ACTA ARITHMETICA
171.3 (2015)

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

by

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

1. Introduction. We continue our study, initiated in [3], of the system of equations

$$(1) \qquad xyz = 1 \quad \text{and} \quad x + y + z = k,$$

with $k \in \mathbb{Z}$ and x, y, z algebraic integers in a field of degree at most four over $\mathbb{Q}$. Easily, the only solutions with $x, y, z \in \mathbb{Q}$ are $(1, 1, 1)$ for $k = 3$ and $(1, -1, -1)$ and its permutations for $k = -1$. In [3], we define, for each $k \neq 3$, the related elliptic curve

$$(2) \qquad \mathcal{E}_k : \ Y^2 = 1 - 2kX + k^2X^2 - 4X^3,$$

and determine all solutions to the system (1) with $k \in \mathbb{Z}$ such that $|\mathcal{E}_k(\mathbb{Q})| = 3$.

In this work, we extend the results to include $k = -1$ and $k = 5$, and prove that this, then, solves the problem for all k with $\mathcal{E}_k(\mathbb{Q})$ finite. (Note that $k = 3$ is excluded from consideration since, for each $t \in \mathbb{Q}$, the point $(-t(t + 1), t^3 + (t + 1)^3)$ is in $\mathcal{E}_3(\mathbb{Q})$, and thus $\mathcal{E}_3(\mathbb{Q})$ is infinite.)

We begin with notation and some basic results from [3] and from Bremner's paper [2] that inspired this work. Let F be an algebraic number field with $[F : \mathbb{Q}] \leq 4$. 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). Without loss of generality (permuting, if necessary), assume that x is of norm 1. As explained in [3], letting $x_P = 1/x$ and $y_P = \pm\sqrt{1 - 2k/x + k^2/x^2 - 4/x^3}$ (choosing either square root) yields a point $P = (x_P, y_P)$ on the curve (2), 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, letting

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

DOI: 10.4064/aa171-3-4

$$\begin{aligned} x &= 1/x_P, \\ y &= (k - 1/x_P + y_P/x_P)/2, \\ z &= (k - 1/x_P - y_P/x_P)/2 \end{aligned} \tag{3}$$

yields a solution (x, y, z) to (1), with $x, y, z \in \mathcal{O}_F$ and x a unit of norm 1.

As usual, two solutions given by permuting coordinates are considered to be equivalent. Recall from [3] that the automorphism $\varphi : \mathcal{E}_k(F) \to \mathcal{E}_k(F)$ defined by $\varphi(X, Y) = (X, -Y)$ fixes equivalence classes of solutions to (1).

In Section 2, we prove that for $k \in \mathbb{Z}$, if $\mathcal{E}_k(\mathbb{Q})$ is finite, but not of order 3, then $k \in \{-1, 5\}$. Thus, since [3] settled the case $|\mathcal{E}_k(\mathbb{Q})| = 3$, in order to completely solve the problem for all k with $\mathcal{E}_k(\mathbb{Q})$ finite, it suffices to consider only the cases with $k \in \{-1, 5\}$.

In Section 3, we find all solutions to the system of equations (1) with $(x, y, z) \in \mathcal{O}_F^3$ where $[F : \mathbb{Q}] \leq 3$ and $k \in \{-1, 5\}$. Finally, in Section 4, we solve the case where $[F : \mathbb{Q}] = 4$. In each of these sections, we again follow the ideas set out by Bremner [2], but we focus on what is different from the cases addressed in [3], quoting results from that work instead of reproving what is already known.

2. $\mathcal{E}_k(\mathbb{Q})$ finite, but $|\mathcal{E}_k(\mathbb{Q})| \neq 3$. A direct calculation using Magma [1] shows that

$$\mathcal{E}_{-1}(\mathbb{Q}) = \{\mathfrak{O}, (0, 1), (0, -1), (-1, 2), (-1, -2), (1, 0)\}, \tag{4}$$

$$\mathcal{E}_5(\mathbb{Q}) = \{\mathfrak{O}, (0, 1), (0, -1), (2, 7), (2, -7), (1/4, 0)\}. \tag{5}$$

In this section, we prove the following theorem.

Theorem 2.1. *Let $k \in \mathbb{Z} - \{-1, 5\}$. Then $\mathcal{E}_k(\mathbb{Q})$ is infinite or $|\mathcal{E}_k(\mathbb{Q})| = 3$.*

Proof. Let $k \in \mathbb{Z} - \{-1, 5\}$ be such that $\mathcal{E}_k(\mathbb{Q})$ is finite. Since, as noted in the introduction, this means that $k \neq 3$, $\mathcal{E}_k$ is an elliptic curve. Beginning with equation (2), we multiply by 16 and substitute $-X/4$ for X and $Y/4$ for Y to obtain

$$\mathcal{E}_k^* : \ Y^2 = 16 + 8kX + k^2X^2 + X^3. \tag{6}$$

Clearly $\mathcal{E}_k^*(\mathbb{Q}) \cong \mathcal{E}_k(\mathbb{Q})$ and so $\mathcal{E}_k^*(\mathbb{Q})$ is finite.

Note that $S_k^* = \{(0, 4), (0, -4), \mathfrak{O}\}$ is a cyclic subgroup of $\mathcal{E}_k^*(\mathbb{Q})$ and thus $3 \mid |\mathcal{E}_k^*(\mathbb{Q})|$. By Mazur's theorem, it follows that $|\mathcal{E}_k^*(\mathbb{Q})| \in \{3, 6, 9, 12\}$.

Suppose there is a point of order 2 in $\mathcal{E}_k^*(\mathbb{Q})$, say (x, y). Then $y = 0$ and so $16 + 8kx + k^2x^2 + x^3 = 0$. By the Nagell–Lutz theorem, $x \in \mathbb{Z}$ and so $x \mid 16$. Evaluating at each factor of 16 and solving for k, we get values of k not in $\mathbb{Z}$, except when $x = -1$ and $x = -4$, for which k is 3 or 5 and 3 or -1, respectively. Since these values of k have been excluded, we see that $\mathcal{E}_k^*(\mathbb{Q})$ has no points of order 2. Thus $|\mathcal{E}_k^*(\mathbb{Q})| \in \{3, 9\}$.

Suppose that $|\mathcal{E}_k^*(\mathbb{Q})| \neq 3$. Then, again by Mazur's theorem, $\mathcal{E}_k^*(\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$. Let $P = (x, y) \in \mathcal{E}_k^*(\mathbb{Q})$ be a point of order 9. Since S_k^* is the only subgroup of $\mathcal{E}_k^*(\mathbb{Q})$ of order 3, we have $3P \in \{(0, 4), (0, -4)\}$. So, letting $3P = (x_3, y_3)$ yields that $x_3 = 0$.

Since P is of order 9, we know that P is a finite point with $x \neq 0$ (otherwise P is of order 3) and $y \neq 0$ (otherwise P is of order 2). Using the duplication and addition formulas, we find that $x_3 = 0$ if and only if either

$$64 + 16kx - 12x^2 - 4kx^2 + x^3 = 0$$

or

$$\begin{aligned} 4096 + 2048kx + 768x^2 + 256kx^2 + 256k^2x^2 + 128x^3 + 192kx^3 \\ + 64k^2x^3 + 144x^4 - 16kx^4 + 16k^2x^4 + 12x^5 + 4kx^5 + x^6 = 0. \end{aligned}$$

Again, since $x \in \mathbb{Z}$, there are a finite number of possible x-values for each equation. Checking each possible x-value in the first equation and solving for k, we find no values for k in $\mathbb{Z}$, a contradiction. Doing the same for the second equation, we find values for k that are not in $\mathbb{Z}$, except for $x = -4$, for which we get $k = 3$. Thus in no case under consideration do we get a point of order 9.

Hence $\mathcal{E}_k^*(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$, and therefore $\mathcal{E}_k(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. ∎

3. Solutions with $[F : \mathbb{Q}] \leq 3$. We begin by finding all elements of $\mathcal{E}_k(F)$ for F a quadratic number field and $k \in \mathbb{Z}$ with $\mathcal{E}_k(\mathbb{Q})$ finite. This result will be used in the proofs of both Theorem 3.1 and Theorem 4.2. The first two parts of the following lemma are from [3, Lemma 1], where it is shown that, if $|\mathcal{E}_k(\mathbb{Q})| = 3$, then these are the only solutions. Thus, by Theorem 2.1, the only possible additional solutions are for $k = -1$ or $k = 5$.

