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

   Find the sum $P+Q$ of the points $P=(0,1),\ Q=(1,2)$ on the curve
   $$y^2 = x^3 + 2x + 1$$
   over the rationals $\mathbb{Q}$. What is $2P$?

   Answer: *Let $\mathcal{E}$ be the elliptic curve. We choose any point $O \in \mathcal{E}$ as the zero point.*

   Suppose $P, Q \in \mathcal{E}$, the elliptic curve in question. The line PQ meets $\mathcal{E}$ in a third point R (which may coincice with P or Q). We set
   $$P * Q = R.$$

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

   Now we set
   $$P + Q = O * (P * Q).$$

   Suppose the elliptic curve is given in the standard Weierstrass form
   $$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6.$$

   More precisely, $\mathcal{E}$ is the projective curve
   $$Y^2Z + c_1XYZ + c_3YZ^2 = X^3 + c_2X^2Z + c_4XZ^2 + c_6Z^3.$$

   In this case we normally take $O = [0,1,0]$. If now
   $$R = P * Q = (x, y)$$
   then
   $$P + Q = (x, -y).$$

Now consider the points

$$P = (0, 1), \ Q = (1, 2)$$

on the elliptic curve

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

Suppose PQ is the line

$$y = mx + c.$$

Then

$$m = \frac{2-1}{1-0} = 1.$$

Thus the line is

$$y - 1 = x,$$

ie

$$y = x + 1.$$

This line meets the curve where

$$(mx + c)^2 = x^3 + 2x + 1.$$

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

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

ie

$$x_2 = 0.$$

Hence

$$y_2 = x_2 + 1 = 1.$$

Thus

$$P * Q = (0, 1) = P,$$

and so

$$P + Q = (0, -1).$$

Since the line PQ meets the curve again at P, this line is the tangent at P. Hence

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

and so

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

2. Show that all cubics through 8 given points in general position in the plane pass through a 9th point.

   Hence or otherwise show that addition on an elliptic curve is associative.

   Answer:

   (a) *Let the points be P_i $(i = 1-10)$. A cubic curve Γ has 10 coefficients:*

   $$c_1X^3+c_2X^2Y+c_3X^2Z+C_4XY^2+C_5XYZ+C_6XZ^2+c_7Y^3+c_8Y^2Z+c_9YZ^2+C_{10}Z^3 = 0.$$

   The requirement that Γ passes through P_i gives 8 homogeneous linear conditions on these 10 coefficients. The solution space has dimension $\geq 10-8=2$. In other words the cubics form a pencil of homogeneous dimension ≥ 1.

   We may suppose that no 4 of the points are collinear, and that the points do not all lie on a conic.

   We claim this in this case the dimension must be exactly 1. For suppose it is ≥ 2. Then we can find a cubic in the pencil passing through any further 2 points. Let us choose 2 points U, V on the line P_7P_8. Then the line $\ell = P_7P_8UV$ must lie entirly in the cubic, which must therefore split into

   $$\Gamma = \ell C,$$

   where C is a conic. Thus the 6 points $P_i(i = 1-6)$ must lie on a conic.

   By the same argument, any 6 of the 8 given points must lie on a conic.

   But there is only one conic through 5 points $Q_j(j = 1-5)$, no 4 of which are collinear.

   For suppose first that three of the points are collinear, say

   $$m = Q_1Q_2Q_3.$$

   Then the only conic through the 5 points is

   $$C = mn,$$

   where

   $$n = Q_4Q_5.$$

   Now suppose no three of the points are collinear; and suppose there are two conics through the 5 points. Then the conics through the points form a pencil of projective dimension ≥ 1, and we can find a conic in the pencil through any further point W.

Choose W on $m = Q_1Q_2$. Then the conic must degenerate into two lines,

$$C = mn,$$

and Q_3, Q_4, Q_5 must lie on the line n, contrary to hypothesis.

Thus, returning to the 8 points P_i, there is a unique conic through P_1, P_2, P_3, P_4, P_5. But as we have seen, this conic must pass through P_6; and by the same argument it must also pass through P_7 and P_8. Hence all 8 points lie on a conic, contrary to hypothesis.

Therefore the pencil is of dimension 1; and if Γ_1, Γ_2 are two curves in the pencil then the general curve in the pencil is

$$\Gamma = \lambda\Gamma_1 + \mu\Gamma_2.$$

The curves Γ_1, Γ_2 meet in the 8 points P_i. Let the curves have equations

$$F_1(X, Y, Z) = 0, \ F_2(X, Y, Z) = 0.$$

We can regard these as cubics in Z with coefficients in X, Y. If we form the resultant of the two cubics we obtain a homogeneous polynomial $R(X, Y)$ of degree 9 in X, Y, whose vanishing is a condition for the two cubics to have a root in common.

The 8 points P_i will provide 8 roots for this equation. By considering the sum of the roots, it follows that there is a 9th root in the field k we are working over. Thus the two cubics meet in a 9th point $P_9 = [X_9, Y_9, Z_9]$. Moreover, by the argument above $Y_9/X_9 \in k$; and similarly $Z_9/X_9 \in k$. Hence P_9 is defined over k.

