As before, the minimal relation $b_1 \log a_1 + \ldots + b_n \log a_n = 0$ has coefficients $b_j = u^{j-1} v^{n-j}$, and these satisfy

$$b_k > A(n) \prod_{j \neq k} V_j,$$

justifying our earlier assertions.

References

[1] A. Baker, *The theory of linear forms in logarithms*, A. Baker and D. W. Masser (eds.), *Transcendence theory: advances and applications*, Academic Press, 1977, Chapter 1.

[2] D. Bertrand, *Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe*, Compositio Math. 37 (1978), pp. 21–50.

[3] A. Bijlsma, *Simultaneous approximations in transcendental number theory*, Math. Centrum Tracts, number 94, Amsterdam 1978.

[4] A. Bijlsma and P. L. Cijsouw, *Degree-free bounds for dependence relations*, J. Austral. Math. Soc. (A) 31 (1981), pp. 496–507.

[5] J. W. S. Cassels, *An introduction to the geometry of numbers*, Second edition, Springer Verlag, 1971.

[6] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), pp. 391–401.

[7] J. H. Loxton and A. J. van der Poorten, *Multiplicative relations in number fields*, Bull. Austral. Math. Soc. 16 (1977), pp. 83–106. *Corrigenda*, ibid. 17 (1977), pp. 151–155.

SCHOOL OF MATHEMATICS
UNIVERSITY OF NEW SOUTH WALES
Kensington, N.S.W., 2033, Australia

SCHOOL OF MATHEMATICS AND PHYSICS
MACQUARIE UNIVERSITY
North Ryde, N.S.W., 2113, Australia

Received on 19. 9. 1981
and in revised form on 24. 3. 1982 (1268)

ACTA ARITHMETICA
XLII (1983)

On the diophantine equation $y^2 + D^m = p^n$

by

MASAO TOYOIZUMI (Tokyo)

1. Introduction. Let D be a positive square free integer greater than 1 and let $p \equiv 3 \pmod 4$ be a prime number not dividing D. Let further d be the order of a prime ideal divisor of (p) in the ideal class group of the quadratic field $Q(\sqrt{-D})$. In the present paper we consider the diophantine equation

$$y^2 + D^m = p^n \tag{1}$$

in positive integers y, m, n. The aim of this paper is to prove the following two theorems.

THEOREM 1. *Assume $D \equiv 1, 2 \pmod 4$ and $p^d - D$ is a square. Then the equation* (1) *implies that $m = 1$ unless $(p, D) = (3, 2)$.*

THEOREM 2. *The only positive integer solutions of the equation*

$$y^2 + 2^m = 3^n \tag{2}$$

are given by $(y, m, n) = (1, 1, 1), (5, 1, 3), (1, 3, 2), (7, 5, 4)$.

We shall complete the proof of the above theorems by using the techniques of [2].

2. Proof of some lemmas.

LEMMA 1. *Let d and D be as in Theorem* 1. *Assume that s is a fixed positive integer and $D \not\equiv 0 \pmod 3$. If the equation*

$$y^2 + D^{2s+1} = p^n \tag{3}$$

has integer solutions for y and n, then the equation

$$y^2 + D^{2(s-1)+1} = p^n$$

has also integer solutions for y and n.

Proof. Since $p^d - D$ is a square, $-D$ is a quadratic residue modulo p. Then from the theory of quadratic fields, it follows that $(p) = PP'$, where P and P' are distinct conjugate prime ideals in the quadratic field $Q(\sqrt{-D})$.