3.1. Solutions with $[F : \mathbb{Q}] = 2$

LEMMA 3.1. *Let $k \in \mathbb{Z}$ be such that $\mathcal{E}_k(\mathbb{Q})$ is finite and let $[F : \mathbb{Q}] = 2$. If $P = (x_P, y_P) \in \mathcal{E}_k(F)$ is a finite point, then, for some $t \in \mathbb{Q}$, at least one of the following holds:*

(i) *$x_P = t$ and $\pm y_P = \sqrt{1 - 2kt + k^2t^2 - 4t^3}$;*
(ii) *$x_P^2 + t(t - k)x_P + t = 0$ and $\pm y_P = (2t - k)x_P + 1$;*
(iii) *$k = -1$ and either*

(a) *$x_P^2 + (t^2 - t - 1)x_P + t(t + 1) = 0$ and $\pm y_P = (2t - 1)x_P + (2t + 1)$, $t \neq 0, -1$, or*
(b) *$x_P^2 + (t^2 - t + 1)x_P - t(t - 1) = 0$ and $\pm y_P = (2t - 1)x_P - (2t - 1)$, $t \neq 0, 1$;*

(iv) $k = 5$ *and either*

(a) $x_P^2+(t^2+3t-2)x_P-t(2t-1) = 0$ *and* $\pm y_P = (2t+3)x_P-(4t-1)$, $t \neq 0, 1/2$, *or*

(b) $x_P^2+(t^2-6)x_P-(t^2/4-1) = 0$ *and* $\pm y_P = 2tx_P-t/2$, $t \neq \pm 2$.

The proof is similar in form to that of [3, Lemma 1], so we omit many details, particularly where there is overlap.

Proof. If $x_P \in \mathbb{Q}$, then it is immediate that (i) holds. So we 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 let $\mathcal{L}$ be the line passing through P and $\overline{P}$. Since $\mathcal{L}$ is fixed under conjugation over $\mathbb{Q}$, the coefficients of its equation are rational. Let Q be the third point in $\mathcal{E}_k \cap \mathcal{L}$. Then $Q \in \mathcal{E}_k(\mathbb{Q})$ and, since $x_P \notin \mathbb{Q}$, Q is a finite point.

If $Q = (0,1)$ or $(0,-1)$, we get the solutions in (ii). The only other possibilities are when $k = -1$, in which case, by equation (4), we have $Q = (-1,\pm 2)$ or $Q = (1,0)$, and when $k = 5$, in which case, by equation (5), we have $Q = (2,\pm 7)$ or $Q = (1/4, 0)$.

If $k = -1$ and $Q = (-1,2)$, the x-coordinates of the points of $\mathcal{E}_{-1} \cap \mathcal{L}$ satisfy the equation $1 + 2x + x^2 - 4x^3 = (mx + m + 2)^2$ for some $m \in \mathbb{Q}$. Simplifying and removing the factor of $x + 1$, we find that x_P satisfies $4x^2 + (m^2 - 5)x + m^2 + 4m + 3 = 0$. Letting $m = 2t - 1$ yields (iii)(a). The case $Q = (-1,-2)$ yields these same solutions, up to equivalence.

Similarly, if $k = -1$ and $Q = (1,0)$, we get the equation $1+2x+x^2-4x^3 = (mx-m)^2$ for some $m \in \mathbb{Q}$, and so $4x^2+(m^2+3)x+(-m^2+1) = 0$. Again letting $m = 2t - 1$, we get (iii)(b).

Following the same method, if $k = 5$ and $Q = (2,7)$, the x-coordinates of the points of $\mathcal{E}_{-1} \cap \mathcal{L}$ satisfy $1 - 10x + 25x^2 - 4x^3 = (mx - 2m + 7)^2$ for some $m \in \mathbb{Q}$. Letting $m = 2t + 3$ leads to (iv)(a). If $k = 5$ and $Q = (2,-7)$, we obtain a permutation of (iv)(a), and if $k = 5$ and $Q = (1/4, 0)$, then (iv)(b) follows. ■

We now use Lemma 3.1 to find all solutions to (1) in rings of integers of quadratic number fields.

Theorem 3.1. *Let $k \in \mathbb{Z}$ be such that $\mathcal{E}_k(\mathbb{Q})$ is finite and let $[F : \mathbb{Q}] = 2$. The equations $x + y + z = k$ and $xyz = 1$ have simultaneous solutions (x,y,z) with $x,y,z \in \mathcal{O}_F$ in exactly the following instances, allowing for permutations of x,y,z:*

(i) $F = \mathbb{Q}(\nu)$ *with* $\nu^2 = k^2 - 2k - 3$, *and*

$$(x,y,z) = (1,(k-1+\nu)/2,(k-1-\nu)/2);$$

(ii) $F = \mathbb{Q}(\nu)$ *with* $\nu^2 = k^2 + 2k + 5$, *and*

$$(x,y,z) = (-1,(k+1+\nu)/2,(k+1-\nu)/2);$$

(iii) $k = 5$, $F = \mathbb{Q}(\sqrt{2})$, *and*

(a) $(x, y, z) = (3 + 2\sqrt{2}, 1 - \sqrt{2}, 1 - \sqrt{2})$, *or*

(b) $(x, y, z) = (3 - 2\sqrt{2}, 1 + \sqrt{2}, 1 + \sqrt{2})$.

Proof. It is easy to verify that each of these is a solution. Further, for $k \notin \{-1, 5\}$, Theorem 2.1 and [3, Theorem 2.2] show that (i) and (ii) give all of the solutions. Thus, we assume that $(x, y, z) \in \mathcal{O}_F^3$ is a solution to (1), with corresponding point $P = (x_P, y_P) \in \mathcal{E}_k$, and that $k = -1$ or $k = 5$.

If one of x, y, z, say x, is rational, then $x_P = x = \pm 1$ and so $y_P = \pm\sqrt{k^2 - 2k - 3}$ or $\pm\sqrt{k^2 + 2k + 5}$, yielding (i) and (ii). So now we assume that none of x, y, z is rational and, without loss of generality, that $N_F(x) = 1$.

Note that P must have one of the forms given in (ii)–(iv) of Lemma 3.1. If P is of the form in Lemma 3.1(ii), then $t = 1$ and a direct calculation yields that $y = 1$ or $z = 1$, a contradiction. If P is as given in Lemma 3.1(iii) or (iv)(a), it is impossible to have both $N(x_P) = 1$ and $t \in \mathbb{Q}$.

Finally, if P is as given in 3.1(iv)(b), then $k = 5$ and, since $N(x_P) = 1$, we have $t = 0$. So $x_P^2 - 6x_P + 1 = 0$ and $y_P = 0$, yielding the solutions in part (iii) of the theorem. ■

3.2. Solutions with $[F : \mathbb{Q}] = 3$. Our results of this case are summarized in the following theorem.

Theorem 3.2. *Let $k \in \mathbb{Z}$ be such that $\mathcal{E}_k(\mathbb{Q})$ is finite and let $[F : \mathbb{Q}] = 3$. The equations $x + y + z = k$ and $xyz = 1$ have simultaneous solutions (x, y, z) with $x, y, z \in \mathcal{O}_F$ in exactly the following instances, allowing for permutations of x, y, z:*

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

$$(x, y, z) = (\mu^2 - (k + 1)\mu + (k + 2), \mu - 1, -\mu^2 + k\mu - 1);$$

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

$$(x, y, z) = (\mu^2 + (k + 3)\mu + k, -\mu - 1, -\mu^2 - (k + 2)\mu + 1);$$

(iii) *for* $k = -1$,

(a) $(x, y, z) = (1, -1, -1)$;

(b) $F = \mathbb{Q}(\rho)$ *with ρ a fixed root of* $X^3 + 9X^2 - X - 1 = 0$, *and*

$$(x, y, z) = (\rho^2 + 9\rho - 1, -(\rho^2 + 10\rho + 3)/2, -(\rho^2 + 8\rho - 3)/2);$$

(iv) *for* $k = 5$,

(a) $F = \mathbb{Q}(\sigma)$ *with σ a fixed root of* $X^3 - 6X^2 + 5X - 1 = 0$, *and*

$$(x, y, z) = (\sigma^2 - 6\sigma + 5, -2\sigma^2 + 11\sigma - 3, \sigma^2 - 5\sigma + 3);$$

(b) $F = \mathbb{Q}(\sigma)$ *with σ a fixed root of* $X^3 + 4X^2 - X - 1 = 0$, *and*

$$(x, y, z) = (\sigma^2 + 4\sigma - 1, -2\sigma^2 - 7\sigma + 5, \sigma^2 + 3\sigma + 1).$$

Proof. As before, it is straightforward to verify that each of these is a solution. If $x, y, z \in \mathbb{Q}$, then, since $k \neq 3$, the solution in (iii)(a) follows. As in the proof of [3, Theorem 2.3], we can thus assume that $(x, y, z) \in \mathcal{O}_F^3$ is a solution with $x, y, z \in F - \mathbb{Q}$ and $N_F(x) = 1$.

