ON THE DIOPHANTINE EQUATION $2^x = 3^y + 13^z$

To Professor MOTOKITI KONDÔ on his seventieth birthday

SABURÔ UCHIYAMA

Extending the anterior results due to T. Nagell [7] and to A. Makowski [6], T. Hadano [3] recently determined by an elementary, largely congruencial argument, the solutions in non-negative integers x, y, z of all the exponential Diophantine epuations

$$a^x = b^y + c^z$$

in which a, b and c are distinct prime numbers $\leqq 17$, but one equation

$$2^x = 3^y + 13^z. \tag{1}$$

This equation can also be treated by a well-known traditional method, and we shall show in this paper that there are just four solutions in x, y, z of the equation (1). Indeed, we shall prove the following

Theorem. *The only solutions in non-negative integers x, y, z of the Diophantine equation* (1) *are given by*

$$(x, y, z) = (1, 0, 0),\ (2, 1, 0),\ (4, 1, 1) \text{ and } (8, 5, 1).$$

We note that this result has been announced without proof in [4].

1. Obviously there are no solutions x, y, z of the equation (1) with $x=0$, and $y=z=0$ is the only solution of it with $x=1$.

If $x>0$, $y>0$ and $z=0$, then the equation (1) is

$$2^x = 3^y + 1, \text{ or } 2^x - 3^y = 1.$$

Here, we need the following result due to W. J. LeVeque [5].

Lemma. *Let a and b be given positive integers. The equation*

$$a^x - b^y = 1$$

has at most one solution in positive integers x, y if a is even and b is odd. If

$$2^\alpha \parallel a \text{ and } 2^\beta \parallel b+1,$$

the only possible solution is with $x=\beta/\alpha$ if $\alpha>1$, and with $x=1$ or β if $\alpha=1$.

The equation $2^x - 3^y = 1$ has a solution $(x, y) = (2, 1)$ and this is its unique solution since, in view of the lemma, it has at most one solution.

Thus, there are just two solutions x, y, z of (1) with $z = 0$.

If $x > 0$, $y = 0$ and $z > 0$, then the equation (1) becomes

$$2^x = 1 + 13^z, \text{ or } 2^x - 13^z = 1,$$

which has no solutions x, z, since, again by the lemma above, this last equation has at most one solution, and the only possible solution is with $x = 1$.

Therefore, in dealing with the equation (1), we may assume henthforth that $x > 0$, $y > 0$ and $z > 0$.

2. We now proceed by a series of propositions. In propositions (i), (ii) and (iii) below the integers x, y, z are assumed to satisfy the equation (1).

(i) $x \equiv 0$ (mnd 2) and $y \equiv 1$ (mod 2), if $y > 0$.

Indeed, we have by (1) $2^x \equiv 1$ (mod 3), which implies $x \equiv 0$ (mod 2) (since 2 is the (unique) primitive root of 3). Write $x = 2\xi$. Then we see from (1)

$$2^{2\xi} = 3^y + 13^z,$$

so that $0 \equiv (-1)^y + 1$ (mod 4), $y \equiv 1$ (mod 2).

(ii) $x \equiv 0$ (mod 4) if $y > 0$ and $z > 0$.

Since 2 is a primitive root of 13 and $3 \equiv 2^4$ (mod 13), we have

$$2^x = 3^y + 13^z \equiv 3^y \equiv 2^{4y} \pmod{13}.$$

Hence $x \equiv 4y$ (mod 12), or $x \equiv 0$ (mod 4).

(iii) $y \equiv z \equiv 1$ (mod 4) if $y > 0$ and $z > 0$.

By (ii) we have $x = 4\xi$ for some integer ξ. Suppose that z be even and put $z = 2\zeta$. Then, since 3 is a primitive root of 17 and $13 \equiv 3^4$ (mod 17), we have from $2^{4\xi} = 3^y + 13^{2\zeta}$

$$(-1)^\xi \equiv 3^y + 3^{8\zeta} \equiv 3^y + (-1)^\zeta \pmod{17}.$$

It is impossible that ξ and ζ are both odd or both even. If ξ is odd and ζ is even, then

$$3^y \equiv -2 \pmod{17}, \quad y \equiv 6 \pmod{16},$$

and if ξ is even and ζ is odd, then

$$3^y \equiv 2 \pmod{17},\ y \equiv 14 \pmod{16};$$

either choice is again impossible in view of (i).