(b) *Suppose $P, Q, R \in \mathcal{E}$. We have to show that*

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

By definition,

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

where $P * Q$ is the point where PQ meets the curve again, and O is the point chosen as zero point. Thus we have to show that

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

Since

$$U * V = U * W \iff V = W$$

it is sufficient to show that

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

ie

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

Note that

$$U * V = W \iff V * W = U.$$

Thus if we set

$$P * Q = X,\ Q * R = Y$$

then

$$P = Q * X,\ R = Q * Y,$$

and our equation becomes

$$(O * X) * (Q * Y) = (Q * X) * (O * Y),$$

ie (since $V * U = U * V$*)*

$$(O * X) * (Y * Q) = (O * Y) * (X * Q).$$

Thus the result will follow if we show that

$$(P * Q) * (R * S) = (P * R) * (Q * S) \qquad (\dagger)$$

for any 4 points $P, Q, R, S \in \mathcal{E}$.
[Conversely, if the operation $+$ *is associative then it defines an abelian group structure on* $\mathcal{E}$*, with*

$$-P = O * P$$

and

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

In this case,

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

Thus the identity $(\dagger)$ *holds if and only if the operation is associative.]*
Now let us apply the 8-point theorem to the points,

$$P, Q, R, S, U = P * Q, V = R * S, W = P * R, X = Q * S.$$

Let us define lines as follows:

$$\ell = PQU, m = RSV, n = WX,$$
$$f = PRW, g = QSX, h = UV.$$

Then the degenerate cubics

$$\ell mn,\ fgh$$

pass through the 8 points, and so must have a 9th point in common. This 9th point must be where the line n meet $\mathcal{E}$ again, ie the point

$$W * X = (P * R) * (Q * S).$$

But by the same argument, it must be the point where the line h meet $\mathcal{E}$ again, ie the point

$$U * V = (P * Q) * (R * S).$$

We conclude that

$$(P * Q) * (R * S) = (P * R) * (Q * S),$$

as required.

[This argument assumes, on the face of it, that the 9 points arising in this was are distinct. There are several ways of extending the reult to cover the special cases when some of the points coincide.

Thus we could extend the definition of the pencil of cubics so that if eg $P = Q$ then our pencil consisted of the cubics which had the same tangent at P as $\mathcal{E}$.

Alternatively, we could justify the general result when $k = \mathbb{C}$, say, by continuity. The result must then be an algebraic identity which will hold over all fields.

Thirdly, we could appeal to the "Irrelevance of Algebraic Inequalities", which states that if an identity $f(x_1, \ldots, x_n) = 0$ holds subject to an inequailty $g(x_1, \ldots, x_n) \neq 0$ then it must hold in all cases.

But the question is long enough as it is, and I think one can assume that no examiner would expect the student to go into this issue.]

3. Find the order of the point $P = (0, 0)$ on the elliptic curve

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

Answer: *We have*

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

Thus the slope at (x, y) is

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

The tangent

$$y = mx + c$$

at (x, y) *meets the curve where*

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

If this meets the curve again at (x_2, y_2) *then*

$$2x + x_2 = m^2.$$

In particular the slope at P *is*

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

so the tangent

$$y = -x$$

meets the curve again where

$$x_2 = 1,$$

ie at

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

Hence

$$Q = -2P.$$

The slope at Q *is*

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

Thus the tangent at Q *is*

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

ie

$$y = -x - 2,$$

and this meets the curve again where

$$2 + x_2 = 4,$$

ie

$$x_2 = 2,$$

ie at $(2, -4)$. *Thus*

$$-2Q = R = (2, -4).$$

The slope at R *is*

$$m = \frac{3-1}{-8+1} = -\frac{2}{7}.$$

It follows that R *is of infinite order, and so therefore is* P.

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

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

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

Answer: *It is sufficient to show that*

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

for each prime p.

Let us write $\|\cdot\|$ *for* $\|\cdot\|_p$. *Note that*

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

and if this is so then the terms in y^2, x^3 *must balance, ie*

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

since otherwise y^2 *or* x^3 *would dominate [ie would have larger* p*-adic value than any other term]. Let us suppose that this is the case.*

Suppose first that $p \neq 2$. *In this case we can bring the equation to standard form*

$$\mathcal{E}(\mathbb{Q}_p) : y'^2 = x^3 + a'x^2 + b'x + c'$$

by "completing the square" on the left, with the change of coordinates

$$y' = y + c_1 x/2 + c_3/2.$$

The coefficients a', b', c' *will still be* p*-adic integers. Also* y' *will be a* p*-adic integer if and only if* y *is a* p*-adic integer. So we may assume (if* $p \neq 2$*) that the equation takes this simpler form.*

Lemma. Suppose

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

is an elliptic curve with $a, b, c \in \mathbb{Z}_p$; and suppose $P = (x, y)$ is a point on $\mathcal{E}$ of finite order. Then $x, y \in \mathbb{Z}_p$.

Remark: the result (and proof) still hold if $p = 2$. *However, the full equation cannot in general be reduced to this simpler form if* $p = 2$.

Proof. In homogeneous terms the equation takes the form

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

where

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

Since $y \neq 0$ we may take $Y = 1$, so that

$$Z = X^3 + aX^2Z + bXZ^2 + cZ^3, \qquad (*)$$

with

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

or conversely,

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

Note that

$$\begin{aligned}\|X\| &= \|x\|/\|y\| = \|x\|^{-1/2} < 1;\\ \|Z\| &= 1/\|y\| < 1.\end{aligned}$$

By repeatedly substituting for Z in the right-hand side of $(*)$ we obtain a series expansion for Z in terms of X, starting

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

Let

$$\mathcal{E}_{(p^r)} = \{P = [X, 1, Z] \in \mathcal{E}(\mathbb{Q}_p) : \|X\| \leq p^{-r}, \|Z\| < 1\}.$$

Lemma. *$\mathcal{E}_{(p^r)}$ is a subgroup of $\mathcal{E}(\mathbb{Q}_p)$. Moreover, if*

