In the same way as for G_{10}, it was found that the only chain-pair for which $M(\{a_n\}, \{\varepsilon_n\})$ might be greater than $546/4$ consists of the even a-chain from F with the zero ε-chain, for which, in fact, $M(\{a_n\}, \{\varepsilon_n\})$ is $547/4$. A complete period of the (sole) even a-chain of F is:

$$2, -2, -2, 2, 2, -2, -4, -2, 2, 4, 2, -2, -2, 2, 2, -2, 2, 2,$$
$$-2, -2, -2, 2, 2, -2, -2, 2, 2, 2, -2, -2.$$

Another form with a very low minimum is

$$f = (151, 739, 193),$$

for which

$$.31701 < 4M(f)/\Delta(f) < .31775.$$

It should perhaps be noted that for this form, as well as for several others with slightly higher minima which were computed precisely before F was found, $M(f)$ does not correspond to an even a-chain.

References

[1] E. S. Barnes and H. P. F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms II*, Acta Math. 88 (1952), p. 279-316.

[2] — *The inhomogeneous minima of binary quadratic forms III*, Acta Math. 92 (1954), p. 199-234.

[3] E. S. Barnes, *The inhomogeneous minima of binary quadratic forms IV*, Acta Math. 92 (1954), p. 235-264.

[4] H. Davenport, *Indefinite binary quadratic forms*, Quart. J. Math., Oxford Ser. (2) 1 (1950), p. 54-62.

[5] — *Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields*, Proc. London Math. Soc. (2) 53 (1951), p. 65-82.

[6] V. Ennola, *On the first inhomogeneous minimum of indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields*, Ann. Univ. Turkuensis Ser. AI, 28 (1958), p. 9-58.

[7] Jane Pitman, *The inhomogeneous minima of a sequence of symmetric Markov forms*, Acta Arithm. 5 (1958), p. 81-116.

GIRTON COLLEGE, CAMBRIDGE

Reçu par la Rédaction le 1. 10. 1959

ACTA ARITHMETICA
VI (1960)

On a diophantine equation

by

J. W. S. Cassels (Cambridge)

The following theorem answers a problem put to me orally by Professor Mordell. He tells me that he had known about the problem for some time and that it had several times been proposed to him (1).

Theorem I. *The system of equations*

$$r+s+t = rst = 1 \tag{1}$$

is insoluble in rationals r, s, t.

As Professor Mordell pointed out, this is equivalent to the following

Theorem II. *The only rational solutions of*

$$(r+s+t)^3 = rst \tag{2}$$

have

$$rst = 0.$$

The equation of Theorem II represents a curve of genus 1 in homogeneous coordinates. It is, in fact, a particular case of an equation considered by Mordell [4]. He shows that it can be transformed into an apparently quite different shape. Since (2) is homogeneous, we may suppose without loss of generality that r, s, t are integers without common factor. It follows from (2) that r, s, t are coprime in pairs, and so, by (2) again,

$$r = \varrho^3, \quad s = \sigma^3, \quad t = \tau^3$$

where ϱ, σ, τ are integers and

$$\varrho^3+\sigma^3+\tau^3 = \varrho\sigma\tau. \tag{3}$$

This is a special case, as Mordell remarks, of the equation

$$a\varrho^3+b\sigma^3+c\tau^3+d\varrho\sigma\tau = 0 \tag{3'}$$

considered by Sylvester [10] and Hurwitz [5] (cf. [9], p. 80-81).

(1) I am grateful to Professor Mordell for his comments on my MS.

The proof of the theorems depends on the well-known standard techniques for dealing with curves of genus 1 (cf. [1], [7], [8]). Hence we only sketch the proof enunciating the principal steps as lemmas usually without proof. Following Mordell again, we put

$$r+s+t = -\tfrac{1}{4}xt, \quad r-s = \tfrac{1}{4}yt.$$

The equation (2) takes the shape

$$y^2 = x^3+(x+4)^2. \tag{4}$$

We consider the Poincaré-Mordell-Weil group of points on (4) with rational coordinates, taking the point at infinity on the curve as the zero element of the group.

