ACTA ARITHMETICA
162.4 (2014)

Solutions to $xyz = 1$ and $x + y + z = k$ in algebraic integers of small degree, I

by

H. G. Grundman (Bryn Mawr, PA) and
L. L. Hall-Seelig (North Andover, MA)

1. Introduction. In a 1960 paper, Cassels [3] studied the equations $xyz = x + y + z = 1$ and their simultaneous solutions in $\mathbb{Q}$. Numerous papers on this system of equations were inspired by his work; for example, see [1, 2, 4, 6, 7, 8, 10]. Of particular interest here is the work of Bremner [2] in which he devised a method for finding all solutions in algebraic integers in fields of degree less than or equal to four.

In this paper, we generalize Bremner's methods to study the simultaneous solutions of the equations

$$xyz = 1 \quad \text{and} \quad x + y + z = k \tag{1}$$

with $k \in \mathbb{Z}$ and x, y, z algebraic integers in a field of degree at most four over $\mathbb{Q}$. This system was considered briefly by Thomas and Vasquez [9] in their work on the extensively studied system $x^3 + y^3 + z^3 = \lambda xyz$.

Since the equations in (1) are symmetric, permuting the values of x, y, and z in a solution generally yields additional solutions. Considering such permutations to be equivalent, our goal, as is standard, is to determine all equivalence classes of solutions, under specific restrictions.

To fix notation, let F be an algebraic number field with $[F : \mathbb{Q}] \le 4$. Let $\mathcal{O}_F$ be its ring of integers. Fix $k \in \mathbb{Z}$ and let $(x, y, z) \in \mathcal{O}_F^3$ be a solution to the system of equations given in (1).

Since $xyz = 1$, we see that x, y, and z must all be units in $\mathcal{O}_F$ and at least one of them, say x, must have norm 1. Combining $xyz = 1$ and $x + y + z = k$, eliminating z, we obtain $y^2 + (x - k)y + 1/x = 0$. Hence,

$$2y = -x + k \pm x\sqrt{1 - 2k/x + k^2/x^2 - 4/x^3}.$$

Setting $x_P = 1/x$ and $y_P = \pm\sqrt{1 - 2k/x + k^2/x^2 - 4/x^3}$ (choosing either

2010 *Mathematics Subject Classification*: Primary 11D25; Secondary 11G05, 11R16.
Key words and phrases: Diophantine equations, elliptic curves.

DOI: 10.4064/aa162-4-5

square root), we obtain a point $P = (x_P, y_P)$ on the curve

$$\mathcal{E}_k : y^2 = 1 - 2kx + k^2x^2 - 4x^3$$

with x_P, $y_P \in \mathcal{O}_F$ and x_P a unit of norm 1.

Conversely, given a point (x_P, y_P) on $\mathcal{E}_k$ with $x_P, y_P \in \mathcal{O}_F$ and x_P a unit of norm 1, set

$$\begin{aligned} x &= 1/x_P, \\ y &= (k - 1/x_P + y_P/x_P)/2, \\ z &= (k - 1/x_P - y_P/x_P)/2. \end{aligned} \tag{2}$$

Then x is clearly a unit of norm 1 in $\mathcal{O}_F$; y, satisfying the equation $y^2 + (x-k)y + 1/x = 0$, is also in $\mathcal{O}_F$; and $z \in \mathcal{O}_F$, since $x + y + z = k$. Hence we obtain a solution to (1): (x, y, z), with $x, y, z \in \mathcal{O}_F$.

As is easily verified, the point $(x_P, -y_P)$, which is also on $\mathcal{E}_k$, corresponds to the solution (x, z, y), a permutation of the solution corresponding to the point (x_P, y_P). In general, the automorphism $\varphi : \mathcal{E}_k(F) \to \mathcal{E}_k(F)$ defined by $\varphi(x_P, y_P) = (x_P, -y_P)$ fixes equivalence classes of solutions to (1).

In this work, we consider the values of k for which $|\mathcal{E}_k(\mathbb{Q})| = 3$. As is easily verified, for any such k, $\mathcal{E}_k(\mathbb{Q}) = \{\mathfrak{O}, (0,1), (0,-1)\}$. We note that this condition excludes any $k = -d^2$ with $d \in \mathbb{Z} - \{0\}$, since $(d, d^3 - 1) \in \mathcal{E}_{-d^2}(\mathbb{Q})$ implies that

$$|\mathcal{E}_{-d^2}(\mathbb{Q})| > 3. \tag{3}$$

Since this condition also excludes $k = 3$, we see that, for all k under consideration, $\mathcal{E}_k$ is an elliptic curve. We further note that $|\mathcal{E}_k(\mathbb{Q})| = 3$ for almost all values of k for which $|\mathcal{E}_k(\mathbb{Q})|$ is finite. In [5], we prove this fact and examine the remaining cases with $|\mathcal{E}_k(\mathbb{Q})|$ finite.

In the following sections, we find all solutions to the system of equations (1) with $|\mathcal{E}_k(\mathbb{Q})| = 3$ and $(x, y, z) \in \mathcal{O}_F^3$ where $[F : \mathbb{Q}] \leq 4$. We begin, in Section 2, with the case $[F : \mathbb{Q}] \leq 3$, then, in Section 3, we consider $[F : \mathbb{Q}] = 4$.

