MATH. SCAND. 38 (1976), 240–246

THE DIOPHANTINE EQUATION $x^2+11=3^k$ AND RELATED QUESTIONS

EDWARD L. COHEN*

Dedicated to the memory of W. Ljunggren

A review of recent contributions to the study of diophantine equations of the form

$$x^2+D = p^k, \quad D \equiv 3(\mathrm{mod}\,4),$$

is presented and an alternative proof that the diophantine equation $x^2+11=3^k (x \geqq 0)$ has as its only solution $(x,k)=(4,3)$ is given.

1. Review of recent contributions.

A. We consider diophantine equations of the form

$$x^2+D = p^k, \tag{1.1}$$

p prime, mainly when $D \equiv 3 \pmod 4$. D is assumed to be greater than zero unless otherwise specified. We generally do not examine fully all the results of the papers discussed below. It is well known that equations of the forms (1.1)–(1.7) have only a finite number of solutions (e.g., see [3], [11], [19], [28], [29]).

B. S. Ramanujan in 1913 [22, 23] asked whether there were other solutions to the diophantine equation

$$x^2+7 = 2^k \tag{1.2}$$

besides the known ones, namely, $k=3,4,5,7,15$. This problem was again posed by W. Ljunggren [16] in 1943. It was first solved by T. Nagell [20, 21], who showed that the above-mentioned are the only five solutions. After that many different proofs were given (for an extensive list cf. [10]; for recent discussions, cf. [5] and [17]). It is interesting to note that the equation (1.2) has applications to binary error-correcting codes [10], [24] and to differential algebras [17].

Received June 27, 1975.

*Research supported by the National Research Council of Canada under grant no. A-7164.

C. Other papers involving the prime $p=2$ are those of Browkin and Schinzel [6], Skolem, Chowla and Lewis [28] and Hasse [12]. These deal mainly with the equation

$$x^2+D = 2^k . \tag{1.3}$$

In [6], special attention is paid to the cases $D \in \mathbf{Z} \not\equiv 0,4,7 \pmod 8$ and $D \equiv 7 \pmod 8$. Different proofs of the solution to the Ramanujan-Nagell equation (1.2) are given in [12], [28]. Also in [12] a through survey of the literature on the equation

$$x^2+D = l^k , \tag{1.4}$$

especially when $l=2$ and D is odd, is presented; and further results are obtained.

D. An extension of equation (1.2) was investigated by the author [9, 11]. Let $D \equiv 3 \pmod 8$ such that $(D+1)/4=p$, a prime. The main result shows that there are no solutions to the equation (1.1) when $D \geqq 19$. When $D=7$, we are reduced to the Ramanujan–Nagell equation (1.2). Alter and Kubota [1] extended these results, confirming the results of [9, 11], and providing solutions to numerous equations of the type (1.1) when $D \equiv 3 \pmod 4$.

E. The only equation remaining of the type mentioned in section D occurs when $D=11$, from which the diophantine equation

$$x^2+11 = 3^k, \quad x \geqq 0 , \tag{1.5}$$

arises. Ljunggren and the author prove [10] that this equation has only one solution, namely, $(x,k)=(4,3)$. The result is found in Alter and Kubota [2], who also show that for each z the diophantine equation $x^2+11z^2=3^k$ has at most one solution. Another proof of the uniqueness of the solution $(x,k)=(4,3)$ of equation (1.5) is presented in section 2.

F. A related equation to (1.1), viz.,

$$x^2+3 = y^k, \quad k \geqq 2; \quad x,y \in \mathbf{Z} , \tag{1.6}$$

was considered by T. Nagell [19] and E. Brown [7]. They showed by different congruence arguments that the only solutions to equation (1.6) are $(x,y,k)=(\pm 1, \pm 2, 2)$.

G. Bender and Herzberg [4] have considered the bounds on the number of integral solutions to the equation

$$ax^2+D = N^k , \tag{1.7}$$

where a, N, D are positive integers. They have also prepared a survey article [5] on diophantine equations associated with the positive definite quadratic form ax^2+by^2. Bounds on solutions of many types of diophantine equations including the kind discussed above are among the topics investigated.