Again, let $P = (x_P, y_P)$ be the point on $\mathcal{E}_k$ corresponding to the solution (x, y, z). Let $\mathcal{C} : dy = px^2 + qx + r$ be the quadratic curve going through P and its two conjugates, with $d, p, q, r \in \mathbb{Z}$, $d \neq 0$, and $\gcd(d, p, q, r) = 1$. Then the x-coordinates of the points of $\mathcal{E}_k(F) \cap \mathcal{C}$ satisfy

$$p^2x^4+(2pq+4d^2)x^3+(2pr+q^2-k^2d^2)x^2+(2qr+2kd^2)x+(r^2-d^2) = 0. \tag{7}$$

The six elements of $\mathcal{E}_k(F) \cap \mathcal{C}$ are P, its two other conjugates, two infinite points, and another point, Q. Since Q is fixed under conjugation, its coordinates are rational. As shown in the proof of [3, Theorem 2.3], if $Q \in S = \{\mathfrak{O}, (0, 1), (0, -1)\}$, we find the solutions in (i) and (ii) of this theorem. It remains to consider each of the remaining points in $\mathcal{E}_k(\mathbb{Q})$ for $k = -1$ and 5. Assume without loss of generality that $p > 0$.

- If $k = -1$ and $Q = (-1, \pm 2)$, evaluating equation (7) at $x = -1$ yields

$$p^2 - 2pq + 2pr + q^2 - 2qr + r^2 - 4d^2 = 0. \tag{8}$$

Removing the factor of $x + 1$ from (7), we find that x_P is a root of $p^2x^3 + (-p^2 + 2pq + 4d^2)x^2 + (p^2 - 2pq + 2pr + q^2 - 5d^2)x + (-p^2 + 2pq - 2pr - q^2 + 2qr + 3d^2) = 0$. Since x_p is an algebraic integer of norm 1, we have

$$p^2 \mid (-p^2 + 2pq + 4d^2), \tag{9}$$

$$p^2 \mid (p^2 - 2pq + 2pr + q^2 - 5d^2), \tag{10}$$

$$p^2 = -(-p^2 + 2pq - 2pr - q^2 + 2qr + 3d^2). \tag{11}$$

Combining (8) and (11) yields

$$p^2 + r^2 - d^2 = 0. \tag{12}$$

Suppose, for a contradiction, that $p \neq 1$. Let ℓ be a prime factor of p. If $\ell \mid d$, then by (10), $\ell \mid q$ and so by (8), $\ell \mid r$. But this contradicts the fact that $\gcd(d, p, q, r) = 1$. So $\ell \nmid d$. Thus, by (9), $p \mid 4$ and so $\ell = 2$. Further, since $\ell = 2$ does not divide d, (9) implies that $p \neq 4$. Hence, $p = 2$. Since d is odd, considering (12) modulo 8 yields a contradiction.

Therefore, $p = 1$ and, by (12), $r = 0$ and $d = \pm 1$. From (11), $q^2 - 2q - 3 = 0$. If $q = -1$, then x_P is rational, a contradiction. So $q = 3$ and the solution in (iii)(b) follows.

- If $k = -1$ and $Q = (1, 0)$, then evaluating (7) at $x = 1$ gives us

$$p^2 + 2pq + 2pr + q^2 + 2qr + r^2 = 0. \tag{13}$$

Removing the factor of $x - 1$ from (7), we see that x_P is a root of $p^2x^3 + (p^2 + 2pq + 4d^2)x^2 + (p^2 + 2pq + 2pr + q^2 + 3d^2)x + (p^2 + 2pq + 2pr + q^2 + 2qr + d^2) = 0$.

As in the previous case, since x_P is an algebraic integer of norm 1, we have

$$p^2 \mid (p^2 + 2pq + 4d^2), \tag{14}$$

$$p^2 \mid (p^2 + 2pq + 2pr + q^2 + 3d^2), \tag{15}$$

$$-p^2 = p^2 + 2pq + 2pr + q^2 + 2qr + d^2, \tag{16}$$

and combining (13) and (16) yields

$$r^2 - d^2 = p^2. \tag{17}$$

Again, suppose that ℓ is a prime factor of p and note that if $\ell \mid d$, then by (15), $\ell \mid q$ and so by (13), $\ell \mid r$, contradicting the fact that $\gcd(d, p, q, r) = 1$. So $\ell \nmid d$ and, by (14), $\ell = 2$ and $4 \nmid p$. Hence, $p = 1$ or 2. But this contradicts (17), since $d \neq 0$.

- If $k = 5$ and $Q = (2, \pm 7)$, evaluating (7) at $x = 2$ yields

$$16p^2 + 16pq + 8pr + 4q^2 + 4qr + r^2 - 49d^2 = 0. \tag{18}$$

Removing the factor of $x-2$ from (7), we see that x_P is a zero of $p^2x^3 + (2p^2 + 2pq + 4d^2)x^2 + (4p^2 + 4pq + 2pr + q^2 - 17d^2)x + (8p^2 + 8pq + 4pr + 2q^2 + 2qr - 24d^2)$, and so

$$p^2 \mid (2p^2 + 2pq + 4d^2), \tag{19}$$

$$p^2 \mid (4p^2 + 4pq + 2pr + q^2 - 17d^2), \tag{20}$$

$$p^2 = -(8p^2 + 8pq + 4pr + 2q^2 + 2qr - 24d^2), \tag{21}$$

and combining (18) and (21) gives

$$r^2 - d^2 = 2p^2. \tag{22}$$

By (21), we have $2 \mid p$. Then as in the previous cases, $2 \nmid d$ and $p = 2$. By (22), $r = \pm 3$ and $d = \pm 1$ (with independent signs). By (20), q must be odd. If $r = 3$, then (18) simplifies to $q^2 + 11q + 18 = 0$, implying that $q = -9$. Thus x_P is a zero of $x^3 - 6x^2 + 5x - 1$. Alternatively, if $r = -3$, then $q = 1$ and x_P is a zero of $x^3 + 4x^2 - x - 1$. Using the equation for $\mathcal{C}$ to solve for y_P, then using (3), we arrive at the solutions in (iv).

- Finally, if $k = 5$ and $Q = (1/4, 0)$, we obtain

$$p^2 + 8pq + 16q^2 + 32pr + 128qr + 256r^2 = 0, \tag{23}$$

$$64p^2 \mid (256d^2 + 16p^2 + 128pq), \tag{24}$$

$$64p^2 \mid (-1536d^2 + 4p^2 + 32pq + 64q^2 + 128pr), \tag{25}$$

$$64p^2 = -(256d^2 + p^2 + 8pq + 16q^2 + 32pr + 128qr). \tag{26}$$

As above, $2 \nmid d$ and if ℓ is a prime dividing p, then $\ell = 2$. Since d is odd, (24) implies that $8 \nmid p$. So by (23), $p = 4$. But, combining (23) and (26), we have $4(r^2 - d^2) = p^2 = 16$, which is impossible, since $d \neq 0$. ∎

4. Solutions with $[F:\mathbb{Q}]=4$. For the case of $[F:\mathbb{Q}]=4$, we begin by recalling [3, Theorem 3.1], which gives all solutions for the values of k for which $|\mathcal{E}_k(\mathbb{Q})|=3$:

THEOREM 4.1. *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,z. If $|\mathcal{E}_k(\mathbb{Q})|=3$, then these are the only solutions.*

(i) *$F\supseteq\mathbb{Q}(\gamma,\delta)$ 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*
$$(x,y,z)=\left(\delta,\frac{k-\delta+\gamma}{2},\frac{k-\delta-\gamma}{2}\right);$$

(ii) *$F\supseteq\mathbb{Q}(\gamma,\delta)$ 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*
$$(x,y,z)=\left(\delta,\frac{k-\delta+\gamma}{2},\frac{k-\delta-\gamma}{2}\right);$$

(iii) *$F\supseteq\mathbb{Q}(\omega)$ where, for some $t\in\mathbb{Z}-\{1\}$, ω is a fixed root of $X^4+(t^2-kt+2)X^3+(-kt+3t-k+1)X^2+(t-k+2)X+1=0$, and*
$$\begin{aligned}x&=-\omega^3+(-t^2+kt-2)\omega^2\\&\qquad+(kt-3t+k-1)\omega+(-t+k-2),\\(t-1)y&=-\omega^3+(-t^2+kt-1)\omega^2+(t^2-3t+k)\omega+(t-2),\\(t-1)z&=t\omega^3+(t^3-kt^2+2t-1)\omega^2+(-kt^2+2t^2+t-1)\omega+t^2;\end{aligned}$$

(iv) *$F\supseteq\mathbb{Q}(\omega)$ 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*
$$\begin{aligned}x&=-\omega^3+(-t^2+kt+2)\omega^2+(-kt+t-k-1)\omega+(t+k),\\(t-1)y&=-\omega^3+(-t^2+kt+1)\omega^2+(-t^2+t-k)\omega+t,\\(t-1)z&=t\omega^3+(t^3-kt^2-2t+1)\omega^2+(kt^2+t-1)\omega-t^2.\end{aligned}$$

By Theorem 2.1, the only other possible solutions are with $k\in\{-1,5\}$. We address these in the following theorem.