Hence, from (3), we obtain the ideal equation

$$(y+D^s\sqrt{-D})(y-D^s\sqrt{-D}) = P^nP'^n.$$

Since the factors on the left are relatively prime, we have either

$$P^n = (y+D^s\sqrt{-D}) \quad \text{or} \quad P^n = (y-D^s\sqrt{-D}).$$

We may assume that

$$P^n = (y+D^s\sqrt{-D}).$$

Then P^n is a principal ideal, and so $n = dw$ for some positive integer w. By our assumption, we can put $p^d = a^2+D$ for some positive integer a. Thus we have either

$$P^d = (a+\sqrt{-D}) \quad \text{or} \quad P^d = (a-\sqrt{-D}).$$

Therefore we get

(4) $$y+D^s\sqrt{-D} = \pm(a\pm\sqrt{-D})^w$$

since the only units of the imaginary quadratic field $Q(\sqrt{-D})$ are ± 1. From this we obtain

$$D^s = \pm(wa^{w-1}+DK)$$

for some integer K. Since $(a, D) = 1$, we see that $w \equiv 0 (\bmod D)$, say, $w = Db$. Hence from (4), we have

(5) $$y+D^s\sqrt{-D} = \pm(u+v\sqrt{-D})^D,$$

where u and v are rational integers. From this we obtain

(6) $$D^s = \pm Dv\left(u^{D-1}-\binom{D}{3}u^{D-3}v^2+DM\right),$$

where M is a rational integer. Since $(u, D) = (3, D) = 1$, from (6), we get $Dv = \pm D^s$, and so $v = \pm D^{s-1}$. Therefore from (3) and (5), we have

$$(u^2+D^{2(s-1)+1})^D = p^{bdD},$$

which gives

$$u^2+D^{2(s-1)+1} = p^{bd}.$$

This completes the proof.

Corollary 1. *Let d and D be as in Lemma 1. If the positive integers y and n satisfy the equation*

$$y^2+D^3 = p^n,$$

then

$$n \geqslant \begin{cases} 2D & \text{if} \quad D \equiv 1 (\bmod 4), \\ D & \text{if} \quad D \equiv 2 (\bmod 4). \end{cases}$$

Proof. From the proof of Lemma 1, we have $n = Dbd$ for some positive integer b. When $D \equiv 1 (\bmod 4)$, we find that d is even since $p^d - D$ is a square. So we get $d \geqslant 2$. Then we can easily obtain our assertion.

Lemma 2. *Let d and D be as in Theorem 1. Assume that s is a fixed positive integer and $D \equiv 0 (\bmod 3)$, say $D = 3E$. If the equation*

(7) $$y^2+E^{2s}D = p^n$$

has integer solutions for y and n, then the equation

$$y^2+E^{2(s-1)}D = p^n$$

has also integer solutions for y and n.

Proof. Put $p^d = a^2+D$, where a is a rational integer. Using the same argument as in the proof of Lemma 1, we have

(8) $$y+E^s\sqrt{-D} = \pm(a\pm\sqrt{-D})^w,$$

where $n = dw$ and w is a positive integer. From this we see that $w \equiv 0 (\bmod E)$, say $w = Eb$. Then from (8), we get

(9) $$y+E^s\sqrt{-D} = \pm(u+v\sqrt{-D})^E,$$

where u and v are rational integers. So we know that

$$E^s = \pm Ev(u^{E-1}+EK)$$

for some integer K. Since $(u, E) = 1$, we have $Ev = \pm E^s$, and so $v = \pm E^{s-1}$. Therefore from (7) and (9), we obtain

$$u^2+E^{2(s-1)}D = p^{bd}.$$

This completes the proof.

Corollary 2. *Let d, D and E be as in Lemma 2. If the positive integers y and n satisfy the equation*

$$y^2+E^2D = p^n,$$

then

$$n \geqslant \begin{cases} 2E & \text{if} \quad D \equiv 1 (\bmod 4), \\ E & \text{if} \quad D \equiv 2 (\bmod 4). \end{cases}$$

The proof is similar to that of Corollary 1. So we omit it.

LEMMA 3. *Let d, D and E be as in Lemma 2. Assume that s is a fixed positive integer. If the equation*

$$y^2+D^{2s+1} = p^n \tag{10}$$

has integer solutions for y and n, then either the equation

$$y^2+D^{2(s-1)+1} = p^n$$

or the equation

$$y^2+E^{2(s-1)}D = p^n$$

has also integer solutions for y and n.