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

and

$$P_3 = P_1 + P_2 = [X_3, 1, Y_3]$$

then

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

Proof. Suppose P_1P_2 is the line

$$Z = mX + d.$$

Then
$$m = \frac{Z_2 - Z_1}{X_2 - X_1}.$$
Subtracting the equation for P_1 from that for P_2,
$$\begin{aligned}(Z_2 - Z_1) = (X_2^3 - X_1^3) + a(X_2^2 Z_2 - X_1^2 Z_1)\\ +b(X_2 Z_2^2 - X_1 Z_1^2) + c(Z_2^3 - Z_1^3).\end{aligned}$$
We can write this as
$$\begin{aligned}(Z_2 - Z_1) = (X_2^3 - X_1^3) + a(X_2^2 - X_1^2)Z_2 - aX_1^2(Z_2 - Z_1)\\ +b(X_2 - X_1)Z_2 - bX_1(Z_2^2 - Z_1^2) + c(Z_2^3 - Z_1^3).\end{aligned}$$
Hence
$$\begin{aligned}m = (X_1^2 + X_1X_2 + X_2^2) + a(X_1 + X_2)Z_2 - mX_1^2\\ +bZ_2 - bmX_1(Z_1 + Z_2) + cm(Z_1^2 + Z_1Z_2 + Z_2^2).\end{aligned}$$
Thus
$$m = \frac{U}{V},$$
where
$$\begin{aligned}U &= X_1^2 + X_1X_2 + X_2^2 + \cdots \equiv 0 \bmod p^{2r}\\ V &= 1 - X_2^2 + \cdots \equiv 1 bmod p^{2r}.\end{aligned}$$
It follows that
$$m \equiv 0 \bmod p^{2r}.$$
Hence
$$d = Z_1 + mX_1 \equiv 0 \bmod p^{3r}.$$
Suppose
$$P = [X, 1, Z] = [X/Z, 1/Z, 1] = (X/Z, 1/Z) = (x, y),$$
say. Then
$$-P = (x, -y) = (X/Z, -1/Z) = [X/Z, -1/Z, 1] = [-X, 1, -Z].$$
In other words,
$$-[X, 1, Z] = [-X, 1, -Z].$$
In particular,
$$-P_3 = [-X_3, 1, -Z_3].$$

Now $P_1, P_2, -P_3$ lie on the line $Z = mX + d$. Thus, on substituting $Z = mX + d$ in $(*)$ and equating the coefficients of X^2 and X^3,

$$\begin{aligned} X_1 + X_2 - X_3 &= -\frac{(a + 2bm + 3cm^2)d)}{1 + am + bm^2 + cm^3} \\ &\equiv 0 \bmod p^{3r}. \end{aligned}$$

In other words,

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

In particular,

$$\|X_1\|,\ \|X_2\| \le p^{-r} \implies \|X_3\| \le p^{-r}.$$

Thus

$$P_1, P_2 \in \mathcal{E}_{p^r} \implies P_1 + P_2 \in \mathcal{E}_{p^r},$$

ie $\mathcal{E}_{(p^r)}$ is a subgroup. $\square$

Lemma. *The only point of finite order in $\mathcal{E}_{(p)}$ is $P = 0$.*

Proof. It is sufficient to show that there is no point of *prime* order q. For if P is of order $q_1 \cdots q_r$ then $(q_2 \cdots q_r)P$ is of order q_1.

If $q \neq p$ this follows at once from the Lemma. For suppose $P = [X, 1, Z] \in \mathcal{E}_{(p)}$, and suppose

$$\|X\| = p^{-r}.$$

Then (writing $X(qP)$ for the X-coordinate of qP)

$$\begin{aligned} X(qP) &\equiv qX \bmod p^{3r} \\ &\not\equiv 0 \bmod p^r. \end{aligned}$$

The same argument also holds if $q = p$, since

$$X(pP) \equiv pX \bmod p^{3r},$$

while

$$\|pX\| = p^{-(r+1)}.$$

Since $r + 1 < 3r$ it follows that

$$X(pP) \not\equiv 0 \bmod p^{r+1}.$$

$\square$

We have reduced the problem to the case $p = 2$, where we have to return to the original equation.

The argument is similar, but more complicated.

Lemma. *Suppose*

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

is an elliptic curve with $A, B, a, b, c \in \mathbb{Z}_p$. Then

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

is a subgroup of $\mathcal{E}$ for each $r \ge 1$. Moreover, if

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

and

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

then

$$X_3 \equiv X_1 + X_2 \bmod p^{2r}.$$

Proof. As before, on passing to (X, Z) coordinates we can express Z as a power-series in X, though now there is a term in X^4:

$$Z = X^3 - c_1 X^4 + O(X^5).$$

The computation of m and d for the line

$$P_1 P_2 : Z = mX + d$$

is a little more complicated, but as before

$$\|m\| \le p^{-2r}, \quad \|d\| \le p^{-3r}.$$

[In detail, the equation of the curve is now

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

Subtracting the equation for P_1 from that for P_2,

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

We can write this as

$$(Z_2 - Z_1)\left(1 + AX_2 + B(Z_2 + Z_1) - aX_2^2 - b(X_2(Z_2 + Z_1) - c(Z_2^2 + Z_2 Z_1 + Z_1^2)\right) =$$
$$(X_2 - X_1)\left(-AZ_1 + (X_2^2 + X_2 X_1 + X_1^2) + aZ_1(X_2 + X_1) + bZ_1^2\right).$$

Thus

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

where

$$U \equiv 0 \bmod p^{2r}, \quad V \equiv 1 \bmod p^{2r};$$

and so

$$m \equiv 0 \bmod p^{2r}, \quad d \equiv 0 \bmod p^{3r},$$

as before.]

Now suppose

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

Then P_1, P_2, P_3' lie on the line $Z = mX + d$. This line meets the curve where

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

Thus

$$\begin{aligned} X_1 + X_2 + X_3' &= \frac{Am + Bm^2 - (a + 2bm + 3cm^2)d}{1 + am + bm^2 + cm^3} \\ &\equiv 0 \bmod p^{2r}. \end{aligned}$$

[Note that the term Am means that we only have equivalence modp^{2r} rather than modp^{3r} as before.] Hence

$$X_3' \equiv -(X_1 + X_2) \bmod p^{2r}.$$

In particular,

$$\begin{aligned} \|X_1\|, \|X_2\| \equiv 0 \bmod p^r &\implies \|X_3'\| \equiv 0 \bmod p^r \\ &\implies \|Z_3'\| \equiv 0 \bmod p^{3r} \end{aligned}$$

since $Z_3 = mX_3 + d$.