Suppose now that z be odd. Since 3 is a primitive root of 5, we have

$$2^{4\xi} = 3^y + 13^z,\ 1 \equiv 3^y + 3^z \pmod 5).$$

But $3^3 \equiv 2 \pmod 5$. Hence. the only possibility is with $y \equiv z \equiv 1 \pmod 4$, as asserted.

In the equation (1) we write

$$x = 4\xi,\ y = 4\eta + 1,\ z = 4\zeta + 1,$$

where ξ, η, ζ are integers with $\xi \geqq 1$, $\eta \geqq 0$, $\zeta \geqq 0$, and put

$$Y = 3^{2\eta},\ Z = 13^{2\zeta}.$$

Then we have

$$3 \cdot 2^{4\xi} = (3Y)^2 + 39Z^2. \tag{2}$$

3. Now, let us consider the imaginary quadratic number field $\mathbf{Q}(\sqrt{-39})$ whose class number is 4 (cf. [2; Table III, Part 1 (continued), p. 264]; also [1; Table 5, p. 484]). In this field we have the decompositions into prime ideals

$$2 = PP',\ 3 = Q^2,$$

where

$$P = \left(2, \frac{1+\sqrt{-39}}{2}\right),\ P' = \left(2, \frac{1-\sqrt{-39}}{2}\right),\ (P, P') = 1$$

and

$$Q = (3,\ \sqrt{-39}).$$

It follows from (2) that

$$\left(\frac{3Y + Z\sqrt{-39}}{2}\right)\left(\frac{3Y - Z\sqrt{-39}}{2}\right) = Q^2 (PP')^{4\xi - 2},$$

any common divisors of the two factors on the left-hand side dividing $3 = Q^2$. Hence, we must have (for an appropriate choice of signs $\pm$)

$$\left(\frac{3Y \pm Z\sqrt{-39}}{2}\right) = QP^{4\xi-2}$$

or, on squaring both sides and then dividing them by 3,

$$\left(\frac{3Y^2 - 13Z^2 \pm 2YZ\sqrt{-39}}{4}\right) = \left(\frac{5 + \sqrt{-39}}{2}\right)^{2\xi - 1}$$

since

$$P^2=\left(4, \frac{5+\sqrt{-39}}{2}\right), \quad P^4=\left(\frac{5+\sqrt{-39}}{2}\right).$$

The units in the field $\mathbf{Q}(\sqrt{-39})$ being ± 1, we obtain the relation

$$\pm\frac{3Y^2-13Z^2\pm 2YZ\sqrt{-39}}{4}=\left(\frac{5+\sqrt{-39}}{2}\right)^{2\xi-1}$$

Now, we define the sequences of rational integers (u_n) and (v_n) ($n=0, 1, 2, \cdots$) by setting

$$\left(\frac{5+\sqrt{-39}}{2}\right)^n=\frac{u_n+v_n\sqrt{-39}}{2};$$

it is easy to see that these sequences are determined by the relations

$$u_0=2, \ u_1=5, \ u_{n+1}=5u_n-16u_{n-1} \ (n\geqq 1),$$
$$v_0=0, \ v_1=1, \ v_{n+1}=5v_n-16v_{n-1} \ (n\geqq 1).$$

In fact, we have

$$(3) \quad \begin{cases} u_n=\left(\frac{5+\sqrt{-39}}{2}\right)^n+\left(\frac{5-\sqrt{-39}}{2}\right)^n \\ v_n=\frac{1}{\sqrt{-39}}\left\{\left(\frac{5+\sqrt{-39}}{2}\right)^n-\left(\frac{5-\sqrt{-39}}{2}\right)^n\right\} \end{cases}.$$

Note that we have $u_n\neq 0$ for $n\geqq 0$ and $v_n\neq 0$ for $n\geqq 1$.

Using the recurrence relations for (u_n) and (v_n), we find by induction on n that

(iv) $u_n\equiv v_n\equiv 1 \pmod 4$ for all $n\geqq 1$.

The next two propositions are easy deductions from (3).

(v) $2v_{m+n}=u_mv_n+u_nv_m$ for $m\geqq 0$, $n\geqq 0$.

(vi) $v_{2n}=u_nv_n$ for $n\geqq 0$.

(vii) If m (>0) divides n then v_m divides v_n.

