MATHEMATICS OF COMPUTATION
VOLUME 41, NUMBER 164
OCTOBER 1983, PAGES 731-741

# Integer Points on $y^2 = x^3 - 7x + 10$

By Andrew Bremner and Nicholas Tzanakis

**Abstract.** The 26 integer solutions of $y^2 = x^3 - 7x + 10$ are found and an error in a published table of fundamental units is corrected.

**0.** In 1953 Wiman [21] discovered, by a simple application of the chord and tangent process, that the cubic curves

$$y^2 = x^3 - 7x + 10, \tag{0.1}$$

$$y^2 = x^3 - 172x + 820, \tag{0.2}$$

$$y^2 = x^3 - 172x + 505, \tag{0.3}$$

$$y^2 = x^3 - 112x + 2320, \tag{0.4}$$

contain, respectively, 24, 60, 58, 70 integer points (in pairs, symmetric about the $x$-axis). The curve (0.1) occurs again in Hartshorne [10, Chapter IV, Ex. 4.18], where it is pointed out that it contains at least 26 integer points. It is the aim of the present paper to settle the question of the integer points on (0, 1); and in fact we show that there are precisely 26 such points.

It is apparent that the groups of rational points on curves (0.1)–(0.4) will probably have several generators. Using the arithmetic of the field $\mathbf{Q}(\rho)$, $\rho^3 - 7\rho + 10 = 0$ (see Section 1), one can perform the standard 2-descents (see Cassels [6] or Birch and Swinnerton-Dyer [4]) on the curve (0.1) to determine that its rational Mordell-Weil group actually has rank 2, but the details are omitted. It seems plausible that the rank of the curves (0.2), (0.3), (0.4) is in each instance equal to 4, but this has not been specifically verified.

It is perhaps also worth noting here the integer point on (0.4) given by

$$(x, y) = (1645085185, 66724078854865)$$

because of the large size of the coordinates; Lang [11], [12] has made some interesting conjectures on the size of integral points on the curve $y^2 = x^3 + ax + b$, in particular that for an integral point $(x_0, y_0)$ then $|x_0| \ll \max(|a|^3, |b|^2)^k$ for some uniform $k$. The curve (0.1) has conductor $2^3 \cdot 83$ (see Tate [19] for a recipe on calculation of the conductor), rank 2, and 26 integer points, none of which, however, is particularly 'large'. Examples possessing a sizeable solution include:

(i) the curve $y^2 = x^3 - x + 1$ of conductor $2^2 \cdot 23$, rank 1, and 12 integer points including $(x, y) = (56, 419)$. (This is the curve denoted $92c$ in the tables of Birch and Kuyk [3]; see also the review [MR 82g: 10037] by the first author of a paper by Sansone [16].)

Received November 29, 1982.
1980 *Mathematics Subject Classification.* Primary 10B10; Secondary 12A30.

(ii) The curve $y^2 = x^3 - 4x + 1$ of conductor $2^2 \cdot 229$, rank 2, and at least 22 integer points including $(x, y) = (1274, 45473)$. (See Billing [2, Chapter IX, Ex. 1].)

Recently, Mestre [14] has given an example of a curve of rank at least 12 with at least 320 integer points.

The techniques used in this paper of using the arithmetic of the appropriate cubic extension to obtain finitely many equations of type (binary quartic form) = 1, and then disposing of the latter using Skolem's $p$-adic method, are well known and are described in Mordell [15, Chapters 27, 23]. The methods can always be applied to the equation $y^2 = x^3 + ax + b$, although in theory there is no guarantee of all the integer points being found. In practice, it is usually the case that such an equation can be resolved (given an enthusiasm for sometimes excessive arithmetic calculation).

**1.** We work in the field $\mathbf{Q}(\rho)$, $\rho^3 - 7\rho + 10 = 0$. As an integer basis take (see Delone and Faddeev [8, Theorem II, p. 112]): $1$, $\rho$, $\sigma = (2 - \rho + \rho^2)/4$, with the field discriminant being $-83$. It is straightforward to show that the class number of the field is 1, while in Section 5 we prove that $\varepsilon = 1 - \sigma$ is a fundamental unit, thereby correcting an error in a table of Brentjes [5]. Equation (0.1) may be written

$$(1.1) \qquad (x - \rho)(x^2 + \rho x + \rho^2 - 7) = y^2,$$

and any common divisor of the two factors on the left-hand side must divide $3\rho^2 - 7$. Since $\operatorname{Norm}(3\rho^2 - 7) = 16 \cdot 83$, we need the factorizations of the divisors (83) and (2). In the former case, it is easy to check that $(83) = p_{83}^2 p'_{83}$, where $p'_{83} = (-9 + 2\rho + 5\sigma)$ and $p'_{83} = (-7 + 2\rho + 5\sigma)$. For the factorization of (2) we need an element of odd index: such an element is $\rho + \sigma$ of index 1 with minimum polynomial $t^3 - 5t^2 + 9t - 4$. Accordingly, $(2) = p_2 p'_2$ where $p_2 = (-2 + \rho + \sigma)$ is a first-degree divisor, and $p'_2 = (3 - \rho - 2\sigma)$ is a second-degree divisor. Now $3\rho^2 - 7 = -9 + \rho + 4\sigma$ is not divisible by either $p'_{83}$ or $p_2$, and so $(3\rho^2 - 7) = p_2'^2 p_{83}$. From (1.1) it follows that $(x - \rho) = p_2'^i p_{83}^j a^2$ for an integral divisor $a$, and where without loss of generality $i, j \in \{0, 1\}$. However, if $j = 1$, then on taking norms we obtain $y^2 = 83 \cdot$ (integer square), an obvious impossibility. We thus deduce the nondivisor equation

$$(1.2) \quad x - \rho = \pm\varepsilon^k (3 - \rho - 2\sigma)^i (a + b\rho + c\sigma)^2, \qquad , k \in \{0, 1\}, a, b, c \in \mathbf{Z},$$

with the upper sign when $i + k \equiv 0 \bmod 2$ and the lower sign when $i + k \equiv 1 \bmod 2$ (as seen by taking norms). There are four cases to be considered.