2. Solutions with $[F : \mathbb{Q}] \leq 3$. Following the methods of Bremner [2], we begin by determining all points $(x_P, y_P) \in \mathcal{E}_k(F)$ for any quadratic field F.

LEMMA 2.1. *Let $k \in \mathbb{Z}$ be such that $|\mathcal{E}_k(\mathbb{Q})| = 3$ and let $[F : \mathbb{Q}] = 2$. If $P = (x_P, y_P) \in \mathcal{E}_k(F)$ is a finite point, then for some $t \in \mathbb{Q}$, either*

1. *$x_P = t$ and $\pm y_P = \sqrt{1 - 2kt + k^2t^2 - 4t^3}$, or*
2. *$x_P^2 + t(t-k)x_P + t = 0$ and $\pm y_P = (2t-k)x_P + 1$.*

Proof. First note that if $x_P \in \mathbb{Q}$, then the coordinates in part 1 of the lemma are immediate.

Now assume that $x_P \notin \mathbb{Q}$. Let $\overline{P} = (\overline{x}_P, \overline{y}_P)$ be the conjugate of P over $\mathbb{Q}$ and note that $\overline{P} \in \mathcal{E}_k(F)$. Let $\mathcal{L}$ be the line passing through P and $\overline{P}$. Then $\mathcal{L}$ is fixed by conjugation over $\mathbb{Q}$ and hence is defined by an equation with rational coefficients. Let Q be the third point of intersection of $\mathcal{E}_k$ and $\mathcal{L}$, and note that, being fixed by conjugation over $\mathbb{Q}$, Q is in $\mathcal{E}_k(\mathbb{Q})$. Since $x_P \notin \mathbb{Q}$, Q is a finite point in $\mathcal{E}_k(\mathbb{Q})$.

If $Q = (0, 1)$, then the equation for $\mathcal{L}$ is $y = mx + 1$ for some $m \in \mathbb{Q}$. The x-coordinates of the points of intersection of $\mathcal{L}$ and $\mathcal{E}_k$ then satisfy the equation $(mx + 1)^2 = 1 - 2kx + k^2x^2 - 4x^3$, which simplifies to

$$4x^3 + (m^2 - k^2)x^2 + (2m + 2k)x = 0.$$

Since $x_P \notin \mathbb{Q}$, $x_P \neq 0$, and so $4x_P^2 + (m^2 - k^2)x_P + (2m + 2k) = 0$. Letting $t = (m+k)/2 \in \mathbb{Q}$ yields x_P as in part 2 of the lemma and $y_P = (2t-k)x_P+1$.

If $Q = (0, -1)$, by applying the homomorphism φ, from the introduction, to the previous case, we obtain the corresponding point with the same expression for x_P and $-y_P = (2t - k)x_P + 1$. ∎

The following theorem gives all solutions to the system of equations given in (1) with $|\mathcal{E}_k(\mathbb{Q})| = 3$ and $[F : \mathbb{Q}] \leq 2$. It is easily verified that the given solutions are distinct, unless $k = -1$, a value that is excluded by the hypothesis, since $|\mathcal{E}_{-1}(\mathbb{Q})| \neq 3$.

THEOREM 2.2. *Let $k \in \mathbb{Z}$ be such that $|\mathcal{E}_k(\mathbb{Q})| = 3$ and let $[F : \mathbb{Q}] \leq 2$. If $F = \mathbb{Q}$, then the equations $x + y + z = k$ and $xyz = 1$ have no simultaneous solutions (x, y, z) with $x, y, z \in \mathcal{O}_F$. If $[F : \mathbb{Q}] = 2$, the equations are simultaneously solvable with $x, y, z \in \mathcal{O}_F$ in exactly the following instances, allowing for permutations of x, y, and z:*

1. *$F = \mathbb{Q}(\nu)$ with $\nu^2 = k^2 - 2k - 3$ and*
$$(x, y, z) = \left(1, \frac{k - 1 + \nu}{2}, \frac{k - 1 - \nu}{2}\right).$$
2. *$F = \mathbb{Q}(\nu)$ with $\nu^2 = k^2 + 2k + 5$ and*
$$(x, y, z) = \left(-1, \frac{k + 1 + \nu}{2}, \frac{k + 1 - \nu}{2}\right).$$

Proof. It is easy to verify that each of these is a solution with $x, y, z \in \mathcal{O}_F$. To prove there are no other solutions, we assume that $[F : \mathbb{Q}] \leq 2$, $|\mathcal{E}_k(\mathbb{Q})| = 3$, and $(x, y, z) \in \mathcal{O}_F^3$ is a solution to the system of equations.

If $x, y, z \in \mathbb{Q}$ (and thus in $\mathbb{Z}$), then $xyz = 1$ immediately implies that $x, y, z \in \{-1, 1\}$. But then $x + y + z = k$ implies that $k = 3$ or $k = -1$, in which cases $|\mathcal{E}_k(\mathbb{Q})| \neq 3$. So there are no rational solutions.

If not all of x, y, and z are in $\mathbb{Q}$, but at least one is, say $x \in \mathbb{Q}$, then $x = \pm 1$. Solving the equation $1 + y + 1/y = k$ leads to the solution in part 1 of the theorem, and solving $-1 + y - 1/y = k$ leads to the solution in part 2.

