ACTA ARITHMETICA
112.4 (2004)

New solutions to $xyz = x + y + z = 1$ in integers of quartic fields

by

H. G. Grundman and L. L. Hall (Bryn Mawr, PA)

1. Introduction. In 1991, Bremner [1] claimed to have found all solutions in integers of quartic number fields to the diophantine equation $xyz = x + y + z = 1$. He presented an elegant and insightful method for finding these solutions along with an explicit list of solutions. Unfortunately, because of an error in the application of the method, the list was not complete. In this work, we summarize his method, explain the oversight, and complete the process of determining an exhaustive list of solutions. Our main result is the following theorem.

Theorem 1. *The equation*

$$xyz = x + y + z = 1 \tag{1}$$

is solvable with $x, y, z \in \mathcal{O}_k$, the ring of integers of a quartic number field k, in precisely the following instances, up to permutation of x, y, and z:

1. $x = 1$, $y = i$, $z = -i$.
2. $x = -1$, $y = 1 + \sqrt{2}$, $z = 1 - \sqrt{2}$.
3. *If we let θ be either square root of $t^2 + 4$, $t \in \mathbb{Z}$, then*
   $$2x = t + \theta,$$
   $$8y = (4 - 2t - 2\theta) + (t + \theta)\sqrt{8 + 28t + 2t^2 + 8t^3 - (12 + 2t + 8t^2)\theta},$$
   $$8z = (4 - 2t - 2\theta) - (t + \theta)\sqrt{8 + 28t + 2t^2 + 8t^3 - (12 + 2t + 8t^2)\theta}.$$
4. *If we let ϕ be either square root of $t^2 - 4$, $t \in \mathbb{Z}$, then*
   $$2x = t + \phi,$$
   $$8y = (4 - 2t - 2\phi) + (t + \phi)\sqrt{20t + 2t^2 - 8t^3 - (4 + 2t - 8t^2)\phi},$$
   $$8z = (4 - 2t - 2\phi) - (t + \phi)\sqrt{20t + 2t^2 - 8t^3 - (4 + 2t - 8t^2)\phi}.$$
5. *If we let ψ be a fixed root of*
   $$1 + (2 - t)\psi + (2 - 2t)\psi^2 + (2 - t + t^2)\psi^3 + \psi^4 = 0,\ t \in \mathbb{Z} - \{0\},$$

2000 *Mathematics Subject Classification*: 11D25, 11R16.

then

$$x = -(2-t) - (2-2t)\psi - (2-t+t^2)\psi^2 - \psi^3,$$
$$ty = (1+t) + (1-t-t^2)\psi + (1-t+t^2)\psi^2 + \psi^3,$$
$$tz = -(1-2t+t^2) - (1-3t+t^2)\psi - (1-3t+2t^2-t^3)\psi^2 - (1-t)\psi^3.$$

In part 3, $t = 0$ *yields parts* 1 *and* 2. *In part* 4, *each of* $t = 0$ *and* $t = 2$ *yields part* 1 *and* $t = -2$ *yields part* 2. *Otherwise*, *there is no overlap between the parts.*

The first two parts follow from [2], in which $xyz = x+y+z$ was considered over quadratic fields. Part 3 is new and the remaining two parts were found by Bremner (though in different forms).

2. Finding solutions. In [1], Bremner presented a new method for solving equation (1) over the ring of integers of a cubic or quartic number field k. We begin by summarizing his method with k a quartic field.

First note that x, y, and z must all be units and that at least one of them, say x, must have norm 1. Letting $X = 1/x$ and $Y = (x+2y-1)/x$, Bremner obtained a point (X, Y) with $X, Y \in \mathcal{O}_k$, on the elliptic curve

$$E: \quad Y^2 = 1 - 2X + X^2 - 4X^3. \tag{2}$$

Conversely, any point (X, Y) on E with $X, Y \in \mathcal{O}_k$ and X a unit gives rise to a solution to equation (1), specifically

$$x = 1/X, \quad y = (1 - 1/X + Y/X)/2, \quad z = (1 - 1/X - Y/X)/2. \tag{3}$$

For an arbitrary point $P = (X, Y)$ on E with $X, Y \in \mathcal{O}_k$ and X a unit, Bremner considered the cubic curve through P and its three other $\mathbb{Q}$-conjugates:

$$dy = px^3 + qx^2 + rx + s, \quad d, p, q, r, s \in \mathbb{Z},\ d \neq 0,\ (d, p, q, r, s) = 1. \tag{4}$$

Herein lies Bremner's first mistake. He overlooked the possibility that X might not have four distinct conjugates. It is quite reasonable to assume that X and Y are not both in a proper subfield of k, since all such solutions have already been described. The missing case is that where X is quadratic over $\mathbb{Q}$ while Y is quartic. For this, the four conjugates of P lie on a pair of lines:

$$(dy)^2 = (px+q)^2.$$

We find all solutions arising from this missing case in Section 3 of this paper.