LEMMA 1. *The only rational points on* (4) *of finite order are those with* $x = 0$.

This follows at once from a criterion of Nagell [6] rediscovered by Lutz [3] (cf. [9], p. 78-79, Sätze 12a, b). Alternatively, one may remark that Lemma 1 is a special case of the result of Hurwitz [5] about the curve (3′) (cf. also [9], p. 80, Satz 13).

LEMMA 2. *If* (x, y) *is a rational point on* (4), *then*

$$x = X/T^2, \quad y = Y/T^3, \tag{5}$$

where X, Y, T *are integers and*

$$\text{g.c.d.}\,(X, T) = \text{g.c.d.}\,(Y, T) = 1. \tag{6}$$

LEMMA 3. *Let* $\mathfrak{K}$ *be the field defined by adjoining a root of*

$$\lambda^3-\lambda-2 = 0 \tag{7}$$

to the rationals. Then

(i) $\mathfrak{K}$ *has discriminant* -104, *class number* 1 *and fundamental unit*

$$\varepsilon = 1+\lambda-\lambda^2, \tag{8}$$

where

$$\text{Norm}\,\varepsilon = +1.$$

A basis for the integers of $\mathfrak{K}$ *over the rational integers is* $1, \lambda, \lambda^2$.

(ii) *The element*

$$\Phi = \lambda^2-2\lambda-1 \tag{8′}$$

of $\mathfrak{K}$ *satisfies the equation*

$$\Phi^3+(\Phi+4)^2 = 0, \tag{9}$$

the discriminant of which is 64 (-104).

(iii) *The only rational primes which ramify in* $\mathfrak{K}$ *are* 2 *and* 13. *These decompose according to the rule* (2)

$$[2] = \mathfrak{p}\mathfrak{q}^2, \quad [13] = \mathfrak{r}\mathfrak{s}^2, \tag{10}$$

where

$$\begin{aligned} \Phi &\equiv 1 \pmod{\mathfrak{p}}, & \Phi &\equiv 0 \pmod{\mathfrak{q}}, \\ \Phi &\equiv -3 \pmod{\mathfrak{r}}, & \Phi &\equiv 1 \pmod{\mathfrak{s}^2}. \end{aligned} \tag{11}$$

This is all routine. Perhaps the best way to verify that ε is a fundamental unit is that given by Delaunay and Faddeev [2], p. 73-76. All we actually need (3) is that ε is not a square, and this follows from $\varepsilon \equiv -5 \pmod{\mathfrak{r}}$, since -5 is not a quadratic residue of 13.

LEMMA 4. $[X-\Phi T^2]$ *is the square of an ideal.*

The equation (4) takes the shape

$$Y^2 = (X-\Phi T^2)(X-\Phi' T^2)(X-\Phi'' T^2),$$

where Φ is given by (8) and Φ', Φ'' are its conjugates. By (6) any common divisor of $X-\Phi T^2$ and $X-\Phi' T^2$ divides $\Phi-\Phi'$, and so also 64.104 by Lemma 3 (ii). Hence

$$[X-\Phi T^2] = \mathfrak{a}_2\mathfrak{a}_{13}\mathfrak{b}^2,$$

where $\mathfrak{a}_2, \mathfrak{a}_{13}, \mathfrak{b}$ are integral ideals, $\mathfrak{b}$ is prime to 26 and all the prime ideals dividing $\mathfrak{a}_2, \mathfrak{a}_{13}$ divide 2, 13 respectively. But now, by Lemma 3 (iii) and since g.c.d. $(X, T^2) = 1$, the ideals $\mathfrak{a}_2, \mathfrak{a}_{13}$ must be powers of prime ideals (4). Since

$$Y^2 = \text{Norm}(X-\Phi T^2), \tag{12}$$

the truth of Lemma 4 follows.

COROLLARY. *Either*

$$X-\Phi T^2 = \alpha^2$$

or

$$X-\Phi T^2 = \varepsilon\alpha^2$$

where $\alpha \in \mathfrak{K}$.

For $\text{Norm}(X-\Phi T^2) > 0$, by (12).