Now, suppose $x, y, z \in F - \mathbb{Q}$ and assume, without loss of generality, that $N_F(x) = 1$. Let $P = (x_P, y_P)$ be a point in $\mathcal{E}_k(F)$ corresponding to the solution (x, y, z). It follows that $x_P \notin \mathbb{Q}$ and $N_F(x_P) = 1$. By Lemma 2.1, since $|\mathcal{E}_k(\mathbb{Q})| = 3$, $x_P^2 + t(t-k)x_P + t = 0$. Since $N_F(x_P) = 1$, $t = 1$, and so $x_P^2 + (1-k)x_P + 1 = 0$ and $\pm y_P = (2-k)x_P + 1$. But this leads to a solution, (x, y, z), with y or z equal to $1 \in \mathbb{Q}$, contrary to assumption. ∎

The next theorem provides the solutions for the case $[F : \mathbb{Q}] = 3$. Note that the solutions given are distinct and that, for $k \in \mathbb{Z}$, the given cubic polynomials are irreducible. The solutions in part 2 were identified previously in [9].

THEOREM 2.3. *Let $k \in \mathbb{Z}$ and let $[F : \mathbb{Q}] = 3$. The equations $x+y+z = k$ and $xyz = 1$ are simultaneously solvable with $x, y, z \in \mathcal{O}_F$ in the following instances, allowing for permutations of x, y, and z. If $|\mathcal{E}_k(\mathbb{Q})| = 3$, then these are the only solutions.*

1. *$F = \mathbb{Q}(\mu)$ with μ a fixed root of $X^3 - (k+1)X^2 + (k+2)X - 1 = 0$ and*
$$(x, y, z) = (\mu^2 - (k+1)\mu + (k+2), \mu - 1, -\mu^2 + k\mu - 1).$$
2. *$F = \mathbb{Q}(\mu)$ with μ a fixed root of $X^3 + (k+3)X^2 + kX - 1 = 0$ and*
$$(x, y, z) = (\mu^2 + (k+3)\mu + k, -\mu - 1, -\mu^2 - (k+2)\mu + 1).$$

Proof. Let F be a cubic field. It is easy to verify that each of these is a solution with $x, y, z \in \mathcal{O}_F$.

Suppose that $|\mathcal{E}_k(\mathbb{Q})| = 3$ and $(x, y, z) \in \mathcal{O}_F^3$ is a solution to the system of equations. By Theorem 2.2, x, y, and z cannot all be in $\mathbb{Z}$. If at least one is, say $x \in \mathbb{Z}$, then $x = \pm 1$, and y and z are quadratic over $\mathbb{Q}$, contradicting the hypotheses. So $x, y, z \in F - \mathbb{Q}$.

Assume, without loss of generality, that $N_F(x) = 1$. Let $P = (x_P, y_P)$ be a point in $\mathcal{E}_k(F)$ corresponding to the solution (x, y, z). From $x \notin \mathbb{Q}$, it follows that $x_P \notin \mathbb{Q}$.

Let $\mathcal{C}$ be the quadratic curve going through P and its two conjugates. Let $dy = px^2 + qx + r$ be an equation for $\mathcal{C}$ with $d, p, q, r \in \mathbb{Z}$, $d \neq 0$, and $\gcd(p, q, r, d) = 1$. Then the x-coordinates of the points of $\mathcal{E}_k \cap \mathcal{C}$ satisfy
$$d^2(1 - 2kx + k^2x^2 - 4x^3) = (px^2 + qx + r)^2,$$
which simplifies to
$$(4) \quad p^2x^4 + (2pq + 4d^2)x^3 + (2pr + q^2 - k^2d^2)x^2 + (2qr + 2kd^2)x + (r^2 - d^2) = 0.$$

Of the six points in $\mathcal{E}_k \cap \mathcal{C}$, three are (x_P, y_P) and its conjugates and, from (4), at least two are infinite points. Let Q be the one additional point. Since the coefficients of (4) are rational, the set of solutions is closed under conjugation and thus Q must be rational.

If Q is infinite, then $p = 0$. Thus, $x_P \in \mathcal{O}_F$ is a root of

$$4d^2x^3 + (q^2 - k^2d^2)x^2 + (2qr + 2kd^2)x + (r^2 - d^2) = 0.$$

But then, since $N_F(x_P) = 1$, we have $r^2 = -3d^2$, a contradiction.

If $Q = (0, 1)$, then since $(0, 1)$ is on $\mathcal{C}$, we have $d = r$. After removing the extra factor of x, equation (4) becomes

$$p^2x^3 + (2pq + 4d^2)x^2 + (2pd + q^2 - k^2d^2)x + (2qd + 2kd^2) = 0. \tag{5}$$

Since x_p is an algebraic integer of norm 1, each coefficient is divisible by p^2 and $2qd + 2kd^2 = -p^2$.

Suppose that ℓ is a prime factor of d. Since $-p^2 = 2qd + 2kd^2$, we have $\ell \mid p$, and since $p^2 \mid (2pd+q^2-k^2d^2)$, we also have $\ell \mid q$. But $d = r$ then implies that $\ell \mid \gcd(p, q, r, d)$, a contradiction. Hence, $d = \pm 1$. Assume without loss of generality that $d = 1$.

