The equation $xyz = x + y + z = 1$ in integers of a quartic field

by

ANDREW BREMNER (Tempe, Az.)

1. Cassels [2] and Sansone and Cassels [4] showed that there are no rational solutions of the Diophantine equation

\[(1) \quad xyz = x + y + z = 1.\]

Small [5] studies the equation over finite fields, and Mollin et al. [3] investigate the equation over quadratic number fields, finding the finitely many such fields $K$ in which there does exist a solution for integer units $u_1, u_2, u_3$ of $K$ of the equation

$$u_1 u_2 u_3 = u_1 + u_2 + u_3.$$  

Bremner [1] has determined all cubic fields whose ring of integers contains a solution to (1).

Here, we resolve completely the question of finding all quartic number fields whose ring of integers contains a solution to (1). There are two infinite families of such fields. The result is as follows.

**Theorem 1.** Let $K$ be a quartic number field with ring of integers $\mathcal{O}_K$. Then the equation

$$xyz = x + y + z = 1$$

is solvable for $x, y, z \in \mathcal{O}_K$ in precisely the following instances:

(i) The infinite family $K = Q(\theta)$,

$$\theta^4 + (u^2 - u + 2) \theta^3 + 2 u \theta^2 + (u + 1) \theta + 1 = 0, \quad u \in \mathbb{Z}, \; u \neq 1,$$

with solution up to permutation

$$x = -\theta^3 - (u^2 - u + 2) \theta^2 - 2 u \theta - (u + 1),$$

$$(u-1) y = -\theta^3 - (u^2 - u + 1) \theta^2 + (u^2 - 3 u + 1) \theta + (u - 2),$$

$$(u-1) z = u \theta^3 + (u^3 - u^2 + 2 u - 1) \theta^2 + (u^2 + u - 1) \theta + u^2.$$  

(ii) The infinite family $K = Q(\phi)$,
\[
\phi^4 + (u^2 - u - 2) \phi^3 + 2 \phi^2 - (u + 1) \phi + 1 = 0, \quad u \in \mathbb{Z}, \ u \neq \pm 1, 3
\]

with solution up to permutation

\[
x = -\phi^3 - (u^2 - u - 2) \phi^2 - 2 \phi + (u + 1),
\]
\[(u - 1) y = -\phi^3 - (u^2 - u - 1) \phi^2 - (u^2 - u + 1) \phi + u,
\]
\[(u - 1) z = u \phi^3 + (u^3 - u^2 - 2u + 1) \phi^2 + (u^2 + u - 1) \phi - u^2.
\]

2. Let \( K \) be a number field with ring of integers \( \mathcal{O}_K \); suppose that \( x, y, z \) are units of \( \mathcal{O}_K \) satisfying (1). Since

\[
\text{Norm}_{K/Q}(x) \text{Norm}_{K/Q}(y) \text{Norm}_{K/Q}(z) = 1
\]

we may suppose, without loss of generality, that

(2) \quad \text{Norm}_{K/Q}(x) = 1.

Now

\[
x + y + 1/xy = 1
\]

so that

\[
y^2(x) + y(x^2 - x) + 1 = 0
\]

and

(3) \quad 2y = -x + 1 + x \sqrt{1 - \frac{2}{x} + \frac{1}{x^2} - \frac{4}{x^3}}.

Put

(4) \quad 1/x = X

where \( X \) is also a unit of \( \mathcal{O}_K \), with, from (2),

(5) \quad \text{Norm}_{K/Q}(X) = 1.

It follows from (3) that

\[
1 - 2X + X^2 - 4X^3 = W^2, \quad W \in \mathcal{O}_K
\]

so that \( P = (X, W) \) is a point defined over \( \mathcal{O}_K \) on the elliptic curve

(6) \quad \mathcal{E}: 1 - 2x + x^2 - 4x^3 = y^2.

Conversely, it is clear that a point \( P = (X, W) \), defined over \( \mathcal{O}_K \), on the curve (6), with \( X \) a unit of \( \mathcal{O}_K \), gives rise via the transformations (3), (4) to a unit solution \( x, y, z \) of the original equation (1).