The formula for $-[X, 1, Z]$ is a little more complicated than before. We know that $-(x_0, y_0) = (x_0, y_0')$ is the point where the line $x = x_0$ meets the curve again. Considering the given equation as a quadratic in y, we see that

$$y_0 + y_0' = -(c_1 x + c_3).$$

Thus

$$-(x, y) = (x, -(y + c_1 x + c_3));$$

or in (X, Z)-coordinates,

$$\begin{aligned}
-[X, 1, Z] &= -(X/Z, 1/Z) \\
&= (X/Z, -(1/Z + c_1 X/Z + c_3) \\
&= [X, -(1 + c_1 X + c_3 Z), Z] \\
&= \left[-\frac{X}{1 + c_1 X + c_3 Z}, 1, -\frac{Z}{1 + c_1 X + c_3 Z}\right].
\end{aligned}$$

In particular,

$$\begin{aligned}
X_3' &= -\frac{X_3}{1 + c_1 X_3 + c_3 Z_3} \\
&= -X_3 + c_1 X_3^2 + \cdots \\
&\equiv -X_3 \bmod p^{2r}.
\end{aligned}$$

Thus

$$X_3 \equiv X_1 + X_2 \bmod p^{2r}.$$

$\square$

If $r \geq 2$ then

$$X_3 \equiv X_1 + X_2 \bmod p^{r+2};$$

and our argument in the simpler case above yields the following result.

Lemma. *Suppose*

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

where $A, B, a, b, c \in \mathbb{Z}_p$. Then the only point in $\mathcal{E}_{(p^2)}$ of finite order is $P = 0$.

Finally, suppose $p = 2$; and suppose $P = [X, 1, Z] \in \mathcal{E}_{(2)}$ is of finite order. As before, we may assume that P is of prime order q. Let

$$\|X\|_2 = 2^{-r}.$$

If q is odd then our previous argument holds, since

$$X(qP) \equiv qX \bmod 2^{2r}$$

and

$$\|qX\|_2 = \|X\| = 2^{-r}.$$

Our previous argument also holds if $q = 2$ and $r \geq 2$, since in that case

$$X(2P) \equiv 2X \bmod 2^{2r}$$

and

$$\|2X\| = 2^{-r+1} > 2^{-2r}.$$

We are left with the case $q = 2,\ r = 1$. In this case either $2P = 0$ or else

$$2P \in \mathcal{E}_{(2^2)},$$

in which case it follows from our previous argument that 2P is not of finite order. $\square$

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

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

Answer: *By Nagell-Lütz, if $P = (x, y)$ is of finite order then $x, y \in \mathbb{Z}$ and either $y = 0$ or*

$$y^2 \mid D,$$

where

$$D = -(4b^3 + 27c^2) = 27 \cdot 17^2,$$

Thus

$$y = 0 \text{ or } y \mid 3 \cdot 17.$$

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

If $17 \mid y$ then

$$\begin{aligned} 17 \mid x^3 &\implies 17 \mid x \\ &\implies 17 \mid y^2 \\ &\implies 17^2 \mid y^2 \\ &\implies 17^2 \mid 17, \end{aligned}$$

which is absurd.

Hence

$$y = \{\pm 1, \pm 3\}.$$

If $y = \pm 1$ then

$$x^3 = 16,$$

which has no integral solution.

If $y = \pm 3$ then

$$x^3 = -8,$$

giving $x = -2$, ie the points $(-2, \pm 3)$. Let $P = (2, 3)$, so the points are $\pm P$.

It remains to determine if $\pm P$ are of finite or infinite order.

The slope at (x, y) is

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

If the tangent

$$y = mx + c$$

meets the curve again at (x_2, y_2) then x, x, x_2 are the roots of

$$(mx + c)^2 = x^3 + 17.$$

Thus

$$2x + x_2 = m^2.$$

In particular the slope at $P = (-2, 3)$ is

$$m = 126 = 2,$$

so the tangent is

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

ie

$$y = 2x + 7;$$

and this meets the curve again where

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

ie

$$x_2 = 8.$$

6. Show that the elliptic curve

$$E : y^2 + xy = x^3 - x^2 - 2x - 1$$

has good reduction modulo 2 and 5; and determine the groups $\mathcal{E}(\mathbb{F}_2)$ and $\mathcal{E}(\mathbb{F}_5)$.

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

Answer: *The curve takes homogeneous form*

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

At a singular point,

$$\begin{aligned} \partial F/partialX &= YZ - 3X^2 - 2XZ - 2Z^2 = 0, \\ \partial F/partialY &= 2YZ + XZ = 0, \\ \partial F/partialZ &= Y^2 + XY - X^2 - 4XZ - 3Z^2 = 0. \end{aligned}$$

(a) *In characteristic 2, the second equation gives*

$$XZ = 0 \implies X = 0 \text{ or } Z = 0.$$

If $Z = 0$ the first equation gives $X = 0$, and then the third equation gives $Y = 0$. Thus $X = Y = Z = 0$, which is impossible.
If $X = 0$ then the first equation gives

$$YZ = 0 \implies Y = 0 \text{ or } Z = 0.$$

We have excluded $Z = 0$, so

$$X = Y = 0 \implies Z = 0$$

from the third equation, so again $X = Y = Z = 0$, which is impossible.
We conclude that there is no singular point, ie the reduction at 2 is good.