It follows that $p^2 = -2q - 2k$ and $p^2 \mid (2pq + 4)$. From the first condition, p is even; from the second, $p \mid 4$. If $p = \pm 4$, we get $16 \mid (\pm 8q + 4)$, a contradiction. Thus $p = \pm 2$. From $p^2 = -2q - 2k$, $q = -(k + 2)$.

If $p = 2$, then, by (5), the minimal polynomial for x_P is $x^3 - (k+1)x^2 + (k+2)x - 1$ and, from the equation for $\mathcal{C}$, we have $y_P = 2x_P^2 - (k+2)x_P + 1$. Using (2), this yields the solution in part 1 of the theorem. If $p = -2$, the minimal polynomial for x_P is $x^3 + (k + 3)x^2 + kx - 1$ and $y_P = -2x_P^2 - (k + 2)x_P + 1$. This yields the solution in part 2.

As noted in the introduction, if $Q = (0, -1)$, the same solutions (up to permutation) are obtained. ∎

3. Solutions with $[F : \mathbb{Q}] = 4$. The case $[F : \mathbb{Q}] = 4$ is more complicated, as illustrated by the following theorem and proof. Again, our method of proof is motivated by [2].

THEOREM 3.1. *Let $k \in \mathbb{Z}$ and let $[F : \mathbb{Q}] = 4$. The equations $x+y+z = k$ and $xyz = 1$ are simultaneously solvable with $x, y, z \in \mathcal{O}_F$ in the following instances, allowing for permutations of x, y, and z. If $|\mathcal{E}_k(\mathbb{Q})| = 3$, then these are the only solutions.*

1. *$F \supseteq \mathbb{Q}(\gamma, \delta)$ where, for some $t \in \mathbb{Z}$, δ is a fixed root of $X^2 - tX - 1 = 0$, γ is a fixed root of $X^2 = (\delta - k)^2 - 4(\delta - t)$, and*

$$(x, y, z) = \left(\delta, \frac{k - \delta + \gamma}{2}, \frac{k - \delta - \gamma}{2}\right).$$

2. *$F \supseteq \mathbb{Q}(\gamma, \delta)$ where, for some $t \in \mathbb{Z}$, δ is a fixed root of $X^2 - tX + 1 = 0$, γ is a fixed root of $X^2 = (\delta - k)^2 + 4(\delta - t)$, and*

$$(x, y, z) = \left(\delta, \frac{k - \delta + \gamma}{2}, \frac{k - \delta - \gamma}{2}\right).$$

3. $F \supseteq \mathbb{Q}(\omega)$ *where, for some* $t \in \mathbb{Z}$, ω *is a fixed root of* $X^4 + (t^2 - kt + 2)X^3 + (-kt + 3t - k + 1)X^2 + (t - k + 2)X + 1 = 0$ *and*

$$x = -\omega^3 + (-t^2 + kt - 2)\omega^2 + (kt - 3t + k - 1)\omega + (-t + k - 2),$$
$$(t-1)y = -\omega^3 + (-t^2 + kt - 1)\omega^2 + (t^2 - 3t + k)\omega + (t - 2),$$
$$(t-1)z = t\omega^3 + (t^3 - kt^2 + 2t - 1)\omega^2 + (-kt^2 + 2t^2 + t - 1)\omega + t^2.$$

4. $F \supseteq \mathbb{Q}(\omega)$ *where, for some* $t \in \mathbb{Z} - \{1\}$, ω *is a fixed root of* $X^4 + (t^2 - kt - 2)X^3 + (kt - t + k + 1)X^2 - (t + k)X + 1 = 0$ *and*

$$x = -\omega^3 + (-t^2 + kt + 2)\omega^2 + (-kt + t - k - 1)\omega + (t + k),$$
$$(t-1)y = -\omega^3 + (-t^2 + kt + 1)\omega^2 + (-t^2 + t - k)\omega + t,$$
$$(t-1)z = t\omega^3 + (t^3 - kt^2 - 2t + 1)\omega^2 + (kt^2 + t - 1)\omega - t^2.$$

We note that letting $t = 0$ in part 1 of Theorem 3.1 recovers the solutions in Theorem 2.2. (These solutions can also be found using combinations of letting $t = k + 1$ in part 1, letting $t = 2$, -2, or $k - 1$ in part 2, or letting $t = k + 2$ or $k - 2$ in part 4.)

Proof of Theorem 3.1. Let F be a quartic field. Again, it is easy to verify that each of these is a solution with $x, y, z \in \mathcal{O}_F$, so we assume that $|\mathcal{E}_k(\mathbb{Q})| = 3$, with $(x, y, z) \in \mathcal{O}_F^3$ a solution.

Assume, first, that at least one of x, y, and z, say x, is of degree strictly less than four over $\mathbb{Q}$. Then, since x is a unit in the quartic ring $\mathcal{O}_F$, x is a root of $X^2 - tX + \varepsilon = 0$, with $t \in \mathbb{Z}$ and $\varepsilon = \pm 1$. So $1/x = \varepsilon(t - x)$. From the introduction, we see that y satisfies $y^2 + (x - k)y + 1/x = 0$ and thus

$$y = \frac{-x + k \pm \sqrt{(x-k)^2 - 4\varepsilon(t-x)}}{2}.$$

This yields the solutions in parts 1 and 2 of the theorem.