H. Two procedures are frequently used to obtain bounds for the number of solutions of diophantine equations or to find solutions to them: (a) p-adic methods occur in [3], [14], [28]; (b) linear recurrences (of order two) are employed in obtaining solutions in, e.g., [1], [2], [6], [8], [10], [14] and [28]. Interesting expositions on p-adic methods can be found in Skolem [25, 26, 27], Mordell [18, Chapter 23] and Lewis [15] plus several of the references in this last study. We note also that through p-adic methods many results on second order linear recurrences can be obtained. There is considerable literature on this subject that we cannot go into here (e.g., see [13]).

2. The diophantine equation in the title.

I. It is now shown that the diophantine equation

$$x^2+11 = 3^k, \quad x \geqq 0, \tag{2.1}$$

has as its only solution $(x,k)=(4,3)$. Some of the ideas of Hasse [12] as recorded in Mordell's book [18, pp. 205–206] are used.

J. *Even solutions.* When k is even, $(3^{k/2})^2-x^2=11$; therefore,

$$(3^{k/2} \pm x) = 11, \quad (3^{k/2} \mp x) = 1 .$$

Hence, there can be no even solutions. (We shall see in the remark in section L another proof of the impossibility of even solutions.)

K. *Odd solutions.* Now, we can suppose that k is odd and write equation (2.1) as

$$3^y = x^2+11 = (x+\delta)(x-\delta) , \tag{2.2}$$

where y is odd and $\delta^2=-11$. The equation has thus been factorized in the field $Q(\delta)$, in which the integers have the form $(u+v\delta)/2$, where $u \equiv v \pmod 2$, and in which unique factorization occurs.

Since $3=[(1+\delta)/2][(1-\delta)/2]$, we have $(x \pm \delta) = \pm[(1 \pm \delta)/2]^y$; thus,

$$[(1+\delta)/2]^y-[(1-\delta)/2]^y = \pm 2\delta . \tag{2.3}$$

This can be written as

$$a^y - b^y = \pm 2\delta = \pm 2(a-b)\,. \tag{2.4}$$

We show that the positive sign in equation (2.4) is impossible. Note that $a^2 \equiv 1 \pmod b$. Then

$$a^y = a(a^2)^{(y-1)/2} \equiv a \pmod b\,;$$

hence,

$$2(a-b) = a^y - b^y \equiv a-b \pmod b\,;$$

$$\text{or } a \equiv 0 \pmod b\,,$$

establishing a contradiction.

Using the binomial expansion (B.E.) in equation (2.3), we obtain

$$-2^{y+1} = 2\left[\binom{y}{1} - \binom{y}{3}11 + \binom{y}{5}11^2 - \ldots \pm \binom{y}{y}11^{(y-1)/2}\right];$$

and so $y \equiv -2^y \pmod{11}$. This has the odd solutions $y \equiv 3, 31, 37, 45, 49 \pmod{110}$. It suffices to show then that (i) $y \equiv 31, 37, 45, 49 \pmod{110}$ cannot occur; and (ii) there cannot be two solutions y, z with $y - z \equiv 0 \pmod{110}$—thus making $y = 3$ the unique solution.

L. To show (i), let us list the powers of a that will be used:

$$2a = 1+\delta \qquad a^3 = -4-\delta \qquad 2a^4 = 7-5\delta$$
$$2a^5 = 31+\delta \qquad 2a^9 = 136-74\delta \qquad 2a^{11} = 67+253\delta\,.$$

Note that

$$2a^{11} = 67+253\delta \equiv 320 \pmod{253}, \quad \text{or} \quad a^{11} \equiv 160 \equiv -93 \pmod{253}.$$

Therefore,

$$a^{11r} \equiv \pm 1, \pm 93, \pm 47, \pm 70, \pm 68 \pmod{253}\,.$$

We have then the following four relations:

(a) $2a^{11r+9} = G_r + \delta H_r$,
where $H_r \equiv \pm 74, \pm 51, \pm 64, \pm 120, \pm 28 \pmod{253}$;

(b) $2a^{11r+4} = G_r + \delta H_r$,
where $H_r \equiv \pm 5, \pm 41, \pm 18, \pm 97, \pm 87 \pmod{253}$;

(c) $2a^{11r+1} = G_r + \delta H_r$,
where $H_r \equiv \pm 1, \pm 93, \pm 47, \pm 70, \pm 68 \pmod{253}$;

(d) $2a^{11r+5} = G_r + \delta H_r$,
where $H_r \equiv \pm 1, \pm 93, \pm 47, \pm 70, \pm 68 \pmod{253}$;

eliminating, respectively, the possibility that $y \equiv 31, 37, 45, 49 \pmod{110}$, i.e., demonstrating that the coefficient $H_r/2$ of δ in the above a^v cannot be ± 1, or the form $x \pm \delta$ cannot occur.