Now the result of Cassels [2] and Sansone and Cassels [4] is equivalent to the rational rank of (6) being equal to 0. Further, a simple calculation shows that the rational torsion group on (6) is cyclic of order 3, with generator \((0, 1)\).
3. We first describe points on \( E \), given by equation (6), that are defined over a quadratic number field.

It is easy to see that if a point \( P \) on \( E \) has coordinates in a quadratic number field \( k \), then \( k \) is of type \( \mathcal{Q}(\sqrt{1-2\alpha+\alpha^2-4\alpha^3}) \), for some (non-zero) \( \alpha \in \mathcal{Q} \). For denoting the conjugate point under quadratic conjugation by \( \bar{P} \), then \( P^* = P - \bar{P} \) is reversed under conjugation, and so is of type \( P^* = (\alpha, \beta \sqrt{d}) \), with \( k = \mathcal{Q}(\sqrt{d}) \), \( \alpha, \beta \in \mathcal{Q} \). But then \( d\beta^2 = 1 - 2\alpha + \alpha^2 - 4\alpha^3 \), as required. More precisely, we have the following.

**Lemma 1.** Let \( P \in E \) with coordinates of \( P = (x_p, y_p) \) in a quadratic number field.

Then either

\[
(7) \quad x_p = t \in \mathcal{Q} - \{0\}, \quad y_p = \sqrt{1-2t+t^2-4t^3}
\]

or

\[
(8) \quad x_p^2 + t(t-1) x_p + t = 0 \quad \text{for some } t \in \mathcal{Q} - \{0\}
\]

with \( \pm y_p = (2t-1)x_p + 1 \).

**Proof.** Take the straight line \( l \) (defined over \( \mathcal{Q} \)) through \( P \) and \( \bar{P} \). Then \( l \) meets \( E \) in a third rational point \( Q \).

If \( Q = \infty \), the point at infinity, then \( l \) is of type \( x - x_p = 0 \), and (7) follows immediately.

Otherwise, the only possibilities for \( Q \) are \((0, \pm 1)\), and by replacing \( P \) by \(-P\) if necessary, we may suppose that \( Q = (0, 1) \). Then \( l \) is of the form \( y = mx + 1, \ m \in \mathcal{Q} \), whence the points of intersection are given by

\[
1 - 2x + x^2 - 4x^3 = m^2 x^2 + 2mx + 1,
\]

so that \( x_p \) is a root of

\[
4x^2 + (m^2 - 1)x + 2(m + 1) = 0.
\]

Putting \( m = 2t - 1 \) gives

\[
x_p^2 + t(t-1)x_p + t = 0, \quad y_p = (2t-1)x_p + 1,
\]

as required.

**Corollary.** If \( x \) is a unit of its quadratic field, then either (i) \( \pm P = (1, 2i), (-1, 2\sqrt{2}) \) or (ii) \( \pm P = (i, 1+i), (-i, 1-i), (-1+\sqrt{2}, -4+3\sqrt{2}), (-1-\sqrt{2}, -4-3\sqrt{2}). \)

**Proof.** If \( x \) is a unit of \( \mathcal{Z} \), then \( x = \pm 1 \) and (i) follows from (7).

If \( x \) is a unit of a quadratic field, then \( \text{Norm}(x) = \pm 1 \), so necessarily in (8), \( t = \pm 1 \) and the result follows.
We now give a similar argument which deals with the cubic case, leading to the result of Bremner [1] in a neater manner.

For suppose that \( P \in E \), with the coordinates of \( P = (x_p, y_p) \) lying in a cubic number field.

Take a parabola through \( P \) and its two \( Q \)-conjugates, with equation
\[
dy = px^2 + qx + r, \quad d, p, q, r \in \mathbb{Z}, \quad d \neq 0, \quad (d, p, q, r) = 1.
\]
This parabola meets \( E \) in six points, two of which occur at \( o \), and three of which form a conjugate set over \( Q \). The remaining point \( Q \) of intersection is thus rational.