THEOREM 4.2. *Let $k\in\mathbb{Z}$ be such that $\mathcal{E}_k(\mathbb{Q})$ is finite 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 exactly the cases given in Theorem 4.1 and in the following instances, allowing for permutations of x,y,z:*

(i) *For $k=-1$,*

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

$$\begin{aligned} x &= -\upsilon^3 - (t^2 - t - 1)\upsilon^2 - (t^2 - t + 1)\upsilon + 2t, \\ y &= (t + 1)\upsilon^3 + (t^3 - 2t)\upsilon^2 + (t^3 + t^2 - t)\upsilon - (t^2 + 2t), \\ z &= -t\upsilon^3 - (t^3 - t^2 - t + 1)\upsilon^2 - (t^3 - 1)\upsilon + (t^2 - 1); \end{aligned}$$

(b) *$F \supseteq \mathbb{Q}(\upsilon)$ where, for some $t \in \mathbb{Z} - \{0, 1\}$, υ is a fixed root of $X^4 + (t^2 - 3t + 1)X^3 + (t^2 + t - 3)X^2 + 2tX + 1 = 0$, and*

$$\begin{aligned} x &= -\upsilon^3 - (t^2 - 3t + 1)\upsilon^2 - (t^2 + t - 3)\upsilon - 2t, \\ y &= (-t + 1)\upsilon^3 - (t^3 - 4t^2 + 4t - 2)\upsilon^2 \\ &\quad - (t^3 - t^2 - t + 2)\upsilon - (t^2 - 2t + 2), \\ z &= t\upsilon^3 + (t^3 - 3t^2 + t - 1)\upsilon^2 + (t^3 - 1)\upsilon + (t^2 + 1); \end{aligned}$$

(c) *$F \supseteq \mathbb{Q}(\upsilon)$ where, for some $t \in \mathbb{Z}^+ - \{1\}$, υ is a fixed root of $X^4 + (t^2 - t + 5)X^3 - (t^2 - t - 7)X^2 + 4X + 1 = 0$, and*

$$\begin{aligned} x &= -\upsilon^3 - (t^2 - t + 5)\upsilon^2 + (t^2 - t - 7)\upsilon - 4, \\ (2t - 1)y &= (t - 1)\upsilon^3 + (t^3 - 2t^2 + 6t - 4)\upsilon^2 \\ &\quad - (t^3 - 3t^2 - 5t + 4)\upsilon - (t^2 - 4t + 2), \\ (2t - 1)z &= t\upsilon^3 + (t^3 - t^2 + 5t - 1)\upsilon^2 - (t^3 - 8t + 3)\upsilon \\ &\quad + (t^2 + 2t - 1); \end{aligned}$$

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

$$\begin{aligned} x &= -\upsilon^3 - (t^2 - t - 3)\upsilon^2 + (t^2 - t - 1)\upsilon - 2, \\ (2t - 1)y &= t\upsilon^3 + (t^3 - t^2 - 3t + 1)\upsilon^2 - (t^3 - 2t^2 + 1)\upsilon - (t - 1)^2, \\ (2t - 1)z &= (t - 1)\upsilon^3 + (t^3 - 2t^2 - 2t + 2)\upsilon^2 - (t^3 - t^2 - t)\upsilon + t^2. \end{aligned}$$

(ii) *For $k = 5$,*

(a) *$F \supseteq \mathbb{Q}(\eta)$ where, for some $t \in \mathbb{Z}$, η is a fixed root of $X^4 + (t^2 + 3t - 8)X^3 - 2(t^2 + 5t - 9)X^2 + (t - 9)X + 1 = 0$, and*

$$\begin{aligned} x &= -\eta^3 - (t^2 + 3t - 8)\eta^2 + 2(t^2 + 5t - 9)\eta - (t - 9), \\ (3t - 1)y &= t\eta^3 + (t^3 + 3t^2 - 8t + 1)\eta^2 \\ &\quad + (-2t^3 - 9t^2 + 21t - 5)\eta - (t^2 + 6t - 2), \\ (3t - 1)z &= (2t - 1)\eta^3 + (2t^3 + 5t^2 - 19t + 7)\eta^2 \\ &\quad + (-4t^3 - 19t^2 + 43t - 13)\eta + (4t^2 - 7t + 2); \end{aligned}$$

(b) *$F \supseteq \mathbb{Q}(\eta)$ where, for some $t \in \mathbb{Z}$, η is a fixed root of $X^4 + (t^2 + 3t + 4)X^3 - 2t(t - 6)X^2 - (t + 7)X + 1 = 0$, and*

$$\begin{aligned} x &= -\eta^3 - (t^2+3t+4)\eta^2 + 2t(t-6)\eta + (t+7), \\ (3t-1)y &= (2t-1)\eta^3 + (2t^3+5t^2+5t-3)\eta^2 \\ &\quad + (-4t^3+27t^2-9t+1)\eta - (4t^2-t), \\ (3t-1)z &= t\eta^3 + (t^3+3t^2+4t-1)\eta^2 \\ &\quad + (-2t^3+11t^2-3t-1)\eta + (t^2-6t+2); \end{aligned}$$

(c) *$F \supseteq \mathbb{Q}(\eta)$ where, for some $t \in \mathbb{Z}^+$, η is a fixed root of $X^4 + (4t^2-4)X^3 - (t^2+10)X^2 - 4X + 1 = 0$, and*

$$\begin{aligned} x &= -\eta^3 - (4t^2-4)\eta^2 + (t^2+10)\eta + 4, \\ 2ty &= (t+1)\eta^3 + (4t^3+4t^2-4t-5)\eta^2 \\ &\quad - (t^3+5t^2+10t+5)\eta + (t^2+t+1), \\ 2tz &= (t-1)\eta^3 + (4t^3-4t^2-4t+5)\eta^2 \\ &\quad - (t^3-5t^2+10t-5)\eta - (t^2-t+1); \end{aligned}$$

(d) *$F \supseteq \mathbb{Q}(\eta)$ where, for some $t \in \mathbb{Z}^+$, η is a fixed root of $X^4 + (4t^2-8)X^3 - (t^2-14)X^2 - 8X + 1 = 0$, and*

$$\begin{aligned} x &= -\eta^3 - (4t^2-8)\eta^2 + (t^2-14)\eta + 8, \\ 2ty &= (t+1)\eta^3 + (4t^3+4t^2-8t-7)\eta^2 \\ &\quad + (-t^3+3t^2+14t+7)\eta + (-t^2-3t-1), \\ 2tz &= (t-1)\eta^3 + (4t^3-4t^2-8t+7)\eta^2 \\ &\quad + (-t^3-3t^2+14t-7)\eta + (t^2-3t+1). \end{aligned}$$

We note that in (i)(c)–(d) and (ii)(c)–(d), allowing for $t \leq 0$ would simply duplicate the solutions already listed. Certain other values are disallowed because they would give solutions in fields of degree 3, not 4.

Proof of Theorem 4.2. As usual, it is easy to verify that each of these is a solution. Suppose that $(x,y,z) \in \mathcal{O}_F^3$ is a solution that is not given in Theorem 4.1.

If at least one of x, y, z, say x, is of degree strictly less than four over $\mathbb{Q}$, then by the proof of Theorem 4.1 (found in [3]), (x,y,z) is of the form in Theorem 4.1(i) or (ii). Thus x, y, z are each of degree four over $\mathbb{Q}$.