(b) *In characteristic 5, the second equation gives*

$$Z(2Y + X) = 0 \implies Z = 0 \text{ or } X = -2Y.$$

If $Z = 0$, then as before the first equation gives $X = 0$, and then the third gives $Y = 0$.
Thus $X = -2Y \implies Y = 2X$ (as $-1/2 = 4/2 = 2$), and the first equation gives

$$2X^2 = 2Z^2 \implies X = \pm Z.$$

The third equation now gives

$$(4 + 2 - 1 \mp 4 - 3)X^2 = 0 \implies X = 0.$$

Thus $X = Y = Z = 0$, which is impossible.
We conclude that the curve is non-singular, ie the reduction at 5 is good.

[Alternatively, one could bring the curve to reduced form since the characteristic is neither 2 nor 3. Thus the equation can be written

$$y^2 - 4xy = x^3 - x^2 - 2x - 1,$$

ie

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

Writing y for $y - 2x$, and continuing the reduction,

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

ie

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

Hence the discriminant

$$D \bmod 5 = -27 \cdot (-2)^2 \neq 0,$$

ie 5 is a good prime.]

In any characteristic, the only point on the line at infinity $Z = 0$ is $[0, 1, 0]$.

(a) *In characteristic 2 there are just 4 finite points:* $(0, 0), (1, 0), (0, 1), (1, 1)$. *Of these,* $(0, 1)$ *and* $(1, 1)$ *lie on the curve. Thus*

$$\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(3).$$

(b) *In characteristic 5 we can write the equation*

$$y^2 - 4xy = x^3 - x^2 - 2x - 1,$$

ie

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

Setting $y' = y - 2x$,

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

ie

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

where $x' = x + 1$.

Dropping the $'s$*, we have to determine the group on the curve*

$$\mathcal{E}(\mathbb{F}_5) : y^2 = x^3 - 2.$$

The quadratic residues $\bmod 5$ *are:* $0, 1, 4$*, ie* $0, \pm 1$*. We have the following table.*

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

With $O = [0, 1, 0]$,

$$\|\mathcal{E}(\mathbb{F}_5)\| = 6.$$

It follows that

$$\mathcal{E}(\mathbb{F}_5) = \mathbb{Z}/(6).$$

If $T \subset \mathcal{E}(\mathbb{Q})$ *is the torsion subgroup, and* p *is a good prime, then the map*

$$T \to \mathcal{E}(\mathbb{F}_p)$$

is an injective homomorphism.

Thus in this case $p = 2$ *gives an injective homomorphism*

$$T \to \mathbb{Z}/(3).$$

It follows that

$$T = \{0\} \text{ or } \mathbb{Z}/(3).$$

(The prime $p = 5$ *does not give any further information.)*

7. Define a *lattice* $L \subset \mathbb{C}$. Show that the series

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

defines a function $\wp(z)$ which is periodic with respect to L.

Show also that $\wp(z)$ satisfies the functional equation

$$\wp'(z)^2 = 4\wp(z)^3 + A\wp(z) + B$$

for certain constants A, B.

Answer:

(a) *A lattice is a subgroup*

$$L = \langle \omega_1, \omega_2 \rangle$$

of the additive group $\mathbb{C}$ *generated by two non-zero complex numbers* ω_1, ω_2 *such that*

$$\omega_2/\omega_1 \notin \mathbb{R}.$$

[One could equally well define a lattice as a discrete subgroup of $\mathbb{C}$ *of rank 2. A discrete subgroup of* $\mathbb{C}$ *is isomorphic to* $\mathbb{Z}^r$ *where* $r \leq 2$*. In this subject we would normally exclude lattices of rank 0 (ie the group* $\{0\}$*) or 1 (ie the group* $\langle \omega \rangle$ *consisting of multiples of some* $\omega \in \mathbb{C}$*).]*

(b) *Let*

$$\wp(z) = \frac{1}{z^2} + \sum{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Then

i. *The series converges absolutely for any* $z \notin L$*;*
ii. *the convergence is uniform in any bounded closed region excluding lattice points, and so the series defines a merormorphic function on* $\mathbb{C}$ *with a double pole at each lattice point;*
iii. *The function is periodic with respect to* L*, ie*

$$\omega \in L \implies \wp(z + \omega) = \wp(z).$$

To prove (i), note that

$$\begin{aligned} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega(1-z/\omega)^2} - \frac{1}{\omega^2} \\ &= \omega^{-2}\left((1-z/\omega)^{-2} - 1\right) \\ &= \omega^{-2}\left(2z/\omega + 3z^2/\omega^2 + \cdots\right) \\ &= 2z/\omega^3 + 3z^2/\omega^4 + \cdots. \end{aligned}$$

If

$$\omega = m\omega_1 + n\omega_2$$

then

$$\begin{aligned} |\omega|^2 &= \omega\bar{\omega} \\ &= Q(m, n), \end{aligned}$$

where $Q(m, n)$ *is a positive-definite quadratic form. It follows that*

$$C_1(m^2 + n^2) \leq |\omega|^2 \leq C_2(m^2 + n^2)$$

for some $C_1, C_2 > 0$.
In particular
$$\left|\omega^{-r}\right| \leq C(m^2+n^2)^{-r/2}.$$
But
$$\sum{}'(m^2+n^2)^{-r/2}$$
converges for $r > 2$, *eg by comparison with*
$$\int (x^2+y^2)^{-r/2} dx\, dy.$$
It follows that
$$\sum{}' \omega^{-r}$$
converges absolutely for $r \geq 3$; *and so the series for* $\varphi(z)$ *converges absolutely for* $z \notin L$.
This argument also shows that the convergence is uniform in any bounded region where say
$$|z-\omega| \geq \epsilon > 0$$
for all $\omega \in L$.
[It is a little more difficult to prove periodicity than one might think. If one could completely separate the terms
$$\frac{1}{(z-\omega)^2} \text{ and } \frac{1}{\omega^2}$$
it would be trivial, but unfortunatele these two series do not converge.]
Suppose $z \notin L = \langle \omega_1, \omega_2 \rangle$. *We regard* z *as fixed. It is sufficient to show that*
$$\varphi(z+\omega_1) = \varphi(z).$$
Given $\epsilon > 0$ *we can find* R *such that*
$$\sum_{m^2+n^2>R^2} \left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| < \epsilon$$
and
$$\sum_{m^2+n^2>R^2} \left|\frac{1}{((z+\omega_1)-\omega)^2} - \frac{1}{\omega^2}\right| < \epsilon$$
Thus it is sufficient to consider the terms with $m^2+n^2 \leq R^2$.