*Case* I: $(i, k) = (0, 0)$. Now $x - \rho = (a + b\rho + c\sigma)^2$ giving

$$(1.3) \qquad \begin{gathered} x = a^2 - 2b^2 - 4bc, \quad -b^2 + c^2 - 2ab - 4bc = 1, \\ 4b^2 + 3c^2 + 2ac - 2bc = 0. \end{gathered}$$

The third equation is easily solved by standard techniques (e.g. consider it as a second degree equation in $b$ with discriminant which must be a perfect square). Suppose without loss of generality that $c < 0$; then it follows that $a = 3m^2 + mn + n^2$, $b = mn$, $c = -2m^2$ for certain integers $m$, $n$. Substituting into the second equation at (1.3) gives $m(4m^3 + 2m^2 n - 3mn^2 - 2n^3) = 1$, and, since without loss of generality $m > 0$, we have $m = 1$ and $(2n + 3)(n^2 - 1) = 0$. Thus $(m, n) = (1, 1)$, $(1, -1)$ giving, respectively, $(a, b, c) = (5, 1, -2)$, $(3, -1, -2)$ and $(x, \pm y) = (31, 172), (-1, 4)$.

*Case* II: $(i, k) = (0, 1)$. Now $x - \rho = (-1 + \sigma)(a + b\rho + c\sigma)^2$ giving

$$x = -a^2 + 2c^2 - 4ab - 4bc, \quad 3b^2 + 4c^2 - 2ab + 2ac - 6bc = 1,$$
$$a^2 + 5b^2 + 7c^2 - 2ab + 4ac - 12bc = 0.$$

As above, the third equation leads now to two possibilities: assuming that $c > 0$, we have, for certain integers $m, n$ of opposite parity, either $a = -2n^2 + mn$, $b = m^2 + mn + n^2$, $c = m^2 + n^2$, or $a = -m^2 + 4mn - 3n^2$, $b = 3m^2 + n^2$, $c = 2(m^2 + n^2)$. In the first instance, substitution results in

$$(1.4) \qquad m^4 + 3m^2n^2 + 4mn^3 + n^4 = 1,$$

while in the second instance,

$$(1.5) \qquad n^4 + 8n^3m + 6n^2m^2 - 8nm^3 + 9m^4 = 1.$$

In Section 2 it is shown that the only solutions of (1.4) with $m, n$ of opposite parity are $\pm(m, n) = (1, 0)$, $(0, 1)$, $(3, -4)$, leading, respectively, to $(a, b, c) = (0, 1, 1)$, $(-2, 1, 1)$, $(-44, 13, 25)$ and $(x, \pm y) = (-2, 4)$, $(2, 2)$, $(302, 5248)$; and that the only solutions of (1.5) are $\pm(m, n) = (0, 1)$, $(-1, 2)$ with corresponding $(a, b, c) = (-3, 1, 2)$, $(-21, 7, 10)$, and $(x, \pm y) = (3, 4)$, $(67, 548)$.

*Case* III: $(i, k) = (1, 0)$. Now $x - \rho = -(3 - \rho - 2\sigma)(a + b\rho + c\sigma)^2$ giving

$$x = 3a^2 + 8b^2 + 12ab + 4ac + 8bc, \quad -a^2 + 2c^2 - 4ab - 4bc = 1,$$
$$-2a^2 - 6b^2 - 4c^2 - 4ab - 4ac + 4bc = 0.$$

As before, the third equation leads to the two possibilities (on supposing $b > 0$): either $a = -3m^2 + 4mn - 3n^2$, $b = m^2 + n^2$, $c = m^2 - 2mn + 3n^2$, or $a = -m^2 - 5n^2$, $b = m^2 + n^2$, $c = m^2 - 2mn + 3n^2$, where $m, n$ are relatively prime and of opposite parity. In the first instance we deduce

$$(1.6) \qquad m^4 + 8m^3n - 6m^2n^2 - 8mn^3 + 9n^4 = 1,$$

while in the second case

$$(1.7) \qquad m^4 + 18m^2n^2 - 16mn^3 + n^4 = 1.$$

The above two equations are solved in Section 3. It is proved there that the only situation to (1.6) is $\pm(m, n) = (1, 0)$, with corresponding $(a, b, c) = (-3, 1, 0)$ and $(x, \pm y) = (5, 10)$; and that the only solutions to (1.7) are $\pm(m, n) = (1, 0)$, $(0, 1)$ with respective $(a, b, c) = (-1, 1, 1)$, $(-5, 1, 3)$ and $(x, \pm y) = (-3, 2)$, $(13, 46)$.