LEMMA 5. *Suppose that*

$$X-\Phi T^2 = \alpha^2. \tag{13}$$

---

(2) We use square brackets to denote principle ideals.

(3) Indeed we do not even need this. Since we show from congruence considerations that (14) below does not hold, it is easy to see that ε cannot be a square.

(4) For example, if $X-\Phi T^2$ were divisible by $\mathfrak{p}\mathfrak{q}$ then we should have $X \equiv 0 \pmod 2$ from $\mathfrak{q}$ and $X \equiv T^2 \pmod 2$ from $\mathfrak{p}$.

Then the point $(X/T^2, Y/T^3)$ *is twice a rational point in the sense of the Poincaré-Mordell-Weil group.*

This follows substantially from the general theory (cf. [1], [7], [8], [9], [11], [12]). Alternatively, put

$$a = f+g\Phi+h\Phi^2,$$

where f, g, h are rational but not necessarily integral. On equating the coefficients of Φ and Φ^2 on both sides of (13) (using (9)) and eliminating f it is easy to see that

$$T/h = y_1, \quad (g-h)/h = x_1$$

satisfy $y_1^2 = x_1^3+(x_1+4)^2$. The point (x_1, y_1) is that required.

COROLLARY. *If there are rational points on* (4) *with* $x \neq 0$, *then there are such points with*

$$X-\Phi T^2 = \varepsilon a^2. \tag{14}$$

This follows from Lemmas 1 and 5, together with Mordell's theorem that the group of rational points has a finite basis.

We now put

$$a = f+g\lambda+h\lambda^2$$

in (14), where, by Lemma 3 (i), f, g, h are integers. On using (7), (8) and (8′) and equating the coefficients of λ and λ^2 on both sides of (14) we get

$$f^2-g^2-2fh+4gh-h^2 = 2T^2, \tag{15}$$

$$-f^2+2fg-2gh+2h^2 = -T^2. \tag{16}$$

Hence, on eliminating T,

$$-f^2+4fg-g^2-2fh+3h^2 = 0. \tag{17}$$

On putting

$$h = f+k \tag{18}$$

in (17) and (16) we get

$$4f(g+k) = g^2-3k^2 \tag{19}$$

and

$$f^2-2gk+4fk+2k^2 = -T^2 \tag{20}$$

respectively. Hence, on eliminating f, we have

$$-\{4(g+k)T\}^2 = (g^2-3k^2)^2+16k(g+k)(g^2-3k^2)+16(2k^2-2gk)(g+k)^2. \tag{21}$$

If $g = k = 0$, the equations (18) and (16) show that $T^2 < 0$, which is impossible. If $(g, k) \neq (0, 0)$, we shall show that (21) is impossible by considering congruences to powers of 2.

Put

$$k = 2^\mu k_1, \quad g = 2^\mu g_1$$

where

$$2 \nmid \text{g.c.d.}(k_1, g_1).$$

We distinguish two cases. Suppose, first, that $2|k_1g_1$. Then the right hand side of (21) is

$$2^{4\mu}M,$$

where

$$M \equiv \begin{cases} (g_1^2-3k_1^2)^2 \pmod{16}, \\ 1 \pmod 8. \end{cases}$$

Secondly, suppose that $2 \nmid k_1g_1$. Then

$$g_1^2-3k_1^2 \equiv 2 \pmod 4, \quad k_1-g_1 \equiv k_1+g_1 \equiv 0 \pmod 2.$$

Hence the right hand side of (21) is

$$2^{4\mu+2}M,$$

where

$$M \equiv \begin{cases} \left(\dfrac{g_1^2-3k_1^2}{2}\right)^2 \pmod{16} \\ 1 \pmod 8. \end{cases}$$

Hence in neither of these two cases can $-M$ be a perfect square. Hence there are no solutions of (21) with $(g, k) \neq (0,0)$. By Lemma 5 Corollary this proves the theorems.

References

[1] J. W. S. Cassels, *The rational solutions of the diophantine equation* $Y^2 = X^3-D$, Acta Math. Stockholm 82 (1950), p. 243-273.

[2] B. N. Delaunay, D. K. Faddeev, *The theory of irrationals of the third degree* (in Russian), Trudy Mat. Inst. Steklov. 11 (1950).