But now the terms in the finite sums can be split in two. Now all the terms will cancel except for the terms

$$\frac{1}{(m\omega_1 + n\omega_2)^2}$$

when one of

$$m^2 + n^2 \text{ and } (m+1)^2 + n^2$$

is $\leq R$ *and the other is* $> R$. *But this implies that*

$$|m| \leq R + 1.$$

Hence

$$(m, n) \in A = \{(x, y) : R^2 - 3R < x^2 + y^2 < R^2 + 3R\}.$$

Since

$$\left|(m\omega_1 + n\omega_2)^2\right| \geq C(m^2 + n^2),$$

the discrepancy will be

$$< C' \sum_{(m,n)\in A} \frac{1}{m^2 + n^2}.$$

But this is

$$< C' \int_{(x,y)\in A'} \frac{dx\, dy}{x^2 + y^2}$$

where

$$A' = \{(x, y) : R^2 - 4R < x^2 + y^2 < R^2 + 4R\},$$

say. But the area of A' *is* $8\pi R$, *while the value of the integrand is always* $\geq 1/(R^2 - 4R)$. *Thus the integral is of order* $O(1/R)$ *and so* $\to 0$ *as* $R \to \infty$. *Hence the discrepancy can be ignored, and*

$$\wp(z + \omega_1) = \wp(z).$$

Similarly

$$\wp(z + \omega_2) = \wp(z),$$

and so

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

for all $\omega \in L$.

(c) Since

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left((1-z/\omega)^{-2} - 1\right)$$
$$= \frac{2z}{\omega^3} + \frac{3z^2}{\omega^4} + \frac{4z^3}{\omega^5} + \cdots,$$

in the neighbourhood of $z = 0$

$$\varphi(z) = \frac{1}{z^2} + 2G_3 z + 3G_4 z^2 + \cdots,$$

where

$$G_r = \sum{}' \frac{1}{\omega^r}$$

(for $r \geq 3$*). If* r *is odd then*

$$G_r = 0,$$

since the terms in $\pm\omega$ *cancel out. Thus*

$$\varphi(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + O(z^6).$$

Hence

$$\varphi'(z) = \frac{-2}{z^3} + 6G_4 z + 20G_6 z^3 + O(z^5),$$

and so

$$\varphi'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z_2} + O(1).$$

On the other hand,

$$\varphi(z)^3 = \frac{1}{z^6} + \frac{9G_4}{z^2} + O(1).$$

Thus

$$\varphi'(z)^2 - 4\varphi(z)^3 = -\frac{60G_4}{z^2} + O(1).$$

Hence

$$\varphi'(z)^2 - 4\varphi(z)^3 + 60G_4\varphi(z) = O(1).$$

Thus the periodic function on the left has no poles. But such a function is bounded on a fundamental parallelogram, and so on the whole of $\mathbb{C}$*. Hence it is constant, say*

$$\varphi'(z)^2 - 4\varphi(z)^3 + 60G_4\varphi(z) = B,$$

ie

$$\varphi'(z)^2 = 4\varphi(z)^3 + A\varphi(z) + B,$$

where $A = 60G_4$*.*

8. Find the rank of the curve

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

Answer: *The associated elliptic curve is*

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

The rank r of $\mathcal{E}$ is given by

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

where

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

are the auxiliary homomorphisms.

We know that

$$\{1, 5\} \subset im\chi \subset \{\pm 1, \pm 5\}.$$

If $e = -1$ then $ef = b = -5 \implies f = 5$ (working always $\mathrm{mod}\mathbb{Q}^{\times 2}$). Thus $-1 \in im\chi$ if and only if the equation

$$u^2 = -s^4 + 5t^4$$

has a solution with $\gcd(s, t) = \gcd(u, t) = 1$. This equation has the obvious solution

$$s = 1, \ t = 1, \ u = 2.$$

We conclude that $-1 \in im\chi$, and so

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

[The solution $(s, t) = (1, 1)$ corresponds to a point on the curve. To see what is, recall how the auxiliary homomorphisms are defined. Any rational point on the curve is of the form $(a/t^2, b/t^3)$, with $\gcd(a, t) = \gcd(b, t) = 1$. This lies on the curve if and only if

$$b^2 = a^3 - 5at^4 = a(a^2 - 5t^4).$$

Now

$$\gcd(a, a^2 - 5t^4) = \gcd(a, 5t^4) = \gcd(a, 5).$$

If $\gcd(a, 5) = 1$ then

$$a = \pm s^2, \quad a^2 - 5t^4 = \pm u^2,$$

and so

$$u^2 = s^4 - 5t^4 \text{ or } u^2 = -s^4 + 5t^4.$$

Conversely, the solution $(s, t, u) = (1, 1, 2)$ *of* $u^2 = -s^4 + 5t4$ *arises from the point* $(a/t^3, b/t^2) = (-1, 2)$. *The slope at this point is*

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

Thus the point is of infinite order, and the rank of $\mathcal{E}(\mathbb{Q})$ *is* ≥ 1.