*Case* IV: $(i, k) = (1, 1)$. Now $x - \rho = (1 - \sigma)(3 - \rho - 2\sigma)(a + b\rho + c\sigma)^2$ giving

$$x = a^2 + 8b^2 + 4c^2 + 4ab + 4ac, \quad a^2 + 6b^2 + 6c^2 + 4ac - 8bc = 1,$$
$$2b^2 + 5c^2 - 4ab + 2ac - 10bc = 0.$$

On supposing $a + 2c > 0$, the third equation leads to either $a = m^2 - 8mn + n^2$, $b = 2(m^2 + mn)$, $c = 4mn$, or $a = -3m^2 + 5n^2$, $b = 2(m^2 + mn)$, $c = 2(m^2 - n^2)$ where $m, n$ are relatively prime and of opposite parity. In the first instance we may deduce

$$(1.8) \qquad n^4 - 6n^2m^2 - 16nm^3 + 25m^4 = 1,$$

and in the second instance

$$(1.9) \qquad m^4 + 16m^3n + 42m^2n^2 + 32mn^3 + 9n^4 = 1.$$

These equations are solved in Section 4. It is shown that $\pm(m, n) = (0, 1)$ is the only solution to (1.8), with $(a, b, c) = (1, 0, 0)$ and $(x, \pm y) = (1, 2)$; and that $\pm(m, n) = (1, 0), (2, -1)$ are the only solutions to (1.9), with $(a, b, c) = (-3, 2, 2)$, $(-7, 4, 6)$ and $(x, \pm y) = (9, 26)$, $(41, 262)$, respectively. We have then proved the following result.

THEOREM. *The elliptic curve* $y^2 = x^3 - 7x + 10$ *has exactly* 26 *integral points, which are the following*:

$$(x, \pm y) = (1,2), (2,2), (-3,2), (-1,4), (-2,4), (3,4), (5,10), (9,26),$$
$$(13,46), (31,172), (41,262), (67,548), (302,5248).$$

**2. The Solution of Eqs. (1.4) and (1.5).** We work in the field $\mathbf{Q}(\theta)$, $\theta^4 + 3\theta^2 + 4\theta + 1 = 0$. By standard methods it is easy to prove that $\{1, \theta, \theta^2, \theta^3\}$ is an integer basis with discriminant $-2^4 \cdot 83$. In Section 6 it is shown that a pair of fundamental units in $\mathbf{Q}(\theta)$ may be taken as $\varepsilon_1 = \theta$, $\varepsilon_2 = 1 + \theta$. Then Eqs. (1.4) and (1.5) can be written, respectively, in the form

$$\text{Norm}(m - n\theta) = 1, \tag{2.1}$$
$$\text{Norm}((m + n) - (m - n)\theta) = 1, \tag{2.2}$$

and so it suffices to find all solutions of just Eq. (2.1). We wish to work $p$-adically for an appropriate prime $p$, which in practice involves finding a prime $p$ such that the coefficients of $\theta^2$, $\theta^3$ in $\varepsilon_1^r\varepsilon_2^s$ vanish modulo $p$ as infrequently as possible for varying $r$, $s$. Primes $p$ which split into first degree factors in $\mathbf{Q}(\theta)$ are particularly suitable for investigation since then the order of $\varepsilon_i$ modulo $p$ has to divide $p - 1$, and the amount of checking of the coefficients of $\theta^2$, $\theta^3$ in $\varepsilon_1^r\varepsilon_2^s$ is relatively limited. In this particular instance $p = 397$ is a suitable prime. Direct (machine) calculation gives

$$\begin{aligned}
\varepsilon_1^{198} &\equiv -1 - 397(46 - 123\theta - 128\theta^2 - 53\theta^3) \mod 397^2\\
&= -1 - 397\xi_1, \quad \text{say;}\\
\varepsilon_2^{396} &= 1 + 397(111 + 48\theta + 321\theta^2 + 75\theta^3) \mod 397^2\\
&= 1 + 397\xi_2, \quad \text{say;}
\end{aligned}$$

and the only values $r$, $s$ with $-99 < r \leqslant 99$, $-198 < s \leqslant 198$, such that the coefficients of $\theta^2$ and $\theta^3$ in $\varepsilon_1^r\varepsilon_2^s$ are both divisible by 397, are given by:

(2.3)

| $(r, s)$ | $\varepsilon_1^r\varepsilon_2^s$ |
|---|---|
| $(0,0)$ | $1$ |
| $(0,1)$ | $1 + \theta$ |
| $(1,0)$ | $\theta$ |
| $(4,-1)$ | $-1 - 3\theta$ |
| $(-2,4)$ | $3 + 4\theta$ |

Write now

$$m - n\theta = \pm\varepsilon_1^u\varepsilon_2^v,$$

and put $u = 198M + r$, $v = 396N + s$, $-99 < r \leqslant 99$, $-198 < s \leqslant 198$ so that

$$\pm(m - n\theta) = \varepsilon_1^r\varepsilon_2^s(1 + 397\xi_1)^M(1 + 397\xi_2)^N$$
$$= \varepsilon_1^r\varepsilon_2^s\left(K_0 + K_1\theta + K_2\theta^2 + K_3\theta^3\right),$$

where

$$K_0 = 1 + 397(46M + 111N) + 397^2(\,) + \cdots,$$
$$K_1 = 397(-123M + 48N) + 397^2(\,) + \cdots,$$
$$K_2 = 397(-128M + 321N) + 397^2(\,) + \cdots,$$
$$K_3 = 397(-53M + 75N) + 397^2(\,) + \cdots.$$

