MATHEMATICS OF COMPUTATION
VOLUME 39, NUMBER 159
JULY 1982, PAGES 235-238

The Integer Points on Three Related Elliptic Curves

By Andrew Bremner and Patrick Morton

Abstract. The integer points on the three elliptic curves $y^2 = 4cx^3 + 13$, $c = 1, 3, 9$, are found, with an application to coding theory. It is also shown that there are precisely three nonisomorphic cubic extensions of the rationals with discriminant $-3^5 \cdot 13$.

1. In [1] the Diophantine equation

$$y^2 = 4 \cdot 3^k + 13 \tag{1}$$

is shown to arise from coding theory, and its integer solutions are found. By considering congruence classes of k modulo 3, this equation gives rise to the three elliptic curves

$$y^2 = 4x^3 + 13, \tag{2}$$

$$y^2 = 12x^3 + 13, \tag{3}$$

$$y^2 = 36x^3 + 13. \tag{4}$$

We find here all integral solutions of (2), (3), (4), giving as a corollary all solutions to Eq. (1).

2. Since $Q(\sqrt{13})$ has class number 1, Eq. (2) immediately reduces to an equation

$$\frac{y + \sqrt{13}}{2} = \varepsilon^\kappa \left(a + b \frac{1 + \sqrt{13}}{2} \right)^3,$$

where $a, b \in \mathbf{Z}$, $\varepsilon = (3 + \sqrt{13})/2$ is a fundamental unit of $Q(\sqrt{13})$, and where without loss of generality $\kappa = 0, \pm 1$. Since $\alpha^3 \in \mathbf{Z}[\sqrt{13}]$ for every integer $\alpha \in Q(\sqrt{13})$, the case $\kappa = 0$ is impossible. Comparing coefficients of $\sqrt{13}$ in the two cases $\kappa = \pm 1$ gives respectively

$$\kappa = 1:\ 1 = a^3 + 6a^2b + 15ab^2 + 11b^3, \tag{5}$$

$$\kappa = -1:\ 1 = a^3 - 3a^2b + 6ab^2 - b^3. \tag{6}$$

Under the respective substitutions $(A, B) = (a + 2b, b)$, $(A, B) = (a - b, -b)$ both (5) and (6) reduce to

$$1 = A^3 + 3AB^2 - 3B^3. \tag{7}$$

We now work in $Q(\lambda)$, where $\lambda^3 + 3\lambda - 3 = 0$. It is straightforward to verify that the ring of integers in this field is $\mathbf{Z}[\lambda]$, and a fundamental unit is $\eta = 1 - \lambda$. (The

Received May 8, 1981; revised October 13, 1981.

1980 *Mathematics Subject Classification.* Primary 10B10; Secondary 12A30.

0025-5718/81/0000-0446/$01.75

method of [4, p. 7] may be easily adapted to give a proof that η is fundamental. See also [6].) Hence from (7), written as $\operatorname{Norm}(A - B\lambda) = 1$, we deduce that

$$A - B\lambda = \pm\eta^n \tag{8}$$

for some integer n. Note that the minus sign cannot arise because $\operatorname{Norm}\eta = 1$.

Now $\eta = 1 - \lambda$, $\eta^2 = 1 - 2\lambda + \lambda^2$, $\eta^3 = 1 + 3\xi$, with $\xi = -1 + \lambda^2$. If $n \equiv 2 \pmod 3$, then $\eta^n \equiv 1 - 2\lambda + \lambda^2 \pmod 3$, and (8) gives an impossible congruence (mod 3). Thus $n = 3N$ or $3N + 1$. If $n = 3N$, then we expand (8) in the form

$$A - B\lambda = (1 + 3\xi)^N = 1 + 3N\xi + 3^2\binom{N}{2}\xi^2 + \dots . \tag{9}$$

Comparing coefficients of λ^2 in (9) gives

$$0 = 3N + 3^2\binom{N}{2}(-5) + 3^3\binom{N}{3}(\cdot) + \dots . \tag{10}$$

If $3^\nu \| N$, then every term in this expansion except the first is divisible by $3^{\nu+2}$, giving a contradiction modulo $3^{\nu+2}$. Accordingly, $N = 0$ is the only possibility, which does indeed give a solution $(A, B) = (1, 0)$. Alternatively, we can invoke a result of Skolem [5] to show that (10) has at most one solution, which is thus $N = 0$. (See also [3, p. 54], and [7].)