REMARK. The same type of argument shows that $y \equiv 11r + s \pmod{110}$ is eliminated for $s \equiv 2, 6, 7, 8, 10 \pmod{11}$. Thus we have another proof that even solutions, where $y \equiv 8, 10, 46, 62, 94 \pmod{110}$, cannot exist.

M. To show (ii), we suppose that 11^m is the highest power of 11 dividing $z - y$. Then

$$a^z = a^v a^{z-v} = a^v (\tfrac{1}{2})^{z-v} (1+\delta)^{z-v}; \tag{2.5}$$

and, using the B.E., we obtain

$$(\tfrac{1}{2})^{z-v} = ((\tfrac{1}{2})^{10})^{(z-y)/10} \equiv 1 \pmod{11^{m+1}}. \tag{2.6}$$

Also we want to obtain the following modulus:

$$(1+\delta)^{z-v} \equiv 1 + (z-y)\delta \pmod{11^{m+1}}. \tag{2.7}$$

Letting $P = (1+\delta)^{11^m}$, and using the B.E., we get that $P \equiv 1 + 11^m \delta \pmod{11^{m+1}}$. Since 11^m divides $z - y$ and $(z-y)/11^m \geqq 2$, we have (again using the B.E.)

$$P^{(z-y)/11^m} \equiv 1 + (z-y)\delta \pmod{11^{m+1}},$$

proving relation (2.7). Now,

$$a^v = [(1+\delta)/2]^v = \left(1 + y\delta + \binom{y}{2}\delta^2 + \ldots\right)/2^v \equiv (1 + y\delta)/2^v \pmod{11}.$$

Hence,

$$2^v a^v = 1 + y\delta + 11T. \tag{2.8}$$

From relations (2.5) – (2.8), we have, therefore, that

$$a^z \equiv a^v + (z-y)\delta/2^v \pmod{11^{m+1}}. \tag{2.9}$$

Similarly,

$$b^z \equiv b^v - (z-y)\delta/2^v \pmod{11^{m+1}}. \tag{2.10}$$

By subtracting (2.10) from (2.9), and recalling that $a^v - b^v = a^z - b^z = -2\delta$, we find that

$$(z-y)\delta/2^{v-1} \equiv 0 \pmod{11^{m+1}}.$$

This yields the fact that $z - y \equiv 0 \pmod{11^{m+1}}$ since z and y are both rational; hence, a contradiction is established.

N. It was proved in [11] and noted in section D that there are no solutions to equation (1.1) when $p = (D+1)/4$, $19 \leqq D \equiv 3 \pmod 8$. This prob-

lem can also be resolved for each p by the procedure used in section L by letting $a=(1+\sqrt{-D})/2$. This is guaranteed because we already know that no solutions exist. However, as D increases, the computation would, in general, become unwieldy.