Still following the proof in [3], let $P = (x_P, y_P)$ be the point on $\mathcal{E}_k(F)$ corresponding to the solution (x,y,z) and 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 $\gcd(p,q,r,s,d) = 1$. We assume, without loss of generality, that $p \geq 0$. As shown in [3], $\mathcal{E}_k \cap \mathcal{C}$ includes P and its conjugates and exactly three infinite points (and so $p \neq 0$), leaving two finite points to be determined. Eliminating y and simplifying, the x-coordinates of the points of $\mathcal{E}_k \cap \mathcal{C}$ satisfy

$$\begin{aligned}(27)\qquad & p^2x^6 + 2pqx^5 + (2pr + q^2)x^4 + (2ps + 2qr + 4d^2)x^3 \\ & \qquad + (2qs + r^2 - k^2d^2)x^2 + (2rs + 2kd^2)x + (s^2 - d^2) = 0.\end{aligned}$$

We consider the possibility that the two points are rational, then, separately, that they are irrational.

Case I: *Two rational points.* Since the two points to be determined are on $\mathcal{E}_k$, they must be elements of the sets given in (4) and (5). If the two points are both $(0, \pm 1)$, then, as shown in [3], the solution (x, y, z) is given in Theorem 4.1. So we now consider first the subcases where $k = -1$ and at least one of the two points is in $\{(1, 0), (-1, 2), (-1, -2)\}$, and then the subcases where $k = 5$ and at least one of the two points is in $\{(1/4, 0), (2, 7), (2, -7)\}$.

Subcase: $k = -1$ *and exactly one of the points is* $(1, 0)$ *or* $(-1, \pm 2)$. Assume that the other point is $(0, 1)$. (If instead the point is $(0, -1)$, we obtain the same solutions, up to equivalence.) Since $(0, 1) \in \mathcal{C}$, $s = d$.

- If the two points are $(0, 1)$ and $(1, 0)$, then (27) implies that since $(1, 0) \in \mathcal{C}$, we have $p + q + r + s = 0$. Using this, substituting s for d, and removing the factor of $x(x - 1)$ from (27) yields

$$\begin{aligned}(28)\qquad & p^2x^4 + (p^2 + 2pq)x^3 + (p^2 + 2pq + q^2 + 2pr)x^2 \\ & \qquad + (p^2 + 2pq + q^2 + 2pr + 2qr + 2ps + 4s^2)x + 2s^2 - 2rs = 0.\end{aligned}$$

Since x_P is a root of this equation, the left hand side must be the product of p^2 and the minimal polynomial of x_P. Further, since the norm of x_P is 1, we have $p^2 = 2s^2 - 2rs = 2s(s - r)$.

Suppose that ℓ is a prime such that $\ell \mid s$. Then $\ell \mid p$. Since p^2 is a factor of each coefficient in equation (28), we see that $\ell \mid q$ and $\ell \mid r$. But this implies that $\ell \mid \gcd(d, p, q, r, s)$, a contradiction. So $s = \pm 1$.

Now suppose that ℓ is a prime such that $\ell \mid p$. As above, it follows that $\ell \mid q$ and so, using the x-coefficient of equation (28), $\ell \mid 4$. Thus $\ell = 2$. Now, if $4 \mid p$, then using the x^2-coefficient, $8 \mid q^2$ and thus $4 \mid q$. But then the x-coefficient of equation (28) implies that $8 \mid 4$. Thus, since $p^2 = 2s(s - r)$ and $p > 0$, we have $p = 2$. Now, if $s = 1$, then solving for the other variables yields a minimal polynomial for x_P that factors over $\mathbb{Z}$, implying that x_P is rational or cubic, contrary to assumption. If $s = -1$, then solving for the other variables yields the solution in (i)(a) with $t = 0$.

- If, instead, the points are $(0, 1)$ and $(-1, \pm 2)$, then, recalling that $s = d$, we find that $q = p + r + s$ and $p^2 = 2s(r - s)$. As above, we conclude that $s = \pm 1$ and $p = 2$. If $s = 1$, we obtain the solution in (i)(a) with $t = -1$. If $s = -1$, we get the solution in (i)(d) with $t = 1$.

Subcase: $k = -1$ *and both points are in* $\{(1,0),(-1,2),(-1,-2)\}$. Note that the two points cannot be $(-1,2)$ and $(-1,-2)$, since these points cannot both lie on the curve $\mathcal{C}$.

• If the two points are $(1,0)$ and $(-1,2)$, then by the definition of $\mathcal{C}$, $p+q+r+s=0$ and $-p+q-r+s=2d$. So $d=q+s=-p-r$. Removing the factor of $(x+1)(x-1)$ from (27) yields $p^2x^4+2pqx^3+(p^2+q^2+2pr)x^2+(4d^2+2pq+2qr+2ps)x+p^2+q^2+2pr+r^2+2qs-d^2=0$. Since x_P is a root of this equation, the left hand side must be the product of p^2 and the minimal polynomial of x_P. Again, since the norm of x_P is 1, $q=d-s$, and $r=-p-d$, we have $d^2-s^2=p^2$.

Suppose that ℓ is a prime such that $\ell \mid p$. Then, since p^2 divides each of the coefficients above, $\ell \mid q$ and so $\ell \mid 4d^2$. If, in addition, $\ell \mid d$, then $\ell \mid s$ and, from the constant coefficient, $\ell \mid r$. But this is a contradiction, since $\gcd(d,p,q,r,s)=1$, and so $\ell \nmid d$. Hence $\ell \mid 4$ and so $\ell = 2$ and d is odd. As before, if $4 \mid p$, then $4 \mid q$, and so $8 \mid 4d^2$, a contradiction. But if $p=2$, then $d^2-s^2=p^2$ yields a contradiction, since d is odd. Thus, no such ℓ exists and, hence, $p=1$.

It follows from $d^2-s^2=p^2$ that $d=\pm 1$ and $s=0$. This leads to the solutions in Theorem 4.1(iii) and (iv) with $k=-1$ and $t=-1$. As usual, $(1,0)$ and $(-1,-2)$ yield equivalent solutions.

• If $(1,0)$ is a double point on $\mathcal{C} \cap \mathcal{E}_k$, then, dividing equation (27) by $(x-1)^2$, the remainder must be zero, implying that $6p^2+10pq+4q^2+8pr+6qr+2r^2+6ps+4qs+2rs+8d^2=5p^2+8pq+3q^2+6pr+4qr+r^2+4ps+2qs-s^2+8d^2=0$, and the quotient is the product of p^2 and the minimal polynomial of x_P. Hence, x_P is a root of $p^2x^4+(2p^2+2pq)x^3+(3p^2+4pq+q^2+2pr)x^2+(4p^2+6pq+2q^2+4pr+2qr+2ps+4d^2)x+5p^2+8pq+3q^2+6pr+4qr+r^2+4ps+2qs+7d^2=0$ with the constant coefficient equal to p^2. Combining the second part of the remainder with the constant coefficient yields $s^2-d^2=p^2$.

As before, if ℓ is a prime dividing p, then $\ell=2$ and $\ell \nmid d$. Again, $4 \mid p$ leads to a contradiction. So $p=1$ or $p=2$, but then $s^2-d^2=p^2$ implies that $d=0$, a contradiction.

• Finally, if $(-1,2)$ or $(-1,-2)$ is a double point, we obtain the polynomial $p^2x^4+(-2p^2+2pq)x^3+(3p^2-4pq+q^2+2pr)x^2+(-4p^2+6pq-2q^2-4pr+2qr+2ps+4d^2)x+5p^2-8pq+3q^2+6pr-4qr+r^2-4ps+2qs-9d^2$ with $6p^2-10pq+4q^2+8pr-6qr+2r^2-6ps+4qs-2rs-12d^2=5p^2-8pq+3q^2+6pr-4qr+r^2-4ps+2qs-s^2-8d^2=0$, which leads to a contradiction as in the previous case.

Subcase: $k=5$ *and exactly one of the points is* $(1/4,0)$ *or* $(2,\pm 7)$. Assume that one of the points is $(0,1)$ (or equivalently $(0,-1)$) and note that, since $(0,1)$ is on $\mathcal{C}$, $s=d$.