Since $\pm(m - n\theta) \equiv \varepsilon_1^r\varepsilon_2^s \bmod 397$, the only acceptable values of $(r, s)$ are those listed at (2, 3). Now if $(r, s) = (0,0)$, then $K_2 = 0 = K_3$, forcing

$$(-128M + 321N) + 397(\,) + \cdots = 0,$$
$$(-53M + 75N) + 397(\,) + \cdots = 0.$$

But

$$\begin{vmatrix} -128 & 321 \\ -53 & 75 \end{vmatrix} \equiv 267 \mod 397,$$

and so, by the well-known theorem of Skolem (see, e.g., [17], [18]), there is at most one solution $(M, N)$ which is clearly (0,0). In this case $(u, v) = (0, 0)$. Similarly, when $(r, s) = (0, 1), (1,0), (4, -1), (-2, 4)$, we get the following systems in $M$, $N$, respectively: $K_2 + K_3 = 0 = K_1 + K_2 - 3K_3$; $K_2 = 0 = K_1 - 3K_3$; $-3K_1 - K_2 + 9K_3 = 0 = -3K_2 - K_3$; $4K_1 + 3K_2 - 12K_3 = 0 = 3K_3 + 4K_2$ with corresponding determinants

$$\begin{vmatrix} -181 & -1 \\ -92 & 144 \end{vmatrix} \equiv 46, \quad \begin{vmatrix} -128 & 321 \\ 36 & -177 \end{vmatrix} \equiv 381,$$
$$\begin{vmatrix} 20 & 210 \\ 40 & 153 \end{vmatrix} \equiv 218, \quad \begin{vmatrix} -240 & 255 \\ 123 & -79 \end{vmatrix} \equiv 299.$$

Thus, by the aforementioned theorem of Skolem, $(M, N) = (0, 0)$ is the only solution in each case, and $(u, v)$ has the value of the corresponding $(r, s)$. Thus the solutions of (2.1) are $\pm(m, n) = (1, 0), (0, 1), (3, -4), (1, -1), (1, -3)$ leading directly to the previously mentioned solutions to (1.4) and (1.5).

We give an alternative verification for the equation (1.5) to show that here one can give the solutions without necessarily having recourse to a computer.

In $\mathbf{Q}(\theta)$ take as fundamental units $\varepsilon = \theta(1 + \theta)^{-1} = 1 + 4\theta - \theta^2 + \theta^3$, and $\theta = -1 + 3\varepsilon^2 + \varepsilon^3$. Then $\varepsilon^4 + 2\varepsilon^3 - 3\varepsilon^2 + 1 = 0$, and (1.5) can be written:

$$\mathrm{Norm}((m + n) - 2m\varepsilon) = 1.$$

Thus

$$\pm((m + n) - 2m\varepsilon) = \varepsilon^u\theta^v,$$

and putting $u = 2p + i$, $i = 0, 1$, $v = 2p + q$, there results

$$\pm((m + n) - 2m\varepsilon) = \varepsilon^i(\varepsilon^2\theta^2)^p\theta^q = \varepsilon^i(1 + 2\varepsilon)^p\theta^q.$$

Now $(1+2\varepsilon)^2 = 1 + 4(\varepsilon + \varepsilon^2)$ and $\theta^6 = 1 + 4(-\varepsilon + 2\varepsilon^2 + \varepsilon^3) \bmod 16$. Put $p = 2P + r, q = 6Q + s, r = 0, 1, s = 0, 1, \ldots, 5$, so that

$$\begin{aligned} &\pm((m+n) - 2m\varepsilon) \\ &\quad = \varepsilon^i(1+2\varepsilon)^r\theta^s\{[1 + 4^2(\,)] + [4P + 4Q + 4^2(\,)]\varepsilon \\ &\qquad\qquad + [4P - 8Q + 4^2(\,)]\varepsilon^2 + [-4Q + 4^2(\,)]\varepsilon^3\}. \end{aligned}$$

In particular, the coefficient of $\varepsilon$ in $\varepsilon^i(1+2\varepsilon)^r\theta^s$ must be even, while the coefficients of $\varepsilon^2$ and $\varepsilon^3$ must be zero mod 4. Amongst the 24 possible triples $(i, r, s)$ the only ones satisfying these requirements are $(i, r, s) = (0, 0, 0)$, $(0, 1, 0)$. In the first instance, it follows that

$$\begin{aligned} P - 2Q + 4(\,) + \cdots &= 0, \\ -Q + 4(\,) + \cdots &= 0, \end{aligned}$$

while in the second instance

$$\begin{aligned} 3P - 6Q + 4(\,) + \cdots &= 0, \\ 2P - Q + 4(\,) + \cdots &= 0; \end{aligned}$$

but

$$\begin{vmatrix} 1 & -2 \\ 0 & -1 \end{vmatrix} \equiv 1 \bmod 2, \quad \text{and} \quad \begin{vmatrix} 3 & -6 \\ 2 & -1 \end{vmatrix} \equiv 1 \bmod 2,$$

so that, by Skolem's theorem, $(P, Q) = (0, 0)$ is the only solution in each case. Then $(u, v) = (0, 0)$, $(2, 2)$, respectively, corresponding to $\pm(m, n) = (0, 1)$, $(-1, 2)$. We remark that it seems difficult to apply a 2-adic method in the case of (1.4).