Now assume that x, y, and z are each of degree four over $\mathbb{Q}$. Let $P = (x_P, y_P)$ be a point in $\mathcal{E}_k(F)$ corresponding to the solution (x, y, z). Then x_P is also of degree four over $\mathbb{Q}$. Let $\mathcal{C} : dy = px^3 + qx^2 + rx + s$ be the unique cubic curve through P and its three conjugates, with $d, p, q, r, s \in \mathbb{Z}$, $d \neq 0$, and $\gcd(p, q, r, s, d) = 1$. Then the x-coordinates of the points of $\mathcal{E}_k \cap \mathcal{C}$ satisfy

$$d^2(1 - 2kx + k^2x^2 - 4x^3) = (px^3 + qx^2 + rx + s)^2,$$

which simplifies to

$$\begin{aligned}(6)\quad & p^2x^6 + 2pqx^5 + (2pr + q^2)x^4 + (2ps + 2qr + 4d^2)x^3 \\ & + (2qs + r^2 - k^2d^2)x^2 + (2rs + 2kd^2)x + (s^2 - d^2) = 0.\end{aligned}$$

Of the nine points in $\mathcal{E}_k \cap \mathcal{C}$, four are P and its conjugates, and at least three must be infinite. This leaves two points to be determined. Since the co-

efficients of (6) are rational, the set of solutions is closed under conjugation. Thus there are three cases to consider: at least one of the remaining two points is infinite, both points are finite and rational, or neither is rational.

If at least one of the additional points is infinite, then $p = 0$. Thus $x_P \in \mathcal{O}_F$ is a root of

$$q^2x^4 + (2qr + 4d^2)x^3 + (2qs + r^2 - k^2d^2)x^2 + (2rs + 2kd^2)x + (s^2 - d^2) = 0.$$

Since x_P is an algebraic integer of norm 1, each coefficient is divisible by q^2 and $q^2 = s^2 - d^2$. Suppose that ℓ is a prime factor of $\gcd(q, d)$. Then $\ell \,|\, s$ and, since $q^2 \,|\, (2qs + r^2 - k^2d^2)$, $\ell \,|\, r$. Since $p = 0$, we see that $\ell \,|\, \gcd(p, q, r, s, d)$, a contradiction. Thus $\gcd(q, d) = 1$. Now, since $q^2 \,|\, (2qr + 4d^2)$, we find that $q \,|\, 4d^2$, and hence $q \,|\, 4$.

If $q = \pm 1$ or ± 2, then $q^2 = s^2 - d^2$ and $d \neq 0$ yield a contradiction. So $q = \pm 4$ and, thus, $s = \pm 5$ and $d = \pm 3$. But then $q^2 \,|\, (2qr + 4d^2)$ implies that $16 \,|\, (\pm 8r + 36)$, a contradiction. Hence neither of the additional points in the intersection is infinite.

If one of the two additional points is $(0, 1)$, the other cannot be $(0, -1)$, since these points cannot both be on $\mathcal{C}$. So if the two additional points are rational, there is a double point at $(0, 1)$ or $(0, -1)$. If the double point is at $(0, 1)$, then since $(0, 1)$ is on $\mathcal{C}$, we have $d = s$. Removing the extra factor of x and making this substitution in (6) yields

$$\begin{aligned} &p^2x^5 + 2pqx^4 + (2pr + q^2)x^3 \\ &\qquad + (2ps + 2qr + 4s^2)x^2 + (2qs + r^2 - k^2s^2)x + (2rs + 2ks^2) = 0. \end{aligned}$$

The second root at 0 then implies that $2rs + 2ks^2 = 0$ and so $r = -ks$. Making this substitution and removing the extra factor of x, we are left with

$$p^2x^4 + 2pqx^3 + (q^2 - 2pks)x^2 + (2ps - 2qks + 4s^2)x + 2qs = 0. \tag{7}$$

Since x_P is an algebraic integer of norm 1, each coefficient is divisible by p^2 and $p^2 = 2qs$. Suppose that ℓ is a prime factor of s. Then $\ell \mid p$ and so, since $p^2 \mid (q^2 - 2pks)$, $\ell \mid q$. But $d = s$ and $r = -ks$ then imply that $\ell \mid \gcd(p, q, r, s, d)$, a contradiction. Hence $s = \pm 1$. Without loss of generality, assume that $s = 1$.

It follows that $p^2 = 2q$, so $2 \,|\, p$ and $p \,|\, q$. Then, since $p^2 \,|\, (2p - 2qk + 4)$, we find that $p \,|\, 4$. Thus $p = \pm 2$ or ± 4.

If $p = \pm 4$, then $q = 8$, and since $p^2 \,|\, (2p - 2qk + 4)$, we have $16 \,|\, (12 - 16k)$ or $16 \,|\, (-4 - 16k)$, each a contradiction.