[3] E. Lutz, *Sur l'equation* $y^2 = x^3-Ax-B$ *dans les corps* $\mathfrak{p}$ *— adiques*, J. f. Math. 177 (1937), p. 238-247.

[4] L. J. Mordell. *The diophantine equation* $x^3+y^3+z^3+kxyz = 0$, Colloque sur la théorie des nombres, Bruxelles, 1955, p. 67-76.

[5] A. Hurwitz, *Über ternäre diophantische Gleichungen dritten Grades*, Werke II, p. 465-468 (= Vierteljahrschrift d. Naturf. Ges. in Zürich 62 (1917), p. 207-229).

[6] T. Nagell, *Solutions de quelques problèmes dans la théorie arithmetique des cubiques planes du premier genre*, Vid. Akad. Skrifter Oslo 1 (1935), Nr 1.

[7] G. Billing, *Beiträge zur arithmetischen Theorie ebener kubischer Kurven*, Nova Acta Reg. Soc. Scient. Upsaliensis (IV) 9 (1938), p. 1-165.

[8] E. S. Selmer, *The diophantine equation* $ax^3+by^3+cz^3 = 0$, Acta Math. Stockholm 85 (1951), p. 203-362.

[9] T. Skolem, *Diophantische Gleichungen*, Ergeb. d. Math. 54 (1938).

[10] J. J. Sylvester, *On certain ternary cubic-form equations*, Coll. Papers. (1909) III, p. 312-319 (= Amer. J. Math. 2 (1878), p. 280-285, 357-393 and 3 (1880), p. 58-88, 179-189).

[11] A. Weil, *L'arithmetique sur les courbes algebriques*, Acta Math. Stockholm 52 (1928-9), p. 281-315.

[12] — *Sur un théorème de Mordell*, Bull. des Sci. Math. (2) 54 (1930), p. 182-191.

Reçu par la Rédaction le 3. 10. 1959

ACTA ARITHMETICA
VI (1960)

The cyclotomic numbers of order twelve*

by

A. L. Whiteman (Princeton, N. J.)

1. Introduction. Let p be an odd prime and g a fixed primitive root of p. Let e be a divisor of $p-1$ and put $p-1 = ef$. The cyclotomic number $(i, j) = (i, j)_e$ is the number of values of y, $1 \leqslant y \leqslant p-2$, for which

$$y \equiv g^{es+i}, \quad 1+y \equiv g^{et+j} \pmod{p}, \tag{1.1}$$

where the values of s and t are each selected from the integers $0, 1, \ldots, f-1$. A central problem in the theory of cyclotomy is to find exact formulas for the constants (i, j). Until now complete solutions have been obtained only in the cases $e = 2, 3, 4, 5, 6, 8, 10$ and 16. References to these solutions are given in R. H. Bruck's report [2] on the computational aspects of the problem. Since the publication of [2] two more articles [11], [12] relevant to the subject have appeared.

This paper is concerned with the case $e = 12$. The systematic study of this case was initiated by L. E. Dickson [4]. The foundation for his work is the following theorem ([4], Theorem 12): when $e = 12$, the 144 cyclotomic constants (i, j) depend solely upon the decompositions $p = x^2+4y^2$ and $p = A^2+3B^2$ of the prime $p = 12f+1$, where $x \equiv 1 \pmod 4$ and $A \equiv 1 \pmod 6$. In a number of instances Dickson obtained explicit formulas to illustrate this theorem. Two examples are as follows. If 2 is a cubic residue of p and 3 is a biquadratic residue of p, then

$$144(0,0)_{12} = p-35-32A-30x \pm 24(A+x) \qquad (f \text{ even}), \tag{1.2}$$

$$144(0,2)_{12} = p+1-2A+24B-12x \qquad (f \text{ odd}). \tag{1.3}$$

The conditions of the theorem determine x and A uniquely and determine y and B uniquely except for sign. The ambiguous sign in (1.2) is

* Research done in part under Contract NSF G-5877 between the National Science Foundation and the University of Southern California, and in part with support from the Institute for Advanced Study.