**3. The Solution of Eqs. (1.6) and (1.7).** Consider first the equation (1.7), and work in the field $\mathbf{Q}(\theta)$, $\theta^4 + 18\theta^2 - 16\theta + 1 = 0$. An integer basis is $\{1, \theta, \omega, \theta\omega\}$, where $\omega = (1+\theta^2)/4$, and a pair of fundamental units is (see §6): $\theta$, $\varepsilon = 7 - 8\theta - 2\theta\omega$. Then (1.7) is equivalent to

$$\pm(m - n\theta) = \theta^u\varepsilon^v.$$

Put $u = 2M + i, v = 2N + j,\ i, j = 0, 1$, so that

$$\begin{aligned} \pm(m - n\theta) &= \theta^i\varepsilon^j(1 - 4\omega)^M[1 + 4(11 - 13\theta - 3\theta\omega)]^N \\ &= \theta^i\varepsilon^j\{[1 + 4.11N + 8(\,)] + [-4.13N + 8(\,)]\theta \\ &\qquad + [-4M + 16(\,)]\omega + [-4.3N + 16(\,)]\theta\omega\}, \end{aligned}$$

where every term in brackets ( ) is a polynomial in $M$, $N$ with 2-adic integral coefficients. In particular, the coefficients of $\omega$ and $\theta\omega$ in $\theta^i\varepsilon^j$ must be zero mod 4, which forces $(i, j) = (0, 0), (1, 0)$. If $(i, j) = (0, 0)$, then we must have

$$\begin{aligned} -M + 4(\,) + \cdots &= 0, \\ -3N + 4(\,) + \cdots &= 0, \end{aligned}$$

and if $(i, j) = (1, 0)$, then

$$\begin{aligned} 51N + 4(\,) + \cdots &= 0, \\ -M + 4(\,) + \cdots &= 0, \end{aligned}$$

and so in both cases the appropriate determinant is odd and $(0, 0)$ is the only solution, giving $(u, v) = (0, 0)$, $(1, 0)$ and $\pm(m, n) = (0, 0)$, $(1, 0)$. Next consider (1.6). This equation is equivalent to $\mathrm{Norm}(m - n\Theta) = 1$, where $\Theta^4 + 8\Theta^3 - 6\Theta^2 - 8\Theta + 9 = 0$. Put $\Omega = (1 + \Theta^2)/4$; then $\theta = 8 - \Theta - 18\Omega - 2\Theta\Omega$, $\omega = -6 - 2\Theta + 8\Omega + \Theta\Omega$ and, moreover, in $\mathbf{Q}(\Theta) = \mathbf{Q}(\theta)$ we may take as a pair of fundamental units $\theta$, $E = \varepsilon^{-1} = 7 - 8\theta - 2\theta\omega = -1 + 2\Omega$. Now

$$\begin{aligned} \pm(m - n\theta) &= \theta^{2M+i}E^{2N+j}, \qquad i, j = 0, 1, \\ &= \theta^i E^j[1 - 4(2 + 2\Theta + \Theta\Omega)]^M[1 + 4(-1 + \Theta + \Omega - 2\Theta\Omega)]^N \mod 16. \end{aligned}$$

In particular the coefficients of $\Omega$ and $\Theta\Omega$ in $\theta^i E^j$ must both be zero mod 4, forcing $(i, j) = (0, 0)$. As usual, there results a system

$$\begin{aligned} -M - 2N + 4(\,) + \cdots &= 0, \\ N + 4(\,) + \cdots &= 0, \end{aligned}$$

and so $(M, N) = (0, 0)$ is the only solution, whence $\pm(m, n) = (1, 0)$ is the only solution to (1.6).

A simple alternative proof can be given involving machine calculation. Write (1.6), (1.7) in the form

$$\begin{aligned} \mathrm{Norm}(m - n\Theta) &= 1, \\ \mathrm{Norm}((m + n) - (m - n)\Theta) &= 4. \end{aligned}$$

Since $(m + n) - (m - n)\Theta = 2n + (m - n)(1 - \Theta) \equiv 0 \mod (1 - \Theta)$, we can deduce from (1.6), (1.7) equations

$$\begin{aligned} \pm(m - n\Theta) &= \eta^u E^v, \\ \pm((m + n) - (m - n)\Theta) &= (1 - \Theta)\eta^u E^v, \end{aligned}$$

where $\eta = -\theta E = \Theta + 2\Omega$, $E = -1 + 2\Omega$ is clearly a pair of fundamental units. An appropriate choice of prime in this instance (see remarks at beginning of Section 2) is $p = 293$. Working 293-adically, we obtain

$$\begin{aligned} -138 \cdot \eta^{73} &\equiv 1 + 293(-89 - 11\Theta - 36\Omega + 4\Theta\Omega) \mod 293^2 \\ &= 1 + 293\xi_1, \quad \text{say;} \\ E^{292} &\equiv 1 + 293(193 - 76\Theta + 25\Omega + 85\Theta\Omega) \mod 293^2 \\ &= 1 + 293\xi_2, \quad \text{say.} \end{aligned}$$

Put $u = 73M + r$, $v = 292N + s$, $-36 < r \leqslant 36$, $-146 < s \leqslant 146$, so that

$$\pm 138^{-M}(m - n\Theta) = \alpha\eta^r E^s(1 + 293\xi_1)^M(1 + 293\xi_2)^N, \qquad \alpha = 1 \text{ or } 1 - \Theta.$$

In particular, the coefficients of $\Omega$ and $\Theta\Omega$ in $\alpha\eta^r E^s$ must both be zero mod 293, which happens for $\alpha = 1$ only if $(r, s) = (0, 0)$ and for $\alpha = 1 - \Theta$ only if $(r, s) = (0, 0)$, $(1, -1)$. Then we work as in Section 2 and prove in each case that the only possibility is $(M, N) = (0, 0)$, whence $\pm(m, n) = (1, 0)$ is the only solution to (1.6), and $\pm(m, n) = (1, 0)$, $(0, 1)$ are the only solutions to (1.7).