If \( Q = o \), then \( p = 0 \) so that \( x_p \) satisfies
\[
d^2 (1 - 2x_p + x_p^2 - 4x_p^3) = (qx_p + r)^2,
\]
i.e.
\[
4d^2 x_p^3 + (q^2 - d^2) x_p^2 + (2qr + 2d^2) x_p + (r^2 - d^2) = 0. \tag{9}
\]
If \( Q \neq o \), then as before, we may suppose that \( Q = (0, 1) \). Then \( r = d \), and \( x_p \) satisfies
\[
d^2 (1 - 2x + x^2 - 4x^3) = (px^2 + qx + d)^2.
\]
Removing the root at \( 0 \), \( x_p \) thus satisfies the residual cubic equation
\[
p^2 x_p^3 + (2pq + 4d^2) x_p^2 + (q^2 + 2pd - d^2) x_p + (2qd + 2d^2) = 0. \tag{10}
\]
If now \( x_p \) is to be a unit of the cubic number field, then in the first instance, at (9) above, it follows that \( r^2 - d^2 = \mp 4d^2 \), which is impossible. So the second instance must hold, and from (10),
\[
\begin{align*}
\text{(11a)} & \quad \pm p^2 = 2qd + 2d^2, \\
\text{(11b)} & \quad p^2 | 2pq + 4d^2, \\
\text{(11c)} & \quad p^2 | q^2 + 2pd - d^2.
\end{align*}
\]
Now \( (d, p) = 1 \), otherwise (c) leads to a contradiction of \( (d, p, q, r) = 1 \). Then (a) forces \( d = 1 \) and \( 2|p \); and (b) forces \( p | 4 \) and \( 4p | d \). Consequently \( p = \pm 2 \), and (a) gives \( q = 1, -3 \). Hence the only solutions are \((p, q, r, d) = (\pm 2, 1, 1, 1), \quad (\pm 2, -3, 1, 1) \). The former pair returns \( X = x_p \) of norm \(-1 \), contrary to (5). And the latter pair returns the cubic fields given in Bremner [1].

4. Suppose now that \( P \in E \) with coordinates of \( P = (x_p, y_p) \) lying in a quartic number field; further, we assume \( x_p \) is a unit of the field. Take the cubic curve \( \Gamma \) through \( P \) and its three \( Q \)-conjugates, with equation
\[
dy = px^3 + qx^2 + rx + s, \quad d, p, q, r, s \in \mathbb{Z}, \quad d \neq 0, \quad (d, p, q, r, s) = 1. \tag{12}
\]
Then \( \Gamma \) meets \( E \) in nine points. Three of these occur at \( o \), and four form a \( Q \)-rational set. The remaining two points of intersection are thus defined (as a pair) over \( Q \).
The equation \(xyz = x + y + z = 1\)  

(i) Suppose that one of these points is \(o\). Then \(p = 0\), and there is a further zero at \(o\). The quartic satisfied by \(x_p\) is  
\[
d^2 (1 - 2x_p + x_p^2 - 4x_p^3) = (qx_p^2 + rx_p + s)^2,
\]
i.e.  
\[
q^2 x_p^2 + (2qr + 4d^2) x_p^3 + (r^2 + 2qs - d^2) x_p^2 + (2rs + 2d^2) x_p + (s^2 - d^2) = 0.
\]
The requirement that \(x_p\) be a unit, with \(\text{Norm}(x_p) = 1\), implies  
(13a)  
\[q^2 = s^2 - d^2,\]
(13b)  
\[q^2 | 2qr + 4d^2,\]
(13c)  
\[q^2 | r^2 + 2qs - d^2,\]
(13d)  
\[q^2 | 2rs + 2d^2.\]
Now \((q, d) = 1\), otherwise (a), (c) contradict \((d, q, r, s) = 1\). Then (b) forces \(q | 4\); and since \(d \neq 0\), (a) gives \(q = 4\), \((s, d) = (\pm 5, \pm 3)\). But now (b) cannot hold. Consequently no unit solutions \(x_p\) arise in this instance.

(ii) Suppose the residual pair is individually rational. It cannot be the pair \((0, 1), (0, -1)\) for then \(d = s\), \(d = -s\), forcing \(d = 0\). In virtue of (i), we can thus assume it is a double root at one of the points \((0, \pm 1)\). In any event, \(d^2 = s^2\) and \(-2d^2 = 2rs\), so that \(d = \pm s\), \(r = -s\).