However, it not necessary to show this in order to answer the question.]

Turning to $\tilde{\chi}$,

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

(since $20 \equiv 5 \bmod \mathbb{Q}^{\times 2}$*).*

If $e = -1$ *then* $ef = \tilde{b} = 20 \implies f = -20$. *Thus* $-1 \in im\tilde{\chi}$ *if and only if*

$$u^2 = -s^4 - 20t^4,$$

which is absurd. Hence $-1 \notin im\tilde{\chi}$, *and similarly* $-2, -5, -10 \notin im\tilde{\chi}$. *Thus*

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

If $e = 2$ *then* $ef = 20 \implies f = 10$. *Thus* $2 \in im\tilde{\chi}$ *if and only if the equation*

$$u^2 = 2s^4 + 10t^4$$

has a solution with $\gcd(s, t) = \gcd(u, t) = 1$. *Evidently* u *is even, say* $u = 2v$, *and*

$$2v^2 = s^4 + 5t^4.$$

Since $\gcd(s, t) = 1$, t *is odd, and so*

$$s^4 + 5t^4 \equiv 5 \text{ or } 6 \bmod 8,$$

while

$$2v^2 \equiv 0 \text{ or } 2 \bmod 8.$$

Hence $2 \notin im\tilde{\chi}$, *and so*

$$im\tilde{\chi} = \{1, 5\}.$$

We conclude that

$$2^{r+2} = 4 \cdot 2,$$

ie

$$r = 1.$$

9. Find all rational points on the curve

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

Answer: *We begin by determining the points of finite order. By Nagell-Lütz, if $P = (x, y)$ is of finite order then $x, y \in \mathbb{Z}$ and*

$$y = 0 \text{ or } y^2 \mid D,$$

where

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

Thus

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

If $y = 0$ then $x = 1$. Thus there is just one point of order 2, namely $(1, 0)$.

If $y = \pm 1$ then

$$x^3 = -2,$$

which is impossible.

Similarly, if $y = \pm 3$ then

$$x^3 = 10,$$

which is again impossible.

Hence the only points of finite order on the curve are the point $(1, 0)$, of order 2, and the zero point $O = [0, 1, 0]$.

It remains to 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 $'$s, our curve is not

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

The associated elliptic curve is

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

The rank r of $\mathcal{E}$ is given by

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

where

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

are the auxiliary homomorphisms.

We know that

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

If $e = -1$ *then* $ef = b = 3 \implies f = -3$ *(working always* $\bmod \mathbb{Q}^{\times 2}$*). Thus* $-1 \in im\chi$ *if and only if the equation*

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

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

If $3 \nmid s$ *then* $s^4 \equiv 1 \bmod 3$ *and so*

$$u^2 \equiv -1 \bmod 3$$

which is impossible.

Hence $3 \mid s$. *But then*

$$3 \mid u \implies 3^2 \mid -3t^4 \implies 3 \mid t,$$

contradicting $\gcd(s, t) = 1$. *Hence* $-1 \notin im\chi$, *and so*

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

Turning to $\tilde{\chi}$,

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

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

$$u^2 = -s^4 + 6s^2t^2 + 3t^4$$

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

As before, if $3 \nmid s$ *then* $s^4 \equiv 1 \bmod 3$ *and so*

$$u^2 \equiv -1 \bmod 3$$

which is impossible.

Hence $3 \mid s$. *But then*

$$3 \mid u \implies 3^2 \mid 3t^4 \implies 3 \mid t,$$

contradicting $\gcd(s, t) = 1$. *Hence* $-1 \notin im\tilde{\chi}$, *and so*

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

We conclude that $r = 0$, *so the only rational points on the curve are the points of finite order.*

Thus there is only one rational point on the curve, namely the point $(1, 0)$ *of order 2.*

10. Either show that the equation

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

has no solutions in non-zero integers x, y, z; or show that the equation

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

has no solutions in non-zero integers x, y, z.

Answer:

(a) *We may suppose that* $\gcd(x, y, z) = 1$, *which means that* x, y, z *are pairwise co-prime.*

We shall show that the equation

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

has no solution in integers with $xyz \neq 0$ *and* $\gcd(x, y, z) = 1$.

We use the following result on "Pythagorean triples".

Lemma. Suppose

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

where $x, y, z \in \mathbb{Z}$ and $xyz \neq 0, \gcd(x, y, z) = 1$. Then one of x, y is even, and one odd. If we suppose that y is even then

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

for some $u, v \in \mathbb{Z}$.

Applying the Lemma to $x^4 + y^4 = z^2$, *and supposing* x *is odd and* y *is even,*

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

Clearly $\gcd(u, v) = 1$. *Also* u *must be odd and* v *even, since* $x^2 \equiv 1 \bmod 4$.

So from the second equation,

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

with $\gcd(r, s) = 1$. *Hence*

$$x^2 = r^4 - 4s^4.$$

Applying the Lemma again to $x^2 + 4s^4 = r^4$,

$$r^2 = a^2 + b^2,\ 2s^2 = 2ab,$$

with $\gcd(a, b) = 1$. *Hence*

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

with $\gcd(X, Y) = 1$; *and so*

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

Thus from the solution (x, y, z) *of* $x^4 + y^4 = z^2$ *we have derived a second solution* (X, Y, r).
Moreover, this new solution is strictly smaller than the old, in the sense that

$$\begin{aligned}\max(|X|^2, |Y|^2) &< |r| \\ &\le |u| \\ &< |y|^2 \\ &\le \max(|x|^2, |y|^2).\end{aligned}$$

This leads to a contradiction, since a strictly decreasing sequence of positive integers must terminate.
Hence the equation