Proof. Using the same argument as in the proof of Lemmas 1 and 2, we see that $n = Dbd$ for some positive integer b and

$$y+D^s\sqrt{-D} = \pm(u+v\sqrt{-D})^D, \tag{11}$$

where u and v are rational integers. Then from this, we obtain

$$D^s = \pm Dv\left(u^{D-1}-\binom{D}{3}u^{D-3}v^2+DK\right)$$

for some integer K. Since $(u, D) = 1$ and $D = 3E$, we have either

$$v = \pm D^{s-1} \quad \text{or} \quad v = \pm E^{s-1}.$$

If $v = \pm D^{s-1}$, then from (10) and (11), we get

$$u^2+D^{2(s-1)+1} = p^{bd}.$$

If $v = \pm E^{s-1}$, then from (10) and (11), we have

$$u^2+E^{2(s-1)}D = p^{bd}.$$

This completes the proof.

COROLLARY 3. *Let d and D be as in Lemma 2. If the positive integers y and n satisfy the equation*

$$y^2+D^3 = p^n,$$

then

$$n \geqslant \begin{cases} 2D & \text{if} \quad D \equiv 1 \pmod 4, \\ D & \text{if} \quad D \equiv 2 \pmod 4. \end{cases}$$

The proof is similar to that of Corollary 1. So we omit it.

LEMMA 4. *Let d and $D \equiv 1 \pmod 4$ be as in Theorem 1. Then the equation*

$$y^2+D^3 = p^n \tag{12}$$

has no solutions in positive integers y and n.

Proof. Taking the equation (12) modulo 4, we find that n is even, say $n = 2k$. Then we have $(p^k+y)(p^k-y) = D^3$, which gives $p^k \leqslant D^3$.

On the other hand, from Corollaries 1 and 3, we have $n \geqslant 2D$. Therefore we obtain $p^D \leqslant D^3$. But, the inequality is impossible, since $D \geqslant 5$ and $p \geqslant 3$. This completes the proof.

LEMMA 5. *Let d and $D \equiv 2 \pmod 4$ be as in Theorem 1. Then the equation*

$$y^2+D^3 = p^n \tag{13}$$

has no solutions in positive integers y and n if either $D \geqslant 6$ or $p \geqslant 7$.

Proof. Taking the equation (13) modulo 4, we see that n is even, say $n = 2k$. Then from (13), we know that $p^k \leqslant D^3$.

On the other hand, from Corollaries 1 and 3, we get $n \geqslant D$. Hence we have

$$p^D \leqslant D^6. \tag{14}$$

If $p \geqslant 7$ and $D \geqslant 6$, then the inequality (14) is impossible.

If $p \geqslant 7$ and $D = 2$, then from (13) we have

$$(p^k-y)(p^k+y) = 2^3.$$

So we get

$$p^k-y = 2 \quad \text{and} \quad p^k+y = 4,$$

which implies $p = 3$. This is a contradiction.

If $p = 3$ and $D \geqslant 22$, then the inequality (14) is impossible. Moreover, it is easy to see that neither the equation

$$y^2+14^3 = 3^n$$

nor the equation

$$y^2+10^3 = 3^n$$

has positive integer solutions for y and n.

Thus we have completed the proof of Lemma 5.

LEMMA 6. *Let d, E and $D \equiv 1 \pmod 4$ be as in Lemma 2. Then the equation*

$$y^2+E^2D = p^n \tag{15}$$

has no solutions in positive integers y and n.

Proof. Taking the equation (15) modulo 4, we find that n is even, say $n = 2k$. Then from (15), we can easily deduce that $p^k \leqslant E^2D$.

On the other hand, from Corollary 2, we get $n \geqslant 2E$, and so

$$p^E \leqslant E^2D. \tag{16}$$

We note that $E \geqslant 7$, since $D = 3E \equiv 1 \pmod 4$ and D is a square free positive integer. Then the inequality (16) is impossible. This completes the proof.