Indeed, $v_{2m}=u_mv_m\equiv 0$ (mnd v_m) by (vi). Suppose now that $v_{km}\equiv 0 \pmod{v_m}$ for some $k\geqq 2$. Then, by (v),

$$2v_{(k+1)m}=u_{km}v_m+u_mv_{km}\equiv 0 \pmod{v_m}.$$

By (iv) v_m is odd for $m>0$; hence $v_{(k+1)m}\equiv 0 \pmod{v_m}$, completing the induction.

(viii) $(v_n, v_{n+1})=1$ for $n\geqq 0$.

Here, (a, b) denotes the greatest common divisor of the integers a and b. Let $d\,|\,(v_n,\ v_{n+1})$. Then $d\,|\,v_{n+1}=5v_n-16v_{n-1}$. Hence $d\,|\,v_{n-1}$ and so $d\,|\,(v_{n-1},\ v_n)$. Continuing this process we ultimately arrive at $d\,|\,(v_0,\ v_1)=1$, that is, $d=1$.

(ix) $(u_n,\ v_n)=1$ for $n\geqq 1$.

Let $d\,|\,(u_n, v_n)$. Then d is odd and

$$d\,|\,2v_{n+1}=u_nv_1+u_1v_n$$

which implies that $d\,|\,(v_n, v_{n+1})=1$ by (viii). Hence the result.

(x) $(v_m, v_n)=|v_{(m,n)}|$ if $m+n>0$.

If one of m, n is 0, the result is obvious. Suppose now that $m>0$, $n>0$, and put $d=(m, n)$, $v=(v_m, v_n)$. By (vii), $v\,|\,v_{jm}$ for any $j>0$ and $v\,|\,v_{kn}$ for any $k>0$. We have $am-bn=d$ for some positive integers a, b. We find on account of (ix)

$$v\,|\,2v_{aw}=u_{am-n}v_n+u_nv_{am-n},\quad v\,|\,v_{am-n},$$
$$v\,|\,2v_{am-n}=u_{am-2n}v_n+u_nv_{am-2n},\quad v\,|\,v_{am-2n},$$

and repeating this procedure we get finally

$$v\,|\,2v_{am-(b-1)n}=u_{am-bn}v_n+u_nv_{am-bn},\quad v\,|\,v_d.$$

Since $v_d\,|\,v$ is obvious from (vii), we mnst have $v=|v_d|$.

We are now in the final stage of our search of the solutions of the equation (1).

From what we have seen above it will follow that if

$$2^x=3^y+13^z$$

and

$$x=4\xi,\ y=4\eta+1,\ z=4\zeta+1,$$

then we must have

$$|3Y^2-13Z^2|=2|u_{2\xi-1}|,\quad YZ=|v_{2\xi-1}|$$

with $Y=3^{2\eta}$, $Z=13^{2\zeta}$.

It will be easier to deal with YZ than to do with $3Y^2-13Z^2$. Here, we find it convenient to have a table of values of v_n for $0\leqq n\leqq 13$.

$v_0=0$
$v_1=1$
$v_2=5$
$v_3=9=3^2$

$$v_4=-35=-5\cdot 7$$
$$v_5=-319=-11\cdot 29$$
$$v_6=-1035=-3^2\cdot 5\cdot 23$$
$$v_7=-71$$
$$v_8=16205=5\cdot 7\cdot 463$$
$$v_9=82161=3^3\cdot 17\cdot 179$$
$$v_{10}=151525=5^2\cdot 11\cdot 19\cdot 29$$
$$v_{11}=-556951=-241\cdot 2311$$
$$v_{12}=-5209155=-3^2\cdot 5\cdot 7\cdot 23\cdot 719$$
$$v_{13}=-17134559=-13\cdot 313\cdot 4211$$

The use of the next and final proposition (xi), which seems to be of some interest in itself, can in fact be avoided in our argument.

(xi) $v_n \neq \pm 1$ for $n>1$.

By (iv) we have $v_n \equiv 1 \pmod 4$ for $n \geqq 1$, so that $v_n \neq -1$ for $n \geqq 1$. We have by (vii) $v_{2m} \equiv 0 \pmod{v_2}$ with $v_2=5$, whence $v_{2m} \neq \pm 1$ for $m \geqq 1$. Using (iv) again we find for $n \geqq 2$

$$v_{n+1}=5v_n-16v_{n-1}\equiv 5v_n+16 \pmod{32},$$
$$v_{n+2}\equiv 5(5v_n+16)+16\equiv 5^2 v_n \pmod{32},$$

which implies $v_{n+8}\equiv v_n \pmod{32}$ for $n \geqq 2$, since $5^8 \equiv 1 \pmod{32}$. Thus we have for $m \geqq 0$

$$v_{8m+3}\equiv v_3=9,\quad v_{8m+7}\equiv v_7\equiv 25,\quad v_{8m+9}\equiv v_9\equiv 17 \pmod{32}.$$