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

has no non-trivial solution, and the same is therefore true of

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

(b) *Let*

$$\omega = e^{2\pi/3} = \frac{-1 + \sqrt{-3}}{2};$$

and let

$$A = \mathbb{Z}[\omega].$$

For

$$\alpha = a + b\omega \in A$$

we set

$$\begin{gathered}\bar{\alpha} = a + b\omega^2, \\ N(\alpha) = \alpha\bar{\alpha} = a^2 - ab + b^2.\end{gathered}$$

Evidently

$$\begin{gathered}N(\alpha) \in \mathbb{N}, \\ N(\alpha) = 0 \iff \alpha = 0, \bar{\alpha\beta} = \bar{\alpha}\bar{\beta}, \\ N(\alpha\beta) = N(\alpha\beta).\end{gathered}$$

We say that $\alpha \in A$ *is a unit if*

$$N(\alpha) = 1.$$

It is easy to see that the only units in A *are*

$$\pm 1, \pm\omega, \pm\omega^2.$$

We shall assume the following result.

Lemma. The ring A is a unique factorisation domain.

Let

$$\pi = \sqrt{-3} = 1 + 2\omega.$$

Then π *is prime, since*

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

Suppose

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

with $\gcd(x, y, z) = 1$, $xyz \neq 0$.

If $x \equiv 1 \bmod 3$ *then*

$$\begin{aligned} x^3 &= (1 + 3u)^3 \\ &\equiv 1 \bmod 3^2. \end{aligned}$$

Similarly

$$x \equiv -1 \bmod 3 \implies x^3 \equiv -1 \bmod 3^2,$$

while

$$x \equiv 0 \bmod 3 \implies x^3 \equiv 0 \bmod 3^3.$$

Thus

$$x^3 \equiv 0, \pm 1 \bmod 3^2.$$

Since

$$\pm 1 \pm 1 \pm 1 \not\equiv 0 \bmod 9,$$

It follows that just one of x, y, z *is divisible by 3. We may suppose without loss of generality that*

$$3 \mid z,$$

ie

$$\pi^2 \mid z.$$

Thus, replacing z *by* $-z$,

$$x^3 + y^3 = \pi^6 z^3.$$

We want to show that

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

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

$$x^3 + y^3 = \epsilon \pi^6 z^3$$

has no solution with $x, y, z \in A = \mathbb{Z}[\omega]$, $xyz \neq 0$, *and with* ϵ *a unit. We may suppose that*

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

There are 3 residue classes $\bmod \pi$, *represented by* $0, \pm 1$.
Lemma. If $x \equiv \pm 1 \bmod \pi$ then

$$x^3 \equiv \pm 1 \bmod \pi^4.$$

[

Proof. If

$$x = \pm 1 + \pi u$$

then

$$\begin{aligned} x^3 &= (\pm 1 + \pi u)^3 \\ &= \pm 1 + 3\pi u \pm 3\pi^2 u^2 + \pi^3 u^3 \\ &\equiv \pm 1 - \pi^3 u + \pi^3 u^3 \bmod \pi^4 \\ &\equiv \pm 1 - \pi^3 u(u^2 - 1) \bmod \pi^4 \\ &\equiv \pm 1 \bmod \pi^4, \end{aligned}$$

since

$$u \equiv 0, \pm 1 \bmod \pi \implies u^2 - 1 \equiv 0 \bmod \pi.$$

□

]
Evidently

$$x, y \equiv \pm 1 \bmod \pi.$$

We may suppose without loss of generality that

$$x \equiv 1 \bmod \pi, \; y \equiv -1 \bmod \pi.$$

We can write the equation as

$$(x+y)(x+\omega y)(x+\omega^2 y) = \epsilon\pi^6 z^3.$$

Since $x \equiv 1,\ y \equiv -1 \bmod \pi$,

$$x + \omega y \equiv 1 - \omega \equiv 0 \bmod \pi,$$

and similarly for $x + \omega^2 y$. *Thus*

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

On the other hand, since $\gcd(x, y) = 1$,

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

It follows that one of $(x+y), (x+\omega y), (x+\omega^2 y)$ *is divisible by* π^2 *(at least), while the other two are divisible by* π *but not by* π^2. *On replacing* y *by* ωy *or* $\omega^2 y$ *we may suppose that*

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

It follows that

$$x+y = \epsilon_1\pi^4 u^3,\ x+\omega y = \epsilon_2 \pi v^3,\ x+\omega^2 y = \epsilon_3 \pi w^3,$$

where $\epsilon_1, \epsilon_2, \epsilon_3$ *are units, and* $\pi \nmid u, v$.
Now

$$(x+y) + \omega(x+\omega y) + \omega^2(x+\omega^2 y) = 0.$$

Dividing by π,

$$\epsilon_2' v^3 + \epsilon_3' w^3 = \epsilon_1' \pi^3 u^3,$$

where $\epsilon_1', \epsilon_2', \epsilon_3'$ *are units. Dividing by* ϵ_2' *and absorbing* -1 *into the cubes we may suppose that* $\epsilon_2' = 1$ *and that* $\epsilon_3' \in \{1, \omega, \omega^2\}$. *But now*

$$v^3, w^3 \equiv \pm 1 \bmod \pi^3 \implies \epsilon_3' = 1.$$

Moreover,

$$v^3 + w^3 \equiv 1 - 1 \bmod \pi^4 \implies \pi \mid u.$$

Setting $u = \pi u'$, *the equation takes the same form*

$$v^3 + w^3 = \epsilon' \pi^6 u'^3$$

as the equation we started from with v, w, u' *in place of* x, y, z
Moreover,

$$\begin{aligned} N(u) &\le N(u')^3 \\ &= N(u)^3/N(\pi)^3 \\ &= N(x+y)/N(\pi)^7 \\ &\le N(z)/N(\pi). \end{aligned}$$

This leads to a contradiction, since a strictly decreasing sequence of positive integers must terminate.