**4. The Solution of Eqs. (1.8) and (1.9).** Consider (1.8); we work in $\mathbf{Q}(\theta)$, $\theta^4 - 6\theta^2 - 16\theta + 25 = 0$. Put $\omega = (1 + \theta^2)/4$, so that $\{1, \theta, \omega, \theta\omega\}$ is an integer basis, and from Section 6 a pair of fundamental units may be taken as $\varepsilon_1 = -6 + \theta + 6\omega + 2\theta\omega$, $\varepsilon_2 = 1 - 2\theta + 2\omega$. Write (1.8) in the form

$$\pm(n - m\theta) = \varepsilon_1^i\varepsilon_2^j\varepsilon_1^{2M}\varepsilon_2^{2N}, \qquad i,j = 0, 1.$$

Observing that

$$-\varepsilon_1^2 = 1 + 4(37 - 5\theta - 38\omega - 13\theta\omega), \quad \varepsilon_2^2 = 1 + 4(-3 + 7\omega - 2\theta\omega)$$

and thus that the coefficients of $\omega$ and $\theta\omega$ in $\varepsilon_1^i\varepsilon_2^j$ must both be zero mod 4, the only possibility is $(i,j) = (0,0)$. Then as usual we obtain a system

$$\begin{aligned} -38M + 7N + 4(\,) + 4 \cdots &= 0, \\ -13M - 2N + 4(\,) + \cdots &= 0, \end{aligned}$$

with unique solution $(M, N) = (0,0)$ corresponding to $\pm(m, n) = (0, 1)$. Next consider (1.9). This equation is equivalent to Norm$(m - n\Theta) = 1$, with $\Theta^4 + 16\Theta^3 + 42\Theta^2 + 32\Theta + 9 = 0$. Put $\Omega = (1 + \Theta^2)/4$; then $\theta = -4 + 13\Theta + 30\Omega + 2\Theta\Omega$, $\omega = -10\Theta - 16\Omega - \Theta\Omega$ and in $\mathbf{Q}(\Theta) = \mathbf{Q}(\theta)$ the following may be taken as fundamental units: $E_1 = \varepsilon_1^{-1} = 2 + \Theta$, and $E_2 = -(\varepsilon_1\varepsilon_2)^{-1} = \Theta + 2\Omega$. Now (1.9) is equivalent to

$$\pm(m - n\theta) = E_1^iE_2^jE_1^{2M}E_2^{2N}, \qquad i,j = 0, 1.$$

We have $-E_1^2 = 1 - 4(1 + \Theta + \Omega)$, $-E_2^2 = 1 - 4(-2 + \Theta + 9\Omega + 3\Theta\Omega)$, and so the coefficients of $\Omega$ and $\Theta\Omega$ in $E_1^iE_2^j$ must both be zero mod 4, forcing $(i,j) = (0,0)$, $(1,0)$. In the former instance we get the system

$$\begin{aligned} -M + 9N + 2(\,) + \cdots &= 0, \\ 3N + 2(\,) + \cdots &= 0, \end{aligned}$$

and in the latter instance

$$\begin{aligned} -123N + 2(\,) + \cdots &= 0, \\ -M + 9N + (\,) + \cdots &= 0, \end{aligned}$$

each system having the unique solution $(M, N) = (0,0)$ giving the respective solutions $\pm(m, n) = (1,0), (2, -1)$.

*Remark.* A $p$-adic treatment with $p = 401$ will also furnish a solution of (1.8) and (1.9), writing them in the form Norm$(n - m\theta) = 1$, Norm$((m - n) - (m + n)\theta) = 4$; but the details do not present any particular interest.

**5. Appendix 1: The Fundamental Unit in $\mathbf{Q}(\rho)$.** Although in Section 1 (relation (1.2)) we do not actually need a fundamental unit but rather just an odd power thereof, it is of some interest, however, to prove that $\varepsilon = 1 - \sigma$ is in fact fundamental, since this corrects an error in Table 3 of Brentjes [5]. Here the field discriminant is given incorrectly as $-4 \cdot 83$ and in fact the third element $\omega$ of the corresponding integer basis given in the table must be substituted by $(2 + \theta + \theta^2)/4$. The method for proving that $\varepsilon$ is a fundamental unit in $\mathbf{Q}(\rho)$ is based on the ideas of Ljunggren [13, Section 4]. This method has also been used in Finkelstein and London [9] and Tzanakis [20, Appendix A]. Since $\{1, \rho, \sigma\}$ is an integer basis, the algebraic integers of $\mathbf{Q}(\rho)$ have the form $(a + b\rho + c\rho^2)/4$, $a, b, c \in \mathbf{Z}$, where

$$(5.1) \qquad a + 2b \equiv a - 2c \equiv b + c \equiv 0 \bmod 4, \qquad a \equiv 0 \bmod 2.$$

If $\varepsilon$ is not a fundamental unit, then without loss of generality

$$(5.2) \qquad \lambda\varepsilon = \left[(a + b\rho + c\rho^2)/4\right]^n, \qquad \lambda = \pm 1, n \geqslant 2,$$

where $a$, $b$, $c$ are rational integers satisfying (5.1).