If $p = 2$, then, by equation (7), the minimal polynomial for x_P is $x^4 + 2x^3 + (1 - k)x^2 + (2 - k)x + 1$ and, from the equation for $\mathcal{C}$, we have $y_P = 2x_P^3 + 2x_P^2 - kx_P + 1$. This yields the solution in part 3 of

the theorem with $t = 0$. If $p = -2$, then the minimal polynomial for x_P is $x^4 - 2x^3 + (k+1)x^2 - kx + 1$ and $y_P = -2x_P^3 + 2x_P^2 - kx_P + 1$. This yields the solution in part 4 with $t = 0$.

As before, if instead the double root is at $(0, -1)$, then the same solutions (up to permutation) are obtained.

Finally, suppose that neither additional point is rational. Since the points are on the curve $\mathcal{C}$, this implies that the x-coordinates of the points are not rational. Since the two points must be conjugates, the x-coordinates satisfy an irreducible quadratic polynomial with rational integer coefficients. By Lemma 2.1, the quadratic polynomial has the form $x^2 + t(t-k)x + t = 0$ for some $t \in \mathbb{Q} - \{0\}$.

Recalling that x_P is of degree four over $\mathbb{Q}$, let $a, b, c \in \mathbb{Z}$ be such that $x^4 + ax^3 + bx^2 + cx + 1$ is the minimal polynomial of x_P over $\mathbb{Q}$. Then equation (6) factors as

$$p^2(x^2 + t(t-k)x + t)(x^4 + ax^3 + bx^2 + cx + 1) = 0. \tag{8}$$

By Gauss's lemma, since the other coefficients are integers, the coefficients of $p^2(x^2 + t(t-k)x + t)$ must also be integers. So $p^2t(t-k) \in \mathbb{Z}$ and $p^2t \in \mathbb{Z}$. Since $k \in \mathbb{Z}$, we have $p^2tk \in \mathbb{Z}$, and so $p^2t^2 \in \mathbb{Z}$. Since $t \in \mathbb{Q}$ and $p \in \mathbb{Z}$, this implies that $pt \in \mathbb{Z}$ and thus $t = n/p$ for some $n \in \mathbb{Z} - \{0\}$. Making this substitution, expanding (8), and equating coefficients with those in (6), we have:

$$2pq = p^2a + n(n - pk), \tag{9}$$

$$2pr + q^2 = p^2b + n(n - pk)a + np, \tag{10}$$

$$2ps + 2qr + 4d^2 = p^2c + n(n - pk)b + npa, \tag{11}$$

$$2qs + r^2 - k^2d^2 = p^2 + n(n - pk)c + npb, \tag{12}$$

$$2rs + 2kd^2 = n(n - pk) + npc, \tag{13}$$

$$s^2 - d^2 = np. \tag{14}$$

Suppose that ℓ is a prime dividing p. Equations (9) and (10) imply that $\ell \,|\, n$ and $\ell \,|\, q$, respectively, and (11) implies that $\ell \,|\, 4d^2$. If $\ell \,|\, d^2$, then $\ell \,|\, d$, and by (12) and (14), we find that $\ell \,|\, r$ and $\ell \,|\, s$. But then $\ell \,|\, (p, q, r, s, d)$, a contradiction. Thus $(p, d) = 1$ and $\ell \,|\, 4$, implying that $\ell = 2$. Hence $p = \pm 2^m$ for some $m \geq 0$.

If $4 \,|\, p$, then (9) implies that $8 \,|\, n^2$ and so $4 \,|\, n$. Equation (10) then implies $4 \,|\, q$, and from (11), we find that $2 \,|\, d$, a contradiction. Thus $p = \pm 1, \pm 2$. Without loss of generality, assume $p > 0$.

Now, since $p = 1$ or 2, equation (9) implies that $p \,|\, n$ and thus $t = n/p \in \mathbb{Z}$. Then, by equation (14),

$$d^2 = s^2 - p^2t. \tag{15}$$

Replacing n by pt and eliminating d^2 from (9) through (13), we have

$$2q = pa + pt(t-k), \tag{16}$$

$$2pr + q^2 = p^2b + p^2t(t-k)a + p^2t, \tag{17}$$

$$2ps + 2qr + 4(s^2 - p^2t) = p^2c + p^2t(t-k)b + p^2ta, \tag{18}$$

$$2qs + r^2 - k^2(s^2 - p^2t) = p^2 + p^2t(t-k)c + p^2tb, \tag{19}$$

$$2rs + 2k(s^2 - p^2t) = p^2t(t-k) + p^2tc. \tag{20}$$

Using (16) to eliminate q and (20) to eliminate r in (17) through (19), then simplifying, we obtain

$$\begin{aligned} psa^2 - 4psb - 8ks^2 + 4p^2tc + 4kp^2t - 4pst + 2psta(k-t) \\ + 4p^2t^2 + k^2pst^2 - 2kpst^3 + pst^4 = 0, \end{aligned} \tag{21}$$

$$\begin{aligned} 2p^2sc - 4ps^2 + 2kps^2a - 8s^3 - p^3tac - kp^3ta + 8p^2st + 2p^2sta \\ -2kp^2stb - 2k^2ps^2t - p^3t^2a + kp^3t^2c + k^2p^3t^2 \\ +2p^2st^2b + 2kps^2t^2 - p^3t^3c - p^3t^4 = 0, \end{aligned} \tag{22}$$

$$\begin{aligned} 4ps^2 - 4s^3a + 4ps^2tb + 4ks^3t - p^3t^2c^2 - 2kp^3t^2c - k^2p^3t^2 \\ + 4ps^2t^2c + 4kps^2t^2 - 4s^3t^2 - 2p^3t^3c - 2kp^3t^3 - p^3t^4 = 0. \end{aligned} \tag{23}$$