Continuing with Bremner's work, assuming that X is quartic over $\mathbb{Q}$, equations (2) and (4) intersect in nine points in projective space. Four of these points are P and its other conjugates, and at least three of these points are at $\mathfrak{o}$. We will denote the two remaining points by (x_1, y_1) and (x_2, y_2).

Bremner first proved that there cannot be a fourth point of intersection at $\mathfrak{o}$ and that if $x_1, y_1, x_2, y_2 \in \mathbb{Q}$, then $x_1 = x_2 = 0$. This led to the special cases of $t = 1$ in parts 4 and 5 of Theorem 1.

It remained to consider the case where x_1, y_1, x_2, y_2 lie in a quadratic number field, but are not all rational. In [1, Lemma 1], Bremner proved that any such point $(x, y) \in E$ satisfies $x \in \mathbb{Q} - \{0\}$ or $x^2 + m(m-1)x + m = 0$, for some $m \in \mathbb{Q} - \{0\}$. He then showed that $x_1, x_2 \in \mathbb{Q} - \{0\}$ leads to a contradiction. Since x_1 and x_2 are $\mathbb{Q}$-conjugates, they are therefore the two roots of $x^2 + m(m-1)x + m = 0$, for some $m \in \mathbb{Q} - \{0\}$.

Eliminating y from equations (2) and (4) yields an equation for the x-coordinates of the six finite points of intersection. These x-coordinates are the four roots of the minimal polynomial of X, say

$$f(x) = x^4 + ax^3 + bx^2 + cx + 1,$$

and the two roots of $x^2 + m(m-1)x + m = 0$, for some $m \in \mathbb{Q} - \{0\}$. Hence,

$$\begin{aligned}(5)\qquad &(px^3 + qx^2 + rx + s)^2 - d^2(1 - 2x + x^2 - 4x^3)\\ &\qquad = p^2(x^4 + ax^3 + bx^2 + cx + 1)(x^2 + m(m-1)x + m).\end{aligned}$$

By Gauss's Lemma, $p^2(x^2 + m(m-1)x + m) \in \mathbb{Z}[x]$. It follows easily that $m = u/p$ for some $u \in \mathbb{Z} - \{0\}$, but here Bremner erroneously assumed that u and p must be relatively prime. By equating coefficients in (5) and considering possible factors of p, Bremner proved that $p = 1$ or 2. Using the incorrect assumption that $(p, u) = 1$, he concluded that $p = 1$. We will complete the missed case of $p = 2$ at the end of this section.

For $p = 1$, Bremner completed a complicated series of computations and deductions leading to the following solutions with $\alpha = \pm 1$:

$$\begin{aligned} p &= 1, & a &= u(u-1) + 2\alpha,\\ q &= u(u-1) + \alpha, & b &= (\alpha+1)u + (1-\alpha),\\ r &= (\alpha/2 + 1)u - \alpha/2, & c &= \alpha(u+1),\\ s &= \alpha(u+1)/2, & d &= \pm\alpha(u-1)/2. \end{aligned}$$

It follows immediately from the fact that each of these is an element of $\mathbb{Z}$ that u must be odd. If we let $t = 1 - u$ and $\alpha = \pm 1$, then

$$(6)\qquad \begin{aligned} f(x) &= x^4 + (t^2 - t + 2)x^3 - (2t-2)x^2 - (t-2)x + 1, \quad \text{or}\\ f(x) &= x^4 + (t^2 - t - 2)x^3 + 2x^2 + (t-2)x + 1. \end{aligned}$$

The first yields the solutions with even values of t in part 5 of Theorem 1, with $f(x)$ the minimal polynomial of ψ. The second yields the solutions with even values of t in part 4 of Theorem 1, with $f(x)$ the minimal polynomial of $1/y$ (and $1/z$).

Bremner, however, erroneously expanded the domain of u from the set of all odd integers to include all values in $\mathbb{Z}$ for which $f(x)$ is irreducible.

(Note that for even values of u, r and s are nonintegers.) This masked the error of assuming that $p \neq 2$ by retrieving the otherwise missing solutions. We illustrate this by evaluating the omitted case of $p = 2$.

Our starting point is equation (5) with $m = u/p$, $u \in \mathbb{Z}$, and $p = 2$. Equating coefficients yields the following equations:

$$s^2 - d^2 = 2u, \tag{7}$$

$$2d^2 + 2rs = u^2 + 2cu - 2u, \tag{8}$$

$$r^2 - d^2 + 2qs = 4 + 2bu - 2cu + cu^2, \tag{9}$$

$$4d^2 + 2qr + 4s = 4c + 2au - 2bu + bu^2, \tag{10}$$

$$q^2 + 4r = 4b + 2u - 2au + au^2, \tag{11}$$

$$4q = 4a - 2u + u^2. \tag{12}$$

From (12) it follows that u is even. This with (11) implies that q is even. If s were even, then by (7), d is even and, using (9), r is even. But then $(p, q, r, s, d) > 1$, a contradiction. Hence s is odd. Let $u', q', s' \in \mathbb{Z}$ such that $u = 2u'$, $q = 2q'$, and $s = 2s' + 1$. Successively using (7) to eliminate d^2, (12) to eliminate a, (11) to eliminate b, (10) to eliminate c, and (8) to eliminate r, yields