Similarly, if $n = 3N + 1$, we obtain

$$\begin{aligned} A - B\lambda &= (1 - \lambda)(1 + 3\xi)^N \\ &= 1 - \lambda + 3(1 - \lambda)N\xi + 3^2(1 - \lambda)\binom{N}{2}\xi^2 + \dots, \end{aligned}$$

and comparing coefficients of λ^2 gives

$$0 = 3N + 3^2\binom{N}{2}(-8) + \dots .$$

As before, $N = 0$ is the only solution, corresponding to $(A, B) = (1, 1)$.

The solutions $(1, 0)$ and $(1, 1)$ of (7) give the solutions $(a, b) = (1, 0), (-1, 1)$ to (5) and $(a, b) = (1, 0), (0, -1)$ to (6), which in turn give $(x, y) = (-1, 3), (3, 11), (-1, -3), (3, -11)$ as the only solutions of (2).

3. Equation (3) reduces to the equation

$$\frac{y + \sqrt{13}}{2} = \varepsilon^\kappa\left(4 + \sqrt{13}\right)\left(a + b\frac{1 + \sqrt{13}}{2}\right)^3, \qquad \kappa = -2, -1,$$

where we choose the sign of y so that $y \equiv 1 \pmod 3$ (in order that $4 + \sqrt{13}$ divide the left-hand side). Comparing coefficients of $\sqrt{13}$ we have

$$\kappa = -2\colon 1 = -a^3 + 6a^2b - 3ab^2 + 5b^3, \tag{11}$$

$$\kappa = -1\colon 1 = a^3 + 3a^2b + 12ab^2 + 7b^3. \tag{12}$$

We write (11) in the form

$$1 = \operatorname{Norm}(A - B\theta), \tag{11$'$}$$

where $(A, B) = (-a + 2b, b)$ and $\theta^3 - 9\theta + 15 = 0$. The ring of integers in $Q(\theta)$ is $\mathbf{Z}[\theta]$, and a fundamental unit is $\rho = -53 + 18\theta + 9\theta^2$, so from (11′) we deduce that

$$A - B\theta = \pm\rho^n, \qquad n \in \mathbf{Z}.$$

Setting $\rho = 1 + 9\xi$, with $\xi = -6 + 2\theta + \theta^2$, and expanding 3-adically, we see by the same arguments as in Section 2 that $n = 0$ is the only solution, giving $(a, b) = (-1, 0)$ and $(x, y) = (1, -5)$.

Similarly, write (12) in the form

$$(12') \qquad 1 = \operatorname{Norm}(A - B\phi),$$

where $(A, B) = (a + b, b)$ and $\phi^3 + 9\phi - 3 = 0$. The ring of integers in $Q(\phi)$ is $\mathbf{Z}[\phi]$, and a fundamental unit is $\delta = 1 - 3\phi$, with Norm $\delta = 1$. From $A - B\phi = \delta^n$ we have the 3-adic expansion

$$A - B\phi = 1 - 3n\phi + 3^2\binom{n}{2}\phi^2 - 3^3\binom{n}{3}\phi^3 + \dots,$$

and comparing coefficients of ϕ^2 yields

$$0 = 3^2\binom{n}{2} + 3^4\binom{n}{4}(-9) + 3^5\binom{n}{5}(\cdot) + \dots.$$

By Skolem [5] this has at most two solutions. But $n = 0$ and $n = 1$ do give solutions, and hence these are the only ones. (Note that elementary arguments will also succeed as before.) Thus $(a, b) = (1, 0), (-2, 3)$, leading to $(x, y) = (-1, 1), (29, 541)$.

4. Treating Eq. (4) in the same manner, we deduce first of all that

$$\frac{y + \sqrt{13}}{2} = \varepsilon^\kappa\left(4 + \sqrt{13}\right)^2\left(a + b\frac{1 + \sqrt{13}}{2}\right)^3, \qquad \kappa = -2, -1,$$

where $y \equiv 1 \pmod 3$. Comparing coefficients gives the equations

$$(13) \qquad \kappa = -2\colon 1 = a^3 + 12a^2b + 21ab^2 + 19b^3,$$

$$(14) \qquad \kappa = -1\colon 1 = 5a^3 + 33a^2b + 78ab^2 + 59b^3.$$

In fact (13) is

$$1 = \operatorname{Norm}\left((a + 10b) + b\phi^2\right),$$

with ϕ defined as in (12′). Thus

$$a + 10b + b\phi^2 = \delta^n = 1 - 3n\phi + 3^2\binom{n}{2}\phi^2 - 3^3\binom{n}{3}\phi^3 + \dots,$$

and comparing coefficients of ϕ yields the only solution $n = 0$ as above, giving $(a, b) = (1, 0)$ and $(x, y) = (1, 7)$.