Let, in general, $\alpha'$, $\alpha''$ be the conjugates of $\alpha \in \mathbf{Q}(\rho)$. In view of (5.2) we have

$$\begin{pmatrix} 1 & \rho & \rho^2 \\ 1 & \rho' & \rho'^2 \\ 1 & \rho'' & \rho''^2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \pm 4 \begin{pmatrix} \varepsilon^{1/n} \\ \varepsilon'^{1/n} \\ \varepsilon''^{1/n} \end{pmatrix}.$$

Let $D$ denote the determinant of the $3 \times 3$ matrix. Then

$$|c| \leqslant 4D^{-1/2}\left\{|\varepsilon|^{1/n}|\rho'' - \rho'| + 2|\varepsilon'|^{1/n}|\rho' - \rho|\right\}, \tag{5.3}$$

$$|b| \leqslant 4D^{-1/2}\left\{|\rho||\varepsilon|^{1/n}|\rho'' - \rho'| + 2|\rho'||\varepsilon'|^{1/n}|\rho' - \rho|\right\}. \tag{5.4}$$

Now $|\rho| < 3.185$, $|\rho'| < 1.773$ (and $\rho'' = \overline{\rho'}$, the complex conjugate of $\rho'$), $|\rho'' - \rho'| < 1.556$, $|\rho' - \rho| < 4.840$, $|\varepsilon| < 2.832$, $|\varepsilon'| < 0.595$, $D = -2^4 \cdot 83$, $|D|^{1/2} \sim 36.441734$. Now, from (5.3),

$$|c| \leqslant 4|D|^{-1/2}\left\{|\varepsilon|^{1/2}|\rho'' - \rho'| + 2|\rho' - \rho|\right\} < 1.35,$$

and since we may suppose $c \leqslant 0$, it follows that $c = 0$ or $-1$. Also, from (5.4),

$$|b| \leqslant 4|D|^{-1/2}\left\{|\rho||\varepsilon|^{1/2}|\rho'' - \rho'| + 2|\rho'||\rho' - \rho|\right\} < 2.80,$$

so that $b = 0, \pm 1, \pm 2$. From (5.1) there is in addition the restriction $b + c \equiv 0 \bmod 4$, so that only the pairs $(b, c) = (0, 0)$, $(1, 1)$ need to be considered, of which the first pair can clearly be rejected. For the second pair $\operatorname{Norm}(a + \rho - \rho^2) = \pm 64$, and it is straightforward to see that only for $a = 2$ does the last relation hold. Then $(a + b\rho + c\rho^2)/4 = \varepsilon$, which is impossible in view of (5.2). Thus $\varepsilon$ is a fundamental unit.

**6. Appendix 2: The Finding of the Fundamental Units in the Quartic Fields.** We apply Berwick's method [1] and use the following result. Let $\mathbf{Q}(\theta)$ be a quartic field with negative discriminant and such that the minimum polynomial of $\theta$ over $\mathbf{Q}$ is not of the form $t^4 - 2at^2 + (a^2 - mb^2)$. Let $\theta'$, $\theta''$, $\overline{\theta''}$ be the (algebraic) conjugates of $\theta$, with $\theta$, $\theta'$ real and $\theta''$, $\overline{\theta''}$ complex conjugates. Then a pair of fundamental units in the field $\mathbf{Q}(\theta)$ are any two of the three defined by

$$\varepsilon > 1 \text{ and minimal}, \quad |\varepsilon'| < 1, \quad |\varepsilon''| < 1; \tag{6.1}$$

$$|\varepsilon| < 1, \quad \varepsilon' > 1 \text{ and minimal}, \quad |\varepsilon''| < 1; \tag{6.2}$$

$$|\varepsilon| < 1, \quad |\varepsilon'| < 1, \quad |\varepsilon''| > 1 \text{ and minimal}. \tag{6.3}$$

For the field $\mathbf{Q}(\theta)$ corresponding to (1.4) a pair of units $\varepsilon_1$, $\varepsilon_2$ is found using the relations (6.1), (6.3); for the field corresponding to (1.7) we use (6.3), (6.2); and for the field corresponding to (1.8) we use (6.2), (6.3).

We give as an illustrative example the details of the calculation only for the first field; the calculations for the other two fields are more extensive yet do not present any particular interest.

To find $\varepsilon_1$, we have the approximations

$$\theta = -0.74820, \quad \theta' = -0.34009, \quad \theta'' = 0.54415 + 1.90625i.$$

For the general unit $\varepsilon$ put $\varepsilon = x + y\theta + z\theta^2 + w\theta^3$; then we have to find $\varepsilon_1$ from the relations (taking 3 as an upper bound for $\varepsilon_1$):

$$1 < x - 0.74820y + 0.55981z - 0.41885w < 3, \tag{6.4}$$

$$(6.5)\qquad -1 < x - 0.34009y + 0.11566z - 0.03934w < 1,$$

$$(6.6)\qquad -1 < \mathrm{Re}(\varepsilon'') = x + 0.54415y - 3.33769z - 5.77085w < 1,$$

$$(6.7)\qquad -1 < \mathrm{Im}(\varepsilon'') = 1.90625y + 2.07457z - 5.23359w < 1,$$

$$(6.8)\qquad \mathrm{Re}(\varepsilon'')^2 + \mathrm{Im}(\varepsilon'')^2 < 1.$$

Now (6.4), (6.5) and (6.5), (6.6) give, respectively,

$$(6.9)\qquad 0 < -0.40811y + 0.44415z - 0.37951w < 4,$$

$$(6.10)\qquad -2 < -0.88424y + 3.45335z + 5.73151w < 2.$$

Then (6.7), (6.9) and (6.7), (6.10) give

$$(6.11)\qquad -0.40811 < 1.69331z - 2.85932w < 8.03311,$$

$$(6.12)\qquad -4.69674 < 8.41738z + 6.29791w < 4.69674,$$

and (6.11), (6.12) give

$$-11.38826 < 34.73230w < 75.57078,$$

and thus $w = -2, -1$, or 0.