By (v) we have for $m \geqq 1$

$$2v_{4m+1}=u_4 v_{4m-3}+u_{4m-3}v_4,$$

where $u_4=-463\equiv -1 \pmod 7$ and $v_4=-35\equiv 0 \pmod 7$. It follows from this that

$$2v_{4m+1}\equiv -v_{4m-3} \pmod 7,$$

or

$$v_{4m+1}\equiv 3v_{4m-3} \pmod 7,$$

so that

$$v_{4m+1}\equiv 3^m \pmod 7$$

which is valid for all $m \geqq 0$. Hence we have for $m \geqq 0$

$$v_{8m+5}\equiv 3^{2m+1}\equiv 3\cdot 2^m \pmod 7$$

and so

$$v_{8m+5} \equiv 3, 6 \text{ or } 5 \pmod 7$$

according as $m \equiv 0$, 1 or 2 (mod 3). We thus have proved that $v_{2m+1} \neq 1$ for $m > 0$. This completes the proof of (xi). *)

Now, suppose that the equation (1) admit a solution x, y, z with $x > 0$, $y > 0$, $z > 0$. We shall first show that such a solution may exist only with $z = 1$, i. e. with $\zeta = 0$. Indeed, if $z > 1$ then $z = 4\zeta + 1 \geqq 5$ and $YZ = |v_{2\xi-1}|$ would be divisible by 13. But, in view of (x), v_n is divisible by 13 if and only if n itself is divisible by 13, and so $v_{2\xi-1}$ should then be a multiple of v_{13} which has extra prime factors other than 3 and 13. Hence $YZ = |v_{2\xi-1}|$ is impossible if $z > 1$.

Thus, it remains only to examine the case of $z = 1$, i. e. the case of $YZ = Y = 3^{\zeta\eta}$ is a power of 3. If $\eta = 0$ then $Y = 1 = v_1$ by (xi), and this gives the solution $x = 4$, $y = 1$, $z = 1$. If $\eta > 0$ and $Y = |v_{2\xi-1}|$, then $2\xi - 1 = 3n$ for some $n > 0$. If $3 | n$ then $3^2 = 9 | 3n$, so that $v_{2\xi-1}$ is is divisible by v_9 which has prime factors other than 3. Therefore, we must have $(n, 3) = 1$. But then $(v_{3n}, v_9) = v_3 = 3^2$, where $3^3 | v_9$. It follows that $3^2 \| v_{3n}$, $Y = |v_{3n}| = 3^2$, which implies $n = 1$ (since $v_n | v_{3n}$ and since by (xi) v_n has a prime factor $\neq 3$ if $n > 1$), $2\xi - 1 = 3$, $\eta = 1$, giving the solution $x = 4\xi = 8$, $y = 4\eta + 1 = 5$, $z = 1$.

This concludes the proof of our theorem.

Remark. In the concluding part of our proof of the theorem we had two occasions to quote the proposition (xi). However, as is readily seen, this part could be disposed of without appealing to (xi) and with a particular reference to the original equation (1) instead.

REFERENCES

[1] Z. I. BOREVIČ and I. R. ŠAFAREVIČ: The Theory of Numbers. 2nd ed. Nauka, Moscow, 1972 (in Russian).

[2] H. COHN: A Second Course in Number Theory. John Wiley & Sons, Inc., New York and London, 1962.

[3] T. HADANO: On the Diophantine equation $a^x = b^y + c^z$. Math. J. Okayama Univ. **19** (1976), 25—29.

[4] Intrnational Symposium on Algebraic Number Theory (Abstracts of Contributed Papers). March 22—27, 1976. Kyoto, Japan.

[5] W. J. LEVEQUE: On the equation $a^x - b^y = 1$. Amer. Journ. Math. **74** (1952), 325—331.

*) In a private communication with the author Mr. K. Tanahashi has given a proof of (xi), based on a principle somewhat different from ours.

[6] A. MAKOWSKI: On the Diophantine equation $2^x + 11^y = 5^z$. Nordisk Mat. Tidskr. **7** (1959), 81.
[7] T. NAGELL: Sur une classe d'équations exponentielles. Ark. för Mat. **3** (1958), 569—581.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received October 30, 1976)