LEMMA 7. *Let d, E and $D \equiv 2 \pmod 4$ be as in Lemma 2. Then the equation*

$$y^2 + E^2 D = p^n \tag{17}$$

has no integer solutions for y and n unless $D = 6$.

Proof. Taking the equation (17) modulo 4, we see that n is even, say $n = 2k$. Then we get $p^k \leqslant E^2 D$.

On the other hand, from Corollary 2, we have $n \geqslant E$, and so

$$p^E \leqslant E^4 D^2 = 9E^6. \tag{18}$$

If $E \geqslant 10$, then the inequality (18) is impossible, since $p \geqslant 7$. This completes the proof.

LEMMA 8. *Neither the equation*

$$y^2 + 6 \cdot 2^4 = 7^n \tag{19}$$

nor the equation

$$y^2 + 6^5 = 7^n \tag{20}$$

has integer solutions for y and n.

Proof. Taking the equation (19) modulo 4, we find that n is even, say $n = 2k$. Then from (19) we have

$$(7^k - y)(7^k + y) = 6 \cdot 2^4.$$

Thus we have either

$$7^k - y = 2 \quad \text{and} \quad 7^k + y = 3 \cdot 2^4$$

or

$$7^k - y = 2 \cdot 3 \quad \text{and} \quad 7^k + y = 2^4,$$

which give either

$$7^k = 5^2 \quad \text{or} \quad 7^k = 11.$$

But both cases are impossible.

By using the same way as before, we readily find that the equation (20) has no integer solutions. So we omit the proof.

LEMMA 9. *Let p and $D = 6$ be as in Theorem 1. Then the equation*

$$y^2 + 6^{2m+1} = p^n \tag{21}$$

has no solutions in positive integers y, m, n.

Proof. In the case of $m = 1$, it follows from Lemma 5 that the equation (21) has no integer solutions for y and n. By using the same way as in the proof of Lemma 8, we see that the equation $y^2 + 6 \cdot 2^2 = p^n$ implies $p = 7$, since $p \equiv 3 \pmod 4$. Thus the lemma follows immediately from Lemmas 2, 3 and 8.

3. Proof of Theorem 1. On taking the equation (1) modulo p, we find that m is odd.

In the case $D \not\equiv 0 \pmod 3$, our assertion follows immediately from Lemmas 1, 4 and 5.

In the case $D \equiv 0 \pmod 3$, our assertion follows immediately from Lemmas 2, 3, 4, 5, 6, 7 and 9.

4. Proof of Theorem 2. On taking the equation (2) modulo 3, we see that m is odd, say $m = 2s+1$. Then the equation (2) becomes

$$y^2 + 2^{2s+1} = 3^n. \tag{22}$$

In the case of $s = 0$, from the result of R. Apéry [1], we know that the only positive integer solutions of (22) are given by $(y, n) = (1, 1)$, $(5, 3)$.

By an argument similar to the one used in the proof of Lemma 8, we deduce that if $s = 1$, then the positive integer solution of (22) is given by $(y, n) = (1, 2)$ and if $s = 2$, then that of (22) is given by $(y, n) = (7, 4)$. Moreover, if $s = 3$, then the equation (22) has no integer solutions for y and n. We note here that Lemma 1 holds in the case of $D = 2$. Thus the theorem follows immediately from Lemma 1.

References

[1] R. Apéry, *Sur une équation diophantienne*, C.R. Acad. Sci. Paris 251 (1960), pp. 1451–1452.

[2] M. Toyoizumi, *On the diophantine equation $y^2 + D^m = 2^n$*, Comment. Math. Univ. St. Pauli 27 (1979), pp. 105–111.

DEPARTMENT OF MATHEMATICS
RIKKYO UNIVERSITY
Nishi-Ikebukuro, Tokyo 171, Japan

Present address
DEPARTMENT OF MATHEMATICS
TOYO UNIVERSITY
Kawagoe-Shi, Saitama, 350, Japan

Received on 2. 12. 1981 (1281)