$$\begin{aligned}
&(1 - q' - 2q's' - u' + q'^2u' - 2s'u' + u'^2 + 2q'u'^2 + 2s'u'^2 + u'^3 - 2q'u'^3 - 2u'^4 + u'^5) \\
&\times (-1 - 4s' - 4s'^2 + 4q'u' + 8q's'u' + 6u'^2 - q'u'^2 - 4q'^2u'^2 + 12s'u'^2 \\
&- 2q's'u'^2 + 4s'^2u'^2 - 13u'^3 - 6q'u'^3 + q'^2u'^3 - 18s'u'^3 + 4q's'u'^3 - 8s'^2u'^3 \\
&+ 8u'^4 + 9q'u'^4 - 2q'^2u'^4 + 6s'u'^4 - 2q's'u'^4 + 6u'^5 - 6q'u'^5 + q'^2u'^5 \\
&- 6s'u'^5 - 7u'^6 + 6q'u'^6 + 2s'u'^6 + 6u'^7 - 2q'u'^7 - 4u'^8 + u'^9) = 0.
\end{aligned}$$

Setting the second factor equal to zero and reducing modulo 2 shows that u' must be odd. Then reducing the same equation modulo 4 yields a contradiction.

Setting the first factor equal to zero and reducing modulo 2 shows that u' must be even. Solving for $2s'$ yields

$$2s' = -u'^3 + u'^2 + u'q' - 1 + \frac{1}{q' + u' - u'^2}.$$

So $1/(q' + u' - u'^2) \in \mathbb{Z}$ and therefore $q' + u' - u'^2 = \pm 1$. So $q' = u'^2 - u' + \alpha$ with u' even and nonzero (since u is nonzero) and $\alpha = \pm 1$. This yields the following two families of solutions:

$$\begin{aligned}
p &= 2, & a &= 2\alpha - u' + u'^2, \\
q &= 2u'^2 - 2u' + 2\alpha, & b &= (\alpha + 1)u' - \alpha + 1, \\
r &= (2 - \alpha)u' + \alpha, & c &= \alpha(u' + 1), \\
s &= \alpha(u' - 1), & d &= \pm(u' - 1).
\end{aligned}$$

Letting $t = 1 - u'$, we get the same polynomials as in (6) and thus the solutions in parts 4 and 5 of Theorem 1 with odd values of $t \neq 1$ (since $u \neq 0$). This completes the derivations of parts 4 and 5, for all $t \in \mathbb{Z}$.

3. The new solutions. In this section, we determine all points (X, Y) on E where X and Y are algebraic integers in some quartic field k, X is a unit of norm 1, and X, but not Y, lies is some quadratic subfield of k. This case, which Bremner overlooked, yields two families of solutions to (1), one of which is absent from Bremner's original work.

To find all solutions stemming from this case, note that the minimal polynomial of X over $\mathbb{Q}$ is of the form $f(x) = x^2 + tx \pm 1$, with $t \in \mathbb{Z}$. This corresponds to $X = (-t \pm \sqrt{t^2 + 4})/2$ and $X = (-t \pm \sqrt{t^2 - 4})/2$. Solving for Y in (2), and then for x, y, and z in (3), yields the solutions given in parts 3 and 4, respectively, of Theorem 1. (The values of t for which $f(x)$ is reducible give the solutions written explicitly in parts 1 and 2.)

Note that although Bremner missed this case, he did find the solutions in part 4 of Theorem 1. This is easily explained by recalling that any solution can be permuted arbitrarily to obtain additional solutions. Although the x value of these solutions is quadratic over $\mathbb{Q}$, the y and z are both quartic. Therefore, Bremner's method found a permutation of these results, one in which the z is quadratic over $\mathbb{Q}$ and x is quartic.

Bremner did not find the solutions in part 3 of Theorem 1, because he assumed that x must be quartic over $\mathbb{Q}$ *and* $N_k(x) = 1$. These two assumptions combined to eliminate the solutions in part 3 and their permutations since x is quadratic with $N_k(x) = 1$ and y and z are quartic of norm -1.

Finally note that the method Bremner presented in [1] is sound; it was in its application that errors were made. Indeed, his method is what enabled us now to determine the complete set of solutions given in Theorem 1.

References

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

[2] R. A. 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*, ibid. 48 (1987), 341–345.

Bryn Mawr College
101 N. Merion Ave.
Bryn Mawr, PA 19010, U.S.A.
E-mail: grundman@brynmawr.edu
llhall@brynmawr.edu

Received on 24.9.2003 (4631)