The quartic satisfied by \(x_p\) is  
\[
s^2 (1 - 2x + x^2 - 4x^3) = (px^3 + qx^2 - sx + s)^2,
\]
i.e.  
\[
p^2 x^4 + 2pqx^3 + (q^2 - 2ps)x^2 + (2ps - 2qs + 4s^2)x + 2qs = 0.
\]

The requirement that \(x_p\) be a unit of norm 1 gives  
(14a)  
\[p^2 = 2qs,\]
(14b)  
\[p^2 | 2pq,\]
(14c)  
\[p^2 | q^2 - 2ps,\]
(14d)  
\[p^2 | 2ps - 2qs + 4s^2.\]
Now \((p, s) = 1\) otherwise (c) gives \((p, q, s) \neq 1\) where \((d, p, q, r, s) \neq 1\). So (a) gives \(s = 1\), \(p^2 = 2q\). Now (d) gives \(p | 4\), \(4 | p\), and since \(2 | p\), then \(p = 2\varepsilon\) \((\varepsilon = \pm 1)\), \(q = 2\). Thus \(x_p\) satisfies the quartic  
(15)  
\[x^4 + 2\varepsilon x^3 + (1 - \varepsilon)x^2 + \varepsilon x + 1 = 0.\]

Denoting a root of (15) by \(\Theta\), we recover the following unit solution of (1):
\[ x = -\Theta^3 - 2\varepsilon\Theta^2 + (\varepsilon - 1)\Theta - \varepsilon, \]
\[ y = \varepsilon\Theta^2 + \Theta, \]
\[ z = \Theta^3 + \varepsilon\Theta^2 - \varepsilon\Theta + (1 + \varepsilon). \]

(iii) If neither (i) nor (ii) happens, then necessarily the residual pair is not individually defined over \( \mathcal{O} \).

By Lemma 1, the intersection therefore contains either a double point at \( x = t, t \in \mathcal{O} - \{0\} \), or contains the pair of points corresponding to the roots of \( x^2 + t(t-1)x + t = 0, t \in \mathcal{O} - \{0\} \). In particular, the sextic polynomial representing the intersection of the curves (6) and (12) either contains a repeated root at \( x = t \), or contains the quadratic factor \( x^2 + t(t-1)x + t \). Note now that \( p \neq 0 \).

The intersection is given by
\[ d^2 (1 - 2x + x^2 - 4x^3) = (px^3 + qx^2 + rx + s)^2. \]

A rational root \( x = t \) implies \( 1 - 2t + t^2 - 4t^3 \) is square, so that perforce \( t = 0 \), a contradiction.

Consequently, on writing (17) as a sextic equation for \( x \), then it possesses \( x^2 + t(t-1)x + t, t \in \mathcal{O} - \{0\} \), as a quadratic factor. Since we are assuming \( x_p \) is a unit of norm 1, the residual quartic is of type \( x^4 + ax^3 + bx^2 + cx + 1 \), \( a, b, c \in \mathcal{O} \). It follows that
\[ p^2 x^6 + 2pq x^5 + (q^2 + 2pr) x^4 + (2qr + 2ps + 4d^2) x^3 + (r^2 + 2qs - d^2) x^2 + (2rs + 2d^2) x + (s^2 - d^2) \]
\[ = p^2 [x^2 + t(t-1)x + t] [x^4 + ax^3 + bx^2 + cx + 1]. \]

By Gauss' Lemma, \( p^2 [x^2 + t(t-1)x + t] \) has integer coefficients, so that
\[ t = u/p, \quad u \in \mathcal{O}, \quad u \neq 0, \quad (u, p) = 1. \]

The right-hand side at (18) is \( [p^2 x^2 + u(u-p)x + up] [x^4 + ax^3 + bx^2 + cx + 1] \), and equating coefficients of powers of \( x \),
\[ 2pq = p^2 a + u(u-p), \]
\[ q^2 + 2pr = p^2 b + u(u-p) a + up, \]
\[ 2qr + 2ps + 4d^2 = p^2 c + u(u-p) b + upa, \]
\[ r^2 + 2qs - d^2 = p^2 + u(u-p) c + upb, \]
\[ 2rs + 2d^2 = u(u-p) + upc, \]
\[ s^2 - d^2 = up. \]