Next, multiplying (22) by $2t$ and (23) by pt, then using (21) to eliminate b in each and letting

$$A = -2s + pta - pt^2(t-k) \tag{24}$$

and

$$C = p^2c + kp^2 - 2ps - 2s^2 + p^2t \tag{25}$$

yields

$$s(t-k)A^2 - 2tAC + 4s(3t-k)(p^2t - s^2) = 0 \tag{26}$$

and

$$s^2A^2 - t^3C^2 + 4s^2(t^3-1)(s^2 - p^2t) = 0. \tag{27}$$

Recalling that $s^2 - p^2t = d^2$ and using (26) to eliminate C in (27) yields

$$s^2(A^2 - 4d^2)\big((4 - t(t-k)^2)A^2 + 4td^2(3t-k)^2\big) = 0. \tag{28}$$

At least one of the three factors of the left-hand side must be zero. We consider each, beginning with the second.

If $A^2 - 4d^2 = 0$, then $A = 2d\varepsilon$ for some fixed $\varepsilon = \pm 1$. Combining this with (15) and (26), recalling that $t \neq 0$, yields $C = -2sd\varepsilon$, and combining with (24) yields

$$pta = 2d\varepsilon + 2s + pt^2(t-k). \tag{29}$$

Set $\alpha = s - d\varepsilon$. Then $\alpha(s + d\varepsilon) = s^2 - d^2 = p^2t$, by (15). Equation (17) implies that $p \,|\, q$, so there exists $v \in \mathbb{Z}$ such that $pv = q$. Noting that,

by (29), $pt^2(t-k) = pta - 2d\varepsilon - 2s$ and combining this with (16), then multiplying by α, we get $\alpha a = p + \alpha v$. Thus, $\alpha \mid p$.

Clearly, if $p = 1$, $\alpha = \pm 1$. If $p = 2$, then (15) implies that $s \equiv d \pmod 2$, and so $\alpha = s - d\varepsilon$ is even. Thus $\alpha \mid p$ implies that $\alpha = \pm 2$. So in either case, $\alpha = \pm p$. Let $\beta = \pm 1$ be such that

$$\alpha = \beta p.$$

Now, since $\alpha(s + d\varepsilon) = p^2 t$, $s + d\varepsilon = \beta pt$, and so $s = \beta pt - d\varepsilon = \beta pt + \beta p - s$. Thus, $2s = \beta p(t+1)$. Combining $C = -2sd\varepsilon$ with (25), we have

$$cp^2 = 2s(p + s - d\varepsilon) - (k+t)p^2.$$

Using $2s = \beta p(t+1)$ and $s - d\varepsilon = \beta p$, $c = \beta t - k + \beta + 1$. From (29), using $s + d\varepsilon = \beta pt$, $a = t^2 - kt + 2\beta$. Simplifying (21), eliminating a, c, and s, yields $b = t - \beta kt + 2\beta t - k\beta + 1$.

Thus, if $\beta = 1$, we have $(a, b, c) = (t^2 - kt + 2, -kt + 3t - k + 1, t - k + 2)$, which yields the remaining solutions in part 3 of the theorem; and, if $\beta = -1$, we have $(a, b, c) = (t^2 - kt - 2, kt - t + k + 1, -(t + k))$, which yields the remaining solutions in part 4. (In these parts of the theorem, we disallow the value $t = 1$, which would duplicate the solution in part 2 with $t = k - 1$. Further, although $t \neq 0$ at this stage of the proof, the solutions corresponding to $t = 0$ were derived earlier.)

Alternatively, suppose that the first factor of (28) is zero and the second is not, that is, $s^2 = 0$ and $A^2 - 4d^2 \neq 0$. Then $s = 0$ and, by (15), $d^2 = -p^2 t$. If $p = 2$, then this implies that $2 \mid d$. But then, by (17), $2 \mid q$ and, by (19), $2 \mid r$. So $2 \mid \gcd(p, q, r, s, d)$, which is a contradiction. Thus, $p = 1$.

We can now simplify equations (16) through (20) with $s = 0$ and $p = 1$, and eliminate q from (17) and (18), using (16). This leaves us with

$$8r + (a + t(t-k))^2 = 4b + 4t(t-k)a + 4t, \tag{30}$$

$$r(a + t(t-k)) - 4t = c + t(t-k)b + ta, \tag{31}$$

$$r^2 + k^2 t = 1 + t(t-k)c + tb, \tag{32}$$

$$-k = t + c. \tag{33}$$

Using (30) and (33) to eliminate b and c in (31) yields

$$4r(a - t(t-k)) = t^3(t-k)^3 - 2at^2(t-k)^2 - t(t-k)(4t - a^2) - 4(k - 3t - at).$$