If $w = -2$, then (6.12) forces $z = 2, 1$. Now if $z = 2$, then (6.7) forces $y = -8$, (6.6) forces $x = -1, 0$ and (6.4) is not satisfied; and if $z = 1$, then (6.7) forces $y = -7$, (6.6) forces $x = -5, -4$ and (6.5) is not satisfied. Similarly when $w = -1$, the only possibility that arises corresponds to the unit $-1 - 4\theta + \theta^2 - \theta^3$, satisfying all the inequalities. When $w = 0$, then (6.12) forces $z = 0$, and (6.7) forces $y = 0$. Thus $\varepsilon_1 = -1 - 4\theta + \theta^2 - \theta^3$.

One finds $\varepsilon_2 = \theta$ by exactly analogous computations which do not present any extra difficulty. Then $\varepsilon_1$, $\varepsilon_2$ form a pair of fundamental units in $\mathbf{Q}(\theta)$, although it is actually more convenient to work with the unit $-\varepsilon_1^{-1}\varepsilon_2 = 1 + \theta$ instead of $\varepsilon_1$.

Berwick's method is also applied for finding a pair of fundamental units in many quartic fields in [7], but an extensive use of a computer is made for this purpose.

Emmanuel College
Cambridge CB2 3AP, England

Department of Mathematics
University of Crete
Iraklion, Crete, Greece

1. W. E. H. Berwick, "Algebraic number fields with two independent units," *Proc. London Math. Soc.* v. 34, 1932, pp. 360–378.

2. G. Billing, "Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht eins," *Nova Acta Reg. Soc. Scient. Upsaliensis*, Ser. IV, v. 11, 1938.

3. B. J. Birch & W. Kuyk (eds.), *Modular Functions of One Variable* IV, Proc. Internat. Summer School, Antwerp 1972, Springer, 1975.

4. B. J. Birch & H. P. F. Swinnerton-Dyer, "Notes on elliptic curves I," *J Reine Angew. Math.*, v. 212, 1963, pp. 7–25; "Notes on elliptic curves II," *ibid.*, v. 218, 1965, pp. 79–108.

5. A. J. Brentjes, "A two-dimensional continued fraction algorithm for best approximations with an application in cubic number fields", *J. Reine Angew. Math.*, v. 326, 1981, pp. 18–44.

6. J. W. S. Cassels, "Diophantine equations with special reference to elliptic curves," *J. London Math. Soc.*, v. 41, 1966, pp. 193–291.

7. F. B. Coghlan & N. M. Stephens, "The Diophantine equation $x^3 - y^2 = k$," *Computers in Number Theory* (Atkin and Birch, eds.), Proc. Atlas Symp. No. 2, 1969, Academic Press, 1971.

8. B. N. Delone & D. K. Faddeev, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monographs, Vol. 10, Amer. Math. Soc., Providence, R. I., 1964.

9. R. Finkelstein & H. London, "On Mordell's equation $y^2 - k = x^3$: An interesting case of Sierpinski," *J. Number Theory*, v. 2, 1970, pp. 310–321.

10. R. HARTSHORNE, *Algebraic Geometry*, Springer-Verlag, 1977.

11. S. LANG, *Elliptic Curves, Diophantine Analysis*, Springer, 1978.

12. S. LANG, *Conjectured Diophantine Estimates on Elliptic Curves*, Shafarevich's 60th Birthday Volume, Birkhauser, 1983.

13. W. LJUNGGREN, "On the Diophantine equation $y^2 - k = x^3$, *Acta Arith.*, v. 8, 1963, pp. 451–463.

14. J.-F. MESTRE, "Construction d'une courbe elliptique de rang $\geqslant 12$," *Comptes Rendus*, v. 295, 1982, pp. 643–644.

15. L. J. MORDELL, *Diophantine Equations*, Academic Press, 1969.

16. G. SANSONE, "I punti di coordinate rationali e, in particolare, di coordinate intere della cubica ellittica $y^2 = x^3 - x + 1$," *Ann. Mat. Pura Appl.* (4), v. 125, 1980, pp. 1–11.

17. TH. SKOLEM, "The use of a $p$-adic method in the theory of diophantine equations," *Bull. Soc. Math. Belg.*, v. 7, 1955, pp. 83–95.

18. TH. SKOLEM, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen*, 8de Skand. mat. Kongr., Stockholm, 1934.

19. J. TATE, "Algorithm for determining the type of a singular fiber in an elliptic pencil," *Modular Functions of One Variable* IV (Birch and Kuyk, eds.), Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975, pp. 33–52.

20. N. TZANAKIS, "The Diophantine equation $x^3 - 3xy^2 - y^3 = 1$ and related equations," *J. Number Theory*. (To appear.)

21. A. WIMAN, "*Über die Punkte mit ganzzahligen Koordinaten auf gewissen Kurven dritter Ordnung*, 12te Skand. Matematikerkongressen, Lund, 1953, pp. 317–323 (1954).