If \( \pi \) is an odd prime factor of \( p \), then it follows easily that \( p \equiv q \equiv r \equiv s \equiv d \equiv 0 \mod \pi \). Thus \( \pm p \) must be a power of 2. Suppose next \( p \equiv 0 \mod 4 \). Then sequentially, (a) implies \( u \equiv 0 \mod 4 \), (b) implies \( q \equiv 0 \mod 4 \), (c) implies \( d \equiv 0 \mod 2 \), (d) and (e) imply \( r \equiv s \equiv 0 \mod 2 \), contradicting \( (p, q, r, s, d) \neq 1 \).
The equation \(xyz = x + y + z = 1\)

Since we can assume without loss of generality that \(p > 0\), then \(p = 1\) or \(2\). However, (a) implies \(p \mid u^2\), and from (19) we have \((p, u) = 1\). Necessarily therefore \(p = 1\).

Substitute into equations (20), and use (f) to eliminate \(d^2\):

\[
\begin{align*}
\text{(21a)} \quad & 2q = a + u(u - 1), \\
\text{(21b)} \quad & q^2 + 2r = b + u(u - 1)a + u, \\
\text{(21c)} \quad & 2qr + 2s = c + u(u - 1)b + ua + 4u - 4u^2, \\
\text{(21d)} \quad & r^2 + 2qs = 1 + u(u - 1)c + ub - u + s^2, \\
\text{(21e)} \quad & 2rs = u(u + 1) + uc - 2s^2.
\end{align*}
\]

Use (21a) to eliminate \(q\), and, after multiplying (b), (c), (d) by \(s, s, s^2\), respectively, use (21e) to eliminate \(r\):

\[
\begin{align*}
\text{(22a)} \quad & 4sb = sa^2 - 2u(u - 1)sa + 4uc + 4u(u + 1) + (u^4 - 2u^3 + u^2 - 4u)s - 8s^2, \\
\text{(22b)} \quad & (u(u + 1) - 2us - 2s^2)a + uac + (u^2(u - 1) - 2s)c - 2u(u - 1)sb \\
& \quad + u^2(u^2 - 1) - 8us + (-2u^2 + 2u + 4)s^2 + 8s^3 = 0, \\
\text{(22c)} \quad & u^2c^2 + 2u^2(u + 1 - 2s^2)c - 4us^2b + 4s^3a \\
& \quad + u^2(u + 1)^2 - 4(u^2 + 1)s^2 + 4u(u - 1)s^3 = 0.
\end{align*}
\]

Use (22a) to eliminate \(b\): there results

\[
\begin{align*}
\text{(23a)} \quad & -(u - 1)sA^2 + 2uAC + 4(3u - 1)s(s^2 - u) = 0, \\
\text{(23b)} \quad & -s^2A^2 + u^3C^2 - 4s^2(u^3 - 1)(s^2 - u) = 0
\end{align*}
\]

where

\[
\begin{align*}
\text{(24)} \quad & A = ua - (u^2(u - 1) + 2s), \\
\text{(25)} \quad & C = c + (u + 1 - 2s - 2s^2).
\end{align*}
\]

Multiply (23b) by \(A^2\), and use (a) to eliminate \(C\) (recall from (20f) that \(d^2 = s^2 - u\)):

\[
\text{(26)} \quad s^2(A^2 - 4d^2)((-u^3 + 2u^2 - u + 4)A^2 + 4u(3u - 1)^2d^2) = 0.
\]

If \(s^2(A^2 - 4d^2) \neq 0\) then it follows that

\[
(u^3 - 2u^2 + u - 4)A^2 = 4u(3u - 1)^2d^2
\]

so that

\[
\left(1 - \frac{2}{u} + \frac{4}{u^3} \right)A^2 = \left(\frac{2(3u - 1)d}{u}\right)^2,
\]
which in virtue of the remarks of the final paragraph of Section 2, forces
\( A = 0 = 2(3u-1)d \), a contradiction. Accordingly, \( s^2(A^2-4d^2) = 0 \) and we
have either I: \( A = 2de(\varepsilon = \pm 1) \), or II: \( s = 0 \).