Now, if $a - t(t-k) = 0$, then (30) simplifies to $b = 2r - t$ and therefore (32) becomes $r^2 + t^3 = (2r - t)t + 1$. Since $t = -d^2$, this is equivalent to $(r - t)^2 - (d^3)^2 = 1$, which is impossible, since $d \neq 0$. So $a - t(t-k) \neq 0$ and thus

$$r = \frac{t^3(t-k)^3 - 2at^2(t-k)^2 - t(t-k)(4t - a^2) - 4(k - 3t - at)}{4(a - t(t-k))}. \tag{34}$$

Using (30), (33), and (34) to eliminate b, c, and r in (32) yields

$$(35) \qquad (t(a-t(t-k))^2+4)\big((t(t-k)^2-4)(a-t(t-k))^2+4(3t-k)^2\big) = 0.$$

If the first factor of (35) is zero, then $-t(a - t(t - k))^2 = 4$. Using (24) with $s = 0$, $p = 1$, and $d^2 = -t$, we have $A^2 = t^2(a - t(t - k))^2 = 4d^2$, contrary to assumption.

Thus the second factor of (35) is zero, and so

$$(4 - t(t - k)^2)(a - t(t - k))^2 = (2(3t - k))^2.$$

Hence, $4 - t(t - k)^2$ is a square. Recalling $d^2 = -t$, we conclude that $4 + (d(d^2 + k))^2$ is a square, and therefore $d(d^2 + k) = 0$. Hence, since $d \neq 0$, we have $k = -d^2$. But then, by (3), $|\mathcal{E}_k(\mathbb{Q})| > 3$, contrary to assumption.

Finally, returning to (28), suppose that the last factor in the product is zero, while neither of the first two factors is zero. Then

$$(36) \qquad (4 - t(t - k)^2)A^2 + 4td^2(3t - k)^2 = 0.$$

If $A = 0$, then, using $d^2 = s^2 - p^2t$, equation (27) simplifies to $t^3C^2 = 4s^2d^2(t^3-1)$. It follows that $t(t^3-1)$ is a square, and therefore t and t^3-1, being relatively prime, are both squares. Letting $t = j^2$, we have that $(j^3)^2 - 1$ is a square. Thus $j^3 = \pm 1$, and so $j = \pm 1$ and $t = 1$. Now, since $A = 0$, equation (36) implies that $4td^2(3t - k)^2 = 0$ and therefore $k = 3t = 3$, also contrary to assumption.

Thus $A \neq 0$ and so, since $t \neq 0$, equation (36) is equivalent to

$$1 - 2kt^{-1} + k^2t^{-2} - 4t^{-3} = (2d(3t - k)A^{-1}t^{-1})^2.$$

It follows that $(t^{-1}, 2d(3t - k)A^{-1}t^{-1})$ is a finite rational point on $\mathcal{E}_k$. But this implies that $t^{-1} = 0$, which is clearly impossible.

Therefore, there are no solutions other than those given in the statement of the theorem. ∎

Acknowledgements. Research of the first-named author was supported by the Faculty Research Fund of Bryn Mawr College.

Research of the second-named author was supported by Faculty Development Grants of Merrimack College.

References

[1] A. Bremner, *The equation $xyz = x + y + z = 1$ in integers of a cubic field*, Manuscripta Math. 65 (1989), 479–487.

[2] A. Bremner, *The equation $xyz = x + y + z = 1$ in integers of a quartic field*, Acta Arith. 57 (1991), 375–385.

[3] J. W. S. Cassels, *On a diophantine equation*, Acta Arith. 6 (1960), 47–52.

[4] H. G. Grundman and L. L. Hall, *New solutions to $xyz = x + y + z = 1$ in integers of quartic fields*, Acta Arith. 112 (2004), 405–409.

[5] H. G. Grundman and L. L. Hall, *Solutions to $xyz = 1$ and $x+y+z = k$ in algebraic integers of small degree, II*, preprint.

[6] H. G. Grundman and L. L. Hall-Seelig, *Solutions to $xyz = x + y + z = 1$ in quintic number rings*, Congr. Numer. 194 (2009), 129–135.

[7] R. Mollin, C. Small, K. Varadarajan and P. G. Walsh, *On unit solutions of the equation $xyz = x + y + z$ in the ring of integers of a quadratic field*, Acta Arith. 48 (1987), 341–345.

[8] W. Sierpiński, *Remarques sur le travail de M. J. W. S. Cassels 'On a diophantine equation'*, Acta Arith. 6 (1961), 469–471.

[9] E. Thomas and A. T. Vasquez, *A family of elliptic curves and cyclic cubic field extensions*, Math. Proc. Cambridge Philos. Soc. 96 (1984), 39–43.

[10] L.-C. Zhang and J. Gordon, *On unit solutions of the equation $xyz = x + y + z$ in a number field with unit group of rank 1*, Acta Arith. 57 (1991), 155–158.

H. G. Grundman
Department of Mathematics
Bryn Mawr College
Bryn Mawr, PA 19010, U.S.A.
E-mail: grundman@brynmawr.edu

L. L. Hall-Seelig
Department of Mathematics
Merrimack College
North Andover, MA 01845, U.S.A.
E-mail: hallseeligl@merrimack.edu

Received on 3.8.2013
and in revised form on 19.10.2013 (7542)