• If the two points are $(0, 1)$ and either $(2, 7)$ or $(2, -7)$, then factoring $x(x-2)$ out of (27) with $s = d$ yields the polynomial $p^2x^4 + (2p^2 + 2pq)x^3 + (4p^2 + 4pq + q^2 + 2pr)x^2 + (4s^2 + 8p^2 + 8pq + 2q^2 + 4pr + 2qr + 2ps)x + (-17s^2 + 16p^2 + 16pq + 4q^2 + 8pr + 4qr + r^2 + 4ps + 2qs)$ with $16p^2 + 16pq + 4q^2 + 8pr + 4qr + r^2 + 4ps + 2qs + rs - 12s^2 = 0$. Combining the final equation with the constant coefficient, which is equal to p^2, yields $s(5s + r) = -p^2$.

As usual, if p is divisible by an odd prime, we get a contradiction. Further, if $4 \mid p$, then, since p^2 divides the x^2-coefficient, $4 \mid q$. From this it follows that $2 \mid s$, and so $2 \mid r$, again yielding a contradiction. Hence, $p = 1$ or 2.

If $p = 1$, then $s(r + 5s) = -1$ and so $s = \pm 1$ and $r = \mp 6$. This leads to the solutions in (ii)(c) and (ii)(d) with $t = 1$. If $p = 2$, then $2 \mid q$ and r and s are odd. Hence $s(r + 5s) = -4$ implies that $s = \pm 1$ and $r = \mp 9$. Solutions in (ii)(a) and (ii)(b), with $t = 0$, follow.

• Next, if the two points are $(0, 1)$ and $(1/4, 0)$, then since $(1/4, 0)$ lies on $\mathcal{C}$, we have

$$0 = p + 4q + 16r + 64s. \tag{29}$$

Removing the factor of $x(x - 1/4)$ from (27) and noting that the coefficients must all be divisible by p^2 in $\mathbb{Z}$, we obtain

$$4p^2 \mid (p^2 + 8pq), \tag{30}$$

$$16p^2 \mid (p^2 + 8pq + 16q^2 + 32pr), \tag{31}$$

$$64p^2 \mid (256s^2 + p^2 + 8pq + 16q^2 + 32pr + 128qr + 128ps), \tag{32}$$

$$256p^2 \mid (-6144s^2 + p^2 + 8pq + 16q^2 + 32pr + 128qr + 256r^2 + 128ps + 512qs). \tag{33}$$

Suppose ℓ is an *odd* prime such that $\ell \mid p$. By (31), $\ell \mid q$ and so, by (32), $\ell \mid s$ and, by (33), $\ell \mid r$. Since $d = s$, this contradicts $\gcd(p, q, r, s, d) = 1$. Thus p is a power of 2.

Let $p = 2^e$, $q = 2^f q'$, $r = 2^g r'$, and $s = 2^h s'$, with q', r', s' odd integers and $e, f, g, h \geq 0$. Substituting this into (30), we find that $2^{2e+2} \mid (2^{2e} + 2^{e+f+3}q')$. This is only possible if $e = f + 3$.

Combining (30), (31) gives $p^2 \mid (4q^2 + 8pr)$, so $2^{2e} \mid (2^{2e-4}(q')^2 + 2^{e+g+3}r')$. Thus $g = e - 7$.

By (29), $0 = p + 4q + 16r + 64s = 2^e + 2^{e-1}q' + 2^{e-3}r' + 2^{h+6}s'$. This is only possible if $e - 3 = h + 6$. Therefore, $h = e - 9$.

Combining (31) and (32), we get $p^2 \mid (8qr + 8ps + 16s^2)$, and so

$$2^{2e} \mid (2^{2e-7}q'r' + 2^{2e-6}s' + 2^{2e-14}(s')^2),$$

which is clearly impossible.

Subcase: *$k = 5$ and both points are in* $\{(1/4, 0), (2, 7), (2, -7)\}$. Note that the two points cannot be $(2, 7)$ and $(2, -7)$, since we would then get an immediate contradiction from the equation for $\mathcal{C}$.

• If the two points are $(1/4,0)$ and $(2,\pm 7)$, then removing the factor of $(x-2)(x-1/4)$ from (27) and noting that the coefficients must all be divisible by p^2 in $\mathbb{Z}$, we obtain

$$4p^2 \mid (9p^2+8pq), \tag{34}$$

$$16p^2 \mid (73p^2+72pq+16q^2+32pr), \tag{35}$$

$$64p^2 \mid (256d^2+585p^2+584pq+144q^2+288pr+128qr+128ps), \tag{36}$$

$$\begin{aligned}256p^2 \mid (&4681p^2+4680pq+1168q^2+2336pr\\ &+1152qr+256r^2+1152ps+512qs-4096d^2).\end{aligned} \tag{37}$$

Further, since $(1/4,0)$ lies on $\mathcal{C}$, (29) holds, and so $4 \mid p$.

As in the previous case, we find that p is a power of 2. We again let $p=2^e$, $q=2^f q'$, $r=2^g r'$, $s=2^h s'$, and $d=2^i d'$, with q',r',s',d' all odd integers and $e,f,g,h,i \geq 0$. Substituting this into (34), we find that $2^{2e+2} \mid (9\cdot 2^{2e}+2^{e+f+3}q')$. This is possible only if $f=e-3$.

Combining (34) and (35), we find that $4p^2 \mid (64pq+16q^2+32pr)$, and so $2^{2e} \mid (2^{2e+1}q'+2^{2e-4}(q')^2+2^{e+3+g}r')$. Thus $2e-4=e+3+g$, and therefore $g=e-7$.

Again, by (29), $0=p+4q+16r+64s=2^e+2^{e-1}q'+2^{e-3}r'+2^{h+6}s'$. This is only possible if $e-3=h+6$. Hence $h=e-9$.

Combining (35) and (36), we have $2p^2 \mid (32d^2-9p^2-8pq+16qr+16ps)$, and so $2^{2e+1} \mid (2^{2i+5}(d')^2-2^{2e}\cdot 9-2^{2e}q'+2^{2e-6}q'r'+2^{2e-5}s')$. This is only possible if $2i+5=2e-6$, which is a contradiction, since i and e are integers.

• If $(1/4,0)$ is a double point, then again equation (29) holds. Combining this with the fact that $(x-1/4)^2$ is a factor of (27) yields a contradiction, since $d \neq 0$.

• Finally, if $(2,7)$ (or $(2,-7)$) is a double point, then $(x-2)^2$ is a factor of (27), yielding the quotient $p^2x^4+(4p^2+2pq)x^3+(12p^2+8pq+q^2+2pr)x^2+(4d^2+32p^2+24pq+4q^2+8pr+2qr+2ps)x+80p^2+64pq+12q^2+24pr+8qr+r^2+8ps+2qs-9d^2$, and the remainder $(-42d^2+192p^2+160pq+32q^2+64pr+24qr+4r^2+24ps+8qs+2rs)x+35d^2-320p^2-256pq-48q^2-96pr-32qr-4r^2-32ps-8qs+s^2$.

Since the constant coefficient of the quotient is equal to p^2 and the constant coefficient of the remainder is equal to zero, combining these yields

$$s^2-d^2=4p^2. \tag{38}$$

As usual, we find that p has no odd prime factors and $4 \nmid p$. If $p=1$, then (38) implies that $d=0$, which is impossible. Thus, $p=2$. By (38), $s=\pm 5$ and $d=\pm 3$ (with independent signs). This leads to the solutions in Theorem 4.1(iii) and (iv) with $k=5$ and $t=4$.

Case II: *Two conjugate quadratic points.* Finally, we consider the possibility that the two points of $\mathcal{E}_k \cap \mathcal{C}$ to be determined are not rational. Since $\mathcal{E}_k \cap \mathcal{C}$ is closed under conjugation, the two points must be quadratic conjugates. The possible values are given in Lemma 3.1.

If the two points are of the form in Lemma 3.1(i), then the x-coordinates are rational and so, by the definition of the curve $\mathcal{C}$, y is also rational, contrary to assumption.

If the points are of the form in Lemma 3.1(ii), then the arguments in the proof of Theorem 4.1 (found in [3]) apply to show that $t \in \mathbb{Z}$ and the solution is as in Theorem 4.1(iii) or (iv), unless we have $k = -d^2 = t$. But in this case, the polynomial for x in Lemma 3.1(ii) is reducible and the additional points are rational, again contrary to assumption.