Case I. If \( A = 2de \), then (23) gives \( C = -2sde \). Solving (24) for \( a \),
\begin{equation}
 a = 2/(s-de)+u(u-1)
\end{equation}
and from (21a),
\begin{equation}
 q = 1/(s-de)+u(u-1).
\end{equation}
Thus
\begin{equation}
 s-de = \alpha = \pm 1
\end{equation}
so that
\begin{equation}
 s+de = \alpha u
\end{equation}
whence solving (29), (30) for \( s, d \),
\begin{equation}
 s = \alpha(u+1)/2, \quad d = \alpha(u-1)/2.
\end{equation}
Solving (25) for \( c \), (21b) for \( b \), and (21e) for \( r \), gives the following parameterization:
\begin{align*}
p &= 1, \\
q &= u(u-1)+\alpha, \\
r &= (\alpha/2+1)u-\alpha/2, \\
s &= \alpha(u+1)/2, \\
d &= \alpha(u-1)/2, \\
a &= u(u-1)+2\alpha, \\
b &= (\alpha+1)u+(1-\alpha), \\
c &= \alpha(u+1).
\end{align*}
Taking \( \alpha = +1 \), \( \alpha = -1 \), gives the respective triples
\begin{equation}
(a, b, c) = (u^2-u+2, 2u, u+1), \quad (u^2-u-2, 2, -u-1).
\end{equation}
An elementary exercise shows that the quartic of which \( x_p \) is a root, namely
\( x^4+ax^3+bx^2+cx+1 \), is irreducible precisely for \( u \neq 1 \) in the first instance at
(33), and \( u \neq \pm 1,3 \) in the second instance at (33).

It is now possible to recover a solution of the original equation (1), via the
transformations (3), (4).

The first case at (33) leads to the following.
Let \( u \in \mathbb{Z} \), \( u \neq 0, 1 \), and define

\[
(34) \quad \theta^4 + (u^2 - u + 2) \theta^3 + 2u \theta^2 + (u + 1) \theta + 1 = 0.
\]

Then

\[
(35) \quad x = -\theta^3 - (u^2 - u + 2) \theta^2 - 2u \theta - (u + 1),
\]

\[
(u - 1)y = -\theta^3 - (u^2 - u + 1) \theta^2 + (u^2 - 3u + 1) \theta + (u - 2),
\]

\[
(u - 1)z = u \theta^3 + (u^3 - u^2 + 2u - 1) \theta^2 + (u^2 + u - 1) \theta + u^2.
\]

Notice again that the quadratic equation giving (3) ensures that \( y \) (and hence \( z \)) is both an algebraic integer and a unit, so that despite the appearance of denominators at (35), there is an automatic guarantee of integrality. (It can in fact be shown that the equation satisfied by \( y \) is

\[
y^4 - (u + 3)y^3 + 4uy^2 - (u^2 + u - 2)y - 1 = 0;
\]

the equation for \( z \) is left as an exercise.)

Similarly, the second case at (33) leads to the following:

Let \( u \in \mathbb{Z} \), \( u \neq 0, \pm 1, 3 \); and define

\[
(36) \quad \phi^4 + (u^2 - u - 2) \phi^3 + 2 \phi^2 - (u + 1) \phi + 1 = 0.
\]

Then

\[
(37) \quad x = -\phi^3 - (u^2 - u - 2) \phi^2 - 2 \phi + (u + 1),
\]

\[
(u - 1)y = -\phi^3 - (u^2 - u - 1) \phi^2 - (u^2 - u + 1) \phi + u,
\]

\[
(u - 1)z = u \phi^3 + (u^3 - u^2 - 2u + 1) \phi^2 + (u^2 + u - 1) \phi - u^2;
\]

where, as above, \( y \) and \( z \) are both integers and units of \( \mathcal{O}(\phi) \).