Further, it may be checked that the right-hand side of (14) is Norm Λ, where

$$\Lambda = (-19a - 43b) + (2a - b)\theta + (2a + 3b)\theta^2,$$

and θ is defined as in (11′). Thus $\Lambda = \pm\rho^n$, so that $\Lambda \equiv \pm 1 \pmod 3$. However this gives the congruences modulo 3:

$$-19a - 43b \equiv \pm 1, \quad 2a - b \equiv 0, \quad 2a + 3b \equiv 0,$$

which are clearly incompatible. Hence (14) has no solutions and $(1, \pm 7)$ are the only integer points on (4).

5. To summarize, we have

THEOREM. *The only integer points on*
(i) $y^2 = 4x^3 + 13$ *are* $(-1, \pm 3), (3, \pm 11)$;
(ii) $y^2 = 12x^3 + 13$ *are* $(1, \pm 5), (-1, \pm 1), (29, \pm 541)$;
(iii) $y^2 = 36x^3 + 13$ *are* $(1, \pm 7)$.

COROLLARY. *The only integer solutions of*

$$y^2 = 4 \cdot 3^k + 13$$

are $(k, y) = (1, \pm 5), (2, \pm 7), (3, \pm 11)$.

6. Remarks. The fields $Q(\theta)$, $Q(\phi)$, although having the same discriminant $-3^5 \cdot 13$, are nonisomorphic. In fact, there are precisely three cubic extensions of Q with this discriminant, the third generated by a root ψ of $x^3 - 9x + 24 = 0$. For, using Hasse [2], we see that if K is any such field, then $K(\sqrt{-39})$ is a cyclic cubic extension of $Q(\sqrt{-39})$ with conductor 9. Since the 3-Ringklassengruppe with conductor 9 in $Q(\sqrt{-39})$ is a product of 2 cyclic groups of order 3, the corresponding classfield has exactly 4 cubic subfields, each with a conductor (which has to be a rational integer) dividing 9. Similarly, the 3-Ringklassengruppe of conductor 3 has order 3, and so precisely one of these fields has conductor 3. (Note that $Q(\sqrt{-39})$ has class number 4, so none of the fields has conductor equal to 1.)

It only remains to verify that the fields $Q(\theta)$, $Q(\phi)$, $Q(\psi)$ are nonisomorphic. This may be seen from the fact that the rational prime 5 splits in $Q(\theta)$ but not in $Q(\phi)$, and that 2 splits in $Q(\psi)$ but not in either of $Q(\theta)$, $Q(\phi)$. (In fact, 2 is an inessential discriminant divisor in $Q(\psi)$.)

The above also shows that $Q(\lambda)$ is the unique cubic field of discriminant $-3^3 \cdot 13$.

Emmanuel College
Cambridge CB2 3AP, England

Department of Mathematics 253-37
California Institute of Technology
Pasadena, California 91125

1. A. BREMNER, R. CALDERBANK, P. HANLON, P. MORTON & J. WOLFSKILL, "Two-weight ternary codes and the equation $y^2 = 4 \cdot 3^a + 13$," *J. Number Theory*. (To appear.)

2. H. HASSE, "Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage," *Math. Z.*, v. 31, 1930, pp. 565–582.

3. D. J. LEWIS, *Diophantine Equations: p-Adic Methods*, Math. Assoc. Amer. Studies in Math., Vol 6, 1969, pp. 25–75.

4. E. S. SELMER, "Tables for the purely cubic field $k(\sqrt[3]{m})$," *Avh. Norske Vid.-Akad. Oslo I*, no. 5, 1955.

5. TH. SKOLEM, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichunger*, 8de Skad. mat. Kongr. Forh. Stockholm, 1934.

6. J. V. USPENSKY, "A method for finding units in cubic orders of a negative discriminant," *Trans. Amer. Math. Soc.*, v. 33, 1931, pp. 1–22.

7. E. T. VVANESOV, "On a question of a certain theorem of Skolem," *Akad. Nauk Armjan. SSR, Ser. Mat.*, v. 3, 1968, pp. 160–165.