If the two points are of one of the forms in Lemma 3.1(iii) and (iv), then the x-coordinates satisfy an equation of the form x^2+Px+Q with $P, Q \in \mathbb{Q}$. Equation (27) then factors as

$$\begin{aligned}(39)\qquad p^2x^6 + 2pqx^5 + (2pr + q^2)x^4 + (2ps + 2qr + 4d^2)x^3 \\ + (2qs + r^2 - k^2d^2)x^2 + (2rs + 2kd^2)x + (s^2 - d^2) \\ = p^2(x^2 + Px + Q)(x^4 + ax^3 + bx^2 + cx + 1) = 0,\end{aligned}$$

with $a, b, c \in \mathbb{Z}$.

By Gauss's lemma, since the other coefficients are integers, the coefficients of $p^2(x^2 + Px + Q)$ must be integers. Thus, $p^2P, p^2Q \in \mathbb{Z}$.

Equating the coefficients in (39) yields

$$ap^2 + p^2P - 2pq = 0, \tag{40}$$

$$bp^2 + ap^2P - q^2 + p^2Q - 2pr = 0, \tag{41}$$

$$-4d^2 + cp^2 + bp^2P + ap^2Q - 2qr - 2ps = 0, \tag{42}$$

$$d^2k^2 + p^2 + cp^2P + bp^2Q - r^2 - 2qs = 0, \tag{43}$$

$$-2d^2k + p^2P + cp^2Q - 2rs = 0, \tag{44}$$

$$d^2 + p^2Q - s^2 = 0. \tag{45}$$

By (40), $p \mid p^2P$. Since each possible value of P in Lemma 3.1(iii) and (iv) is a monic quadratic with integral coefficients in the variable $t \in \mathbb{Q}$, $p \mid p^2P$ implies that $p \mid p^2t^2$. Thus, for Q in Lemma 3.1(iii) and (iv)(a), we have $p \mid p^2Q$ and for Q in Lemma 3.1(iv)(b) we have $p \mid 4p^2Q$.

Suppose that ℓ is an odd prime dividing p. Then $\ell \mid p^2P$ and $\ell \mid p^2Q$. By (41), $\ell \mid q$, and so, by (42), $\ell \mid d$. Further, by (43), $\ell \mid r$ and by (45), $\ell \mid s$. But then $\ell \mid \gcd(p, q, r, s, d)$, contrary to assumption. Thus p is a power of 2.

Now, if the two points are as in Lemma 3.1(iii) or (iv)(a) and $4 \mid p$, then (40) implies that $8 \mid p^2P$. Then, from the definition of Q in Lemma 3.1, $8 \mid p^2Q$. Hence equation (41) implies that $4 \mid q$. But then, by (42), $2 \mid d$, and we get a contradiction as above. Thus for these cases, we have $p = 1$ or 2, which then implies that $t \in \mathbb{Z}$, since $pP \in \mathbb{Z}$.

If the two points are as in Lemma 3.1(iv)(b), we use a similar argument: If $16 \mid p$, then by (40), $32 \mid p^2P$ and from the definition of Q, $8 \mid p^2Q$, leading again to a contradiction. Further, if $p = 8$, then $8 \mid p^2P$ and $2 \mid p^2Q$, implying that $2 \mid q$ and, since $\gcd(p, q, r, s, d) = 1$, the numbers d, r, s are odd. But then, by (45), $8 \mid p^2Q$, and so (41) and (42) imply that d is even, a contradiction. Thus, $p \in \{1, 2, 4\}$ and since $p \mid p^2t^2$, $2t \in \mathbb{Z}$. But if $u = 2t$ is odd, then $p = 4$, and reducing (40) modulo 8 yields a contradiction. Thus $t \in \mathbb{Z}$.

Again, considering all four of the cases in Lemma 3.1(iii) and (iv), we use (45) to eliminate d^2, (40) to eliminate q, and (44) to eliminate r, then simplify to obtain

$$4p^2P + 4cp^2Q + 8kp^2Q + a^2ps - 4bps - 2apPs + pP^2s - 4pQs - 8ks^2 = 0, \tag{46}$$

$$\begin{aligned} &ap^3P + p^3P^2 + acp^3Q + 2akp^3Q + cp^3PQ + 2kp^3PQ - 2cp^2s \\ &\quad - 2bp^2Ps - 8p^2Qs - 2ap^2Qs + 4ps^2 - 2akps^2 - 2kpPs^2 + 8s^3 = 0, \end{aligned} \tag{47}$$

$$\begin{aligned} &p^3P^2 + 2cp^3PQ + 4kp^3PQ + c^2p^3Q^2 + 4ckp^3Q^2 + 4k^2p^3Q^2 \\ &\quad - 4ps^2 - 4cpPs^2 - 4kpPs^2 - 4bpQs^2 - 4ckpQs^2 - 4k^2pQs^2 \\ &\quad + 4as^3 + 4Ps^3 = 0. \end{aligned} \tag{48}$$

Using (46) to eliminate b in the other two equations, and letting

$$A = pQa - pPQ - 2s, \tag{49}$$

$$C = p^2c + 2kp^2 - 2ps + \frac{p^2P - 2ks^2}{Q} - \frac{2Ps^2}{Q^2}, \tag{50}$$

we obtain

$$2QAC - P/QsA^2 + 4s(p^2Q - s^2)(P/Q + 2k - 4Q) = 0,$$
$$s^2A^2 - Q^3C^2 - 4s^2(p^2Q - s^2)(P^2/Q - 1 + 2kP + k^2Q) = 0.$$

Using the first equation to eliminate C in the second and recalling that $s^2 = d^2 + p^2Q$ yields

$$\begin{aligned} -s^2\big(&A^4(P^2 - 4Q) - 4d^2A^2((2kQ + P)^2 + (P^2 - 4Q) + 8PQ^2) \\ &+ 16d^4(P + 2kQ - 4Q^2)^2\big) = 0. \end{aligned} \tag{51}$$

To complete the proof of Case II, we now consider each of the remaining four cases of Lemma 3.1 separately.

Subcase: *Lemma* 3.1(iii)(a). If the two additional points are of the form in this part of the lemma, then $k = -1$, $P = t^2 - t - 1$, and $Q = t^2 + t$, with $t \neq 0$ or -1. Since $t \in \mathbb{Z}$, for each value of t, P is odd and Q is even. Reducing (44) modulo 2, we see that $p \neq 1$. Thus, $p = 2$.

Further, by (41), q is even and so, by (40), since P is odd, a is odd. Returning to equation (51), we now have

$$(52)\quad s^2(A^2 - 4d^2(2t+1)^2)(4d^2(1+t+3t^2+2t^3)^2 - A^2(P^2-4Q)) = 0.$$

If the first factor of (52) is equal to zero, then $s = 0$ and by (45), $d^2 = -4t(t+1)$. But this implies that $-t(t+1)$ is a square, which is impossible, since $t \neq 0$ or -1.

If the third factor is equal to zero, then

$$4d^2(1+t+3t^2+2t^3)^2 = A^2(P^2-4Q),$$

implying that $P^2 - 4Q$ is a square. But then, since $x^2 + Px + Q = 0$, we have $x \in \mathbb{Q}$, contrary to assumption.

Therefore, the second factor, $A^2 - 4d^2(2t+1)^2$, is equal to zero and the other two factors are nonzero. So for some fixed $\varepsilon = \pm 1$,

$$A = 2d\varepsilon(2t+1).$$

Combining this with (49), we get

$$(53)\qquad Q(a-P) = s+d\varepsilon(2t+1) = (s+d\varepsilon)+2dt\varepsilon = (s-d\varepsilon)+2d(t+1)\varepsilon,$$

and therefore, since $Q = t(t+1)$, we see that $t \mid (s+d\varepsilon)$ and $(t+1) \mid (s-d\varepsilon)$. Let $c_1, c_2 \in \mathbb{Z}$ be such that

$$c_1 t = s + d\varepsilon \quad \text{and} \quad c_2(t+1) = s - d\varepsilon.$$

Then, multiplying, we obtain $c_1c_2Q = s^2 - d^2 = 4Q$ and thus $c_1c_2 = 4$.

If $c_1 = \pm 4$ and $c_2 = \pm 1$, then $s = \pm(5t+1)/2$ and $d\varepsilon = \pm(3t-1)/2$, with the leading signs in agreement. By (53), $a - P = \pm 3$. But this is impossible, since, as noted above, a and P are both odd. Similarly, if $c_1 = \pm 1$ and $c_2 = \pm 4$, we arrive at a contradiction.

Thus $c_1 = c_2 = \pm 2$, and so $s = \pm(2t+1)$ and $d\varepsilon = \mp 1$. By (53), $a = P$. Using (40)–(45), we obtain the remaining solutions in part (i)(a) and (after changing t to $t-1$) part (i)(b) of the theorem.