Case II. If \( s = 0 \), then (21e) implies

\[
(38) \quad c = -u - 1.
\]

The equations (21) become:

\[
(39a) \quad 2q = a + u(u - 1),
\]

\[
(39b) \quad q^2 + 2r = b + u(u - 1)a + u,
\]

\[
(39c) \quad 2qr = u(u - 1)b + ua + 3u - 1,
\]

\[
(39d) \quad r^2 = ub - u^3 + 1,
\]

with, from (20f),

\[
(40) \quad d^2 = -u.
\]

Use (39a) to eliminate \( q \) in (39b):

\[
(41) \quad 2r = b - \frac{1}{4}a^2 + \frac{1}{4}u(u - 1)a - \frac{1}{2}u^2(u - 1)^2 + u.
\]
Use (39a), (41) to eliminate \( q, r \) in (39c):

\[
\begin{align*}
42. \quad b \left( \frac{1}{2} a - \frac{1}{2} u(u-1) \right) &= \frac{1}{8} a^3 - \frac{1}{8} u(u-1) a^2 + \left( -\frac{1}{2} u^2 (u-1)^2 + \frac{1}{2} u \right) a \\
&\quad + \left( \frac{1}{8} u^3 (u-1)^3 - \frac{1}{2} u^2 (u-1) + 3 u - 1 \right).
\end{align*}
\]

Then, using (41) to eliminate \( b \),

\[
43. \quad r \left( a - u(u-1) \right)
= \frac{1}{2} u(u-1) a^2 + \left( -\frac{1}{2} u^2 (u-1)^2 + u \right) a + \left( \frac{1}{4} u^3 (u-1)^3 - u^2 (u-1) + 3 u - 1 \right).
\]

Using (42), (43) in (39d), there results after simplification

\[
44. \quad \left[ (u^3 - 2 u^2 + u - 4) (a^2 - 2 u (u-1) a) \right]
\times \left[ u a^2 - 2 u^2 (u-1) a + (u^3 (u-1)^2 + 4) \right] = 0.
\]

If the first factor is to be zero, then

\[
(u^3 - 2 u^2 + u - 4) (a - u(u-1))^2 + 4 (3 u - 1)^2 = 0,
\]

so in particular

\[
45. \quad -u^3 + 2 u^2 - u + 4 = v^2, \quad v \in \mathbb{Z}.
\]

The elliptic curve represented by (45) has rank 1 (and there are integer points for \( u = 0, 1, -15 \)); however, in virtue of (40), we are only interested in the curve of genus 2 represented by

\[
46. \quad d^6 + 2 d^4 + d^2 + 4 = v^2.
\]

But the only integer points on the curve (46) have \( d = 0 \), for it may be written in the form

\[
(d^3 + d)^2 + 4 = v^2
\]

which clearly forces \( d^3 + d = 0 \), i.e. \( d = 0 \). Since we assumed \( d \neq 0 \), only the second factor at (44) may be zero.

In this instance, then

\[
ua^2 - 2 u^2 (u-1) a + u^3 (u-1)^2 + 4 = 0,
\]

that is,

\[
47. \quad u (a - u(u-1))^2 + 4 = 0.
\]

Using (40),

\[
48. \quad d (a - u(u-1)) = 2 \varepsilon, \quad \varepsilon = \pm 1,
\]

so that

\[
u (a - u(u-1)) = 2 d \varepsilon
\]
and from (24),

\[ A = 2 \delta e; \]

thus this instance has been covered by Case I.

Theorem 1 now follows from the solutions (16), (35) and (37) noting that the solutions at (16) are the particular cases of (35) and (37) at \( u = 0. \)

The discriminant of \( Q(\theta) \) at (34) is equal to

\[ -(u - 1)^2 (4u^7 - 5u^6 - 6u^5 + 77u^4 - 304u^3 + 725u^2 - 1006u + 643); \]

and the discriminant of \( Q(\phi) \) at (36) is

\[ (u + 1)^2 (4u^7 - 35u^6 + 102u^5 - 69u^4 - 216u^3 + 499u^2 - 402u + 117). \]

I am grateful to H. M. Edgar for drawing my attention to this problem.

References