REFERENCES

1. R. Alter and K. K. Kubota, *The diophantine equation* $x^2+D=p^n$, Pacific J. Math. 46 (1973), 11–16. MR 48 #2063.
2. R. Alter and K. K. Kubota, *The Diophantine equation* $x^2+11=3^n$ *and a related sequence*. J. Number Theory 7 (1975), 5–10.
3. R. Apéry, *Sur une équation diophantienne*, C. R. Acad. Sci. Paris, Sér. A251 (1960), 1451–1452. MR 22 #10950.
4. E. A. Bender and N. P. Herzberg, *Some diophantine equations related to the quadratic form* ax^2+by^2, Bull. Amer. Math. Soc. 81 (1975), 161–162.
5. E. A. Bender and N. P. Herzberg, *Some diophantine equations related to the quadratic form* ax^2+by^2, Advances in Math. (submitted).
6. J. Browkin and A. Schinzel, *On the equation* $2^n-D=y^2$, Bull. Acad. Polon. Sci. Math. Astronom. Phys. 8 (1960), 311–318. MR 24 #A82.
7. E. Brown, *Diophantine equations of the form* $x^2+D=y^n$, J. Reine Angew. Math. 274/275 (1975), 385–389.
8. S. Chowla, M. Dunton and D. J. Lewis, *All integral solutions of* $2^n-7=x^2$ *are given by* $n=3,4,5,7,15$, Norske Vid. Selsk. Forh. (Trondheim) 33 (1960), 37–48. MR 26 #6118.
9. E. L. Cohen, *Sur certaines équations diophantiennes quadratiques*, C. R. Acad. Sci. Paris Sér. A 274 (1972), 139–140. MR 45 #169.
10. E. L. Cohen, *Sur l'équation diophantienne* $x^2+11=3^k$, C. R. Acad. Sci. Paris Sér. A 275 (1972), 5–7. MR 46 #3445.
11. E. L. Cohen, *On diophantine equations of the form* $x^2+D=p^k$, Enseignement Math. (2), 20 (1974), 235–241.
12. H. Hasse, *Über eine diophantische Gleichung von Ramanujan-Nagell und ihre Verallgemeinerung*, Nagoya Math. J. 27 (1966), 77–102. MR 34 #136.
13. K. K. Kubota, *On a conjecture of Morgan Ward*, I, II, III (to appear).
14. D. J. Lewis, *Two classes of Diophantine equations*, Pacific J. Math. 11 (1961), 1063–1076. MR 25 #3005.
15. D. J. Lewis, *Diophantine equations: p-adic methods*, Studies in Number Theory (MAA Studies in Mathematics 6), Math. Assoc. Amer., Washington, D. C., 1969, 25–75. MR 39 #2699.
16. W. Ljunggren, Oppg. 2, Norsk Mat. Tidsskr. 25 (1943), 29.
17. D. G. Mead, *The equation of Ramanujan-Nagell and* $[y^2]$, Proc. Amer. Math. Soc. 41 (1973), 333–341. MR 48 #6067.
18. L. J. Mordell, *Diophantine Equations* (Pure and Applied Mathematics 30). Academic Press, New York, London, 1969. MR 40 #2600.
19. T. Nagell, *Sur l'impossibilité de quelques équations à deux indéterminées*, Norsk Mat. Forenings Skr. Ser. 1, Nr. 13 (1923), 65–82.
20. T. Nagell, *Løsning til oppgave* 2 (1943, *s.* 29), Norsk Mat. Tidsskr. 30 (1948), 62–64.
21. T. Nagell, *The diophantine equation* $x^2+7=2^n$, Ark. Mat. 4 (1961), 185–187. MR 24 #A83.

22. S. Ramanujan, *Question* 464, J. Indian Math. Soc. 5 (1913), 120.
23. S. Ramanujan, *Collected Papers*, Chelsea Publishing Co., New York, 1962, 327.
24. H. S. Shapiro and D. L. Slotnick, *On the mathematical theory of error-correcting codes*, IBM J. Res. Develop. 3, 25–34. MR 20 # 5092.
25. Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8th Scand. Math. Congr. (Stockholm 1934), 163–188, Ohlssons Boktryckeri, Lund, 1935. Zbl. 11, 392.
26. Th. Skolem, *Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen*, Math. Ann. 111 (1935), 399–424. Zbl. 12, 13.
27. Th.Skolem, *The use of a p-adic method in the theory of diophantine equations*, Bull. Soc. Math. Belg. 7 (1955), 83–95. MR 17, 237.
28. Th. Skolem, S. Chowla and D. J. Lewis, *The diophantine equation* $2^{n+2}-7=x^2$ *and related problems*, Proc. Amer. Math. Soc. 10 (1959), 663–669 MR 22 # 25.
29. A. Thue, *Über die Unlösbarkeit der Gleichung* $ax^2+bx+c=dy^n$ *in grossen ganzen Zahlen* x *und* y, Archiv for Mathematik og Naturvidenskab 34 (Kristiania 1916).

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF OTTAWA
OTTAWA, ONTARIO, CANADA
K1N 6N5