Subcase: *Lemma* 3.1(iii)(b). In this situation, $k = -1$, $P = t^2 - t + 1$, and $Q = -t^2 + t$, with $t \neq 0$ or 1. As in the previous case, for each $t \in \mathbb{Z}$, P is odd and Q is even. It follows from (44) that $p \neq 1$. Hence, $p = 2$, q is even, and a is odd.

Equation (51) is now

$$(54)\quad s^2(A^2 - 4d^2(2t-1)^2)\big(4d^2(2t-1)^2(t^2-t-1)^2 - A^2(P^2-4Q)\big) = 0.$$

As before, if $s^2 = 0$, then by (45), $d^2 = 4t(t-1)$, which is impossible. If the third factor of (54) is equal to zero, then $P^2 - 4Q$ is a square, implying that $x \in \mathbb{Q}$, a contradiction.

Therefore, the second factor, $A^2 - 4d^2(2t-1)^2$, is equal to zero and the other two factors are nonzero. So for some fixed $\varepsilon = \pm 1$, $A = 2d\varepsilon(2t-1)$.

Combining this with (49), we get

$$Q(a-P) = s + d\varepsilon(2t-1) = s + d\varepsilon + 2(t-1)d\varepsilon = s - d\varepsilon + 2td\varepsilon, \tag{55}$$

and therefore, since $Q = -t(t-1)$, we see that $(t-1) \mid (s+d\varepsilon)$ and $t \mid (s-d\varepsilon)$. Let $c_1, c_2 \in \mathbb{Z}$ be such that

$$c_1(t-1) = s + d\varepsilon \quad \text{and} \quad c_2 t = s - d\varepsilon.$$

Then, multiplying, we obtain $c_1c_2(-Q) = s^2 - d^2 = 4Q$, and thus $c_1c_2 = -4$.

As in the previous case, we obtain contradictions unless $-c_1 = c_2 = \pm 2$. It follows that $s = \pm 1$ and $d\varepsilon = \mp(2t-1)$. By equation (55), $a = P \pm 4$. Using (40)–(45), we obtain the remaining solutions in parts (i)(c) and (i)(d) of the theorem.

Subcase: *Lemma* 3.1(iv)(a). Here, $k = 5$, $P = t^2 + 3t - 2$, and $Q = -2t^2 + t$, with $t \neq 0$ or $1/2$. Recall that $p = 1$ or 2 and $t \in \mathbb{Z}$, and note that P and a are both even.

Again, substituting into (51) and simplifying, we obtain

$$s^2(A^2 - 4d^2(4t-1)^2)\big(4d^2(-2 + 5t - 3t^2 + 4t^3)^2 - A^2(P^2 - 4Q)\big) = 0. \tag{56}$$

If $s^2 = 0$, then combining (44) and (45), we find that $10p^2Q + p^2P + cp^2Q = 0$. It follows that $Q \mid P$, which is possible only if $t = 1$. Using (40)–(45), we obtain the solution in part (ii)(a) of the theorem with $t = 1$ (in which case, the second factor of (56) is also zero). If the third factor is zero, we obtain a contradiction.

Thus, the second factor is zero, and so $A^2 = 4d^2(4t-1)^2$. Set $\varepsilon = \pm 1$ such that

$$A = 2d\varepsilon(4t-1). \tag{57}$$

If $p = 1$, then by (40), $2 \mid (a+P)$, and so $2 \mid (a-P)$. So, for $p = 1$ or 2, there exists $\hat{a}_p \in \mathbb{Z}$ such that

$$2\hat{a}_p = p(a-P). \tag{58}$$

By (49) and (57),

$$\hat{a}_p Q = s + d\varepsilon(4t-1) = s + d\varepsilon + 2d\varepsilon(2t-1) = s - d\varepsilon + 4d\varepsilon t. \tag{59}$$

Since $Q = -t(2t-1)$, there exist $c_1, c_2 \in \mathbb{Z}$ such that

$$c_1(2t-1) = s + d\varepsilon \quad \text{and} \quad c_2 t = s - d\varepsilon.$$

Thus $c_1c_2(-Q) = s^2 - d^2 = p^2Q$, and so $c_1c_2 = -p^2$.

If $p = 2$ and $c_1 = \pm 1$, solving for s leads to a contradiction. If $p = 2$ and $c_1 = \pm 4$, then (58) and (59) imply that $a - P = \mp 9$. But this contradicts the fact that a and P are both even.

Thus, regardless of the value of p, $c_1 = -c_2 = \pm p$ and so $s = \pm p(t-1)/2$ and $d\varepsilon = \pm p(3t-1)/2$. By (58) and (59), $a - P = \mp 6$. Equations (40)–(45) now yield the remaining solutions in parts (ii)(a) and (ii)(b) of the theorem.

SUBCASE: *Lemma* 3.1(iv)(b). Now, $k = 5$, $P = t^2-6$, and $Q = -t^2/4+1$, with $t \neq \pm 2$. Recall that $p \in \{1, 2, 4\}$ and $t \in \mathbb{Z}$.

Substituting into (51) yields

$$s^2(A^2 - d^2t^2)\big(d^2t^2(t^2 - 2)^2 - A^2(P^2 - 4Q)\big) = 0. \tag{60}$$

If $s^2 = 0$, then by (45), $4d^2 = p^2(t^2 - 4)$ and so $t^2 - 4$ is a square, which is impossible, since $t \neq \pm 2$. If the third factor is zero, then $x \in \mathbb{Q}$, a contradiction.

Therefore, only the second factor is zero, and so $A^2 = d^2t^2$. Set $\varepsilon = \pm 1$ such that $A = d\varepsilon t$. Then, by (49),

$$pQ(a - P) = 2s + d\varepsilon t. \tag{61}$$

As above, if $p = 1$, then by (40), $2 \mid (a - P)$. So regardless of the value of p, there exists $\hat{a}_p \in \mathbb{Z}$ such that

$$2\hat{a}_p = p(a - P). \tag{62}$$

Since $Q = -t^2/4 + 1$, equation (61) implies that $2\hat{a}_p(-t^2/4 + 1) = 2s + d\varepsilon t$. As before, we have

$$-\hat{a}_p(t+2)(t-2) = 4s+2d\varepsilon t = 4(s+d\varepsilon)+2d\varepsilon(t-2) = 4(s-d\varepsilon)+2d\varepsilon(t+2).$$

Thus, there exist $c_1, c_2 \in \mathbb{Z}$ such that

$$c_1(t - 2) = 4(s + d\varepsilon) \quad \text{and} \quad c_2(t + 2) = 4(s - d\varepsilon). \tag{63}$$

Solving these for s and $d\varepsilon$, we find that

$$-\hat{a}_p(t + 2)(t - 2) = 4s + 2d\varepsilon t = (c_1 - c_2)(t + 2)(t - 2)/4$$

and therefore, using (62), $c_1 - c_2 = -4\hat{a}_p = -2p(a - P)$. In particular, we have $2p \mid (c_1 - c_2)$.

Now, equations (45) and (63) imply that $c_1c_2(-4Q) = 16(s^2 - d^2) = 16p^2Q$, and thus $c_1c_2 = -4p^2$. Since $2p \mid (c_1 - c_2)$, this implies that $-c_1 = c_2 = \pm 2p$. It follows that $s = \pm p$, $d\varepsilon = \mp pt/2$, and $a = P \pm 2$. Then, by (40), $q = p(P \pm 1)$.

If t is odd, then p is even. But then, since $p \mid q$, equation (41) implies that $2p \mid p^2Q$, which is impossible with t odd. Thus t is even, and so P is even and $Q \in \mathbb{Z}$. Now, if p is even, then q is even, $d\varepsilon = \mp pt/2$ is even, s is even, and, by (43), r is even. Since $\gcd(p, q, r, s, d) = 1$, we conclude that $p = 1$. Returning to equations (40)–(45), replacing t with $2t$, we find the remaining solutions in parts (ii)(c) and (ii)(d) of the theorem. ■

Acknowledgements. Research of H. G. Grundman was supported by the Faculty Research Fund of Bryn Mawr College.

Research of L. L. Hall-Seelig was supported by Faculty Development Grants of Merrimack College.

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

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

[3] H. G. Grundman and L. L. Hall-Seelig, *Solutions to* $xyz = 1$ *and* $x + y + z = k$ *in algebraic integers of small degree, I*, Acta Arith. 162 (2014), 381–392.

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 6.4.2015
and in revised form on 12.8.2015 (8128)