Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 20 (1974)

Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ON DIOPHANTINE EQUATIONS OF THE FORM $x^2 + D = p^k$

Autor: Cohen, Edward L.

Kapitel: 4. COROLLARIES AND RELATED RESULTS

DOI: https://doi.org/10.5169/seals-46907

Proof. One can write equation (2.2) as

$$(3.5) \quad (x+\sqrt{-D})\,(x-\sqrt{-D}) \;=\; [(1+\sqrt{-D})\,/\,2]^k\,[(1-\sqrt{-D})\,/\,2]^k\,.$$

By Lemma 3.7, equation (3.5) can be written as

$$[(1+\sqrt{-D})\,/\,2]^k - [(1-\sqrt{-D})\,/\,2]^k \;=\; \pm\, 2\sqrt{-D}\,,$$

i.e.,
$$a^k - b^k \;=\; \pm\, 2\,(a-b)\,.$$

Therefore,

$$a^k - b^k = (a-b)\,(a^{k-1}+a^{k-2}b+\;\dots\;+ab^{k-2}+b^{k-1}) \;=\; \pm\, 2\,(a-b)\,.$$

Hence, $a^{k-1} = \pm\, 2 \pmod{b}$, or $(a^2)^{\frac{1}{2}(k-1)} \equiv \pm\, 2 \pmod{b}$. By Lemma 3.8, we have that $1 \equiv \pm\, 2 \pmod{b}$. As b cannot divide the units of $Q\,(\sqrt{-D})$, the only possibility is that $1 \equiv -\,2 \pmod{b}$, i.e. $3 \equiv 0 \pmod{b}$. This is impossible since $p \geqslant 5$. ∇

4. Corollaries and related results

The following results are similar to the ones already proved.

Corollary 4.1. If p is an odd prime equal to $(1+n^2D)/4$, then the equation $x^2 + D = p^k$ has no solutions.

By proving a result analogous to Lemma 3.8, another result similar to Theorem 3.1 is obtained:

Theorem 4.2. Let $D \equiv 3 \pmod{4}$, $D > 3$. Let p be an odd prime such that $(-D/p) = +1$. If p does not divide $nm^{2z} \pm 2$ $(z = 0, 1, \dots, p-1)$, then the equation $x^2 + D = p^k$ $(k \geqslant 1)$ has no solutions. (See [4] for details.) ∇

Remark 4.3. By the preceding theorem, many equations can be shown to have no solutions; e.g., (1) $x^2 + 11 = 5^k$, (2) $x^2 + 43 = 13^k$, (3) $x^2 + 91 = 29^k$.

When $D = 3$, one obtains (by slight modifications of the arguments in §3):

Theorem 4.4. Let p be an odd prime such that $(-3/p) = +1$. A sufficient condition for the equation $x^2 + 3 = p^k$ to have no solutions is that p not divide $nm^z \pm 2$, $\left(\dfrac{m+n}{2}\right)\left(\dfrac{m-3n}{2}\right)^{2z} \pm 2$ and $\left(\dfrac{m-n}{2}\right)\left(\dfrac{m+3n}{2}\right)^{2z}$ $\pm\, 2\,(z=0, 1, \dots, p-1)\,.$ ∇

Examples of equations with no solutions are (1) $x^2 + 3 = 13^k$, (2) $x^2 + 3 = 109^k$.

The following remarks are similar to exercises in the book of Stark [15, pp. 309-316] and are related to results presented here. (p below is an odd prime.)

Remark 4.5. When $D > 3$, $n^2 + m^2 D = 4p$ iff $(-D/p) = +1$. In this case there is exactly one solution in natural numbers m, n.

Remark 4.6. $n^2 + 3m^2 = 4p$ iff $(-3/p) = +1$. In this case there are exactly 3 solutions in natural numbers m, n.

REFERENCES

[1] Apéry, R. Sur une équation diophantienne. *C. R. Acad. Sc. Paris, 251* (1960), pp. 1263-1264. MR 22 #10951.

[2] —— Sur une équation diophantienne. *C. R. Acad. Sc. Paris, 251* (1960), pp. 1451-1452. MR 22 #10950.

[3] Cohen, E. L. A note on perfect double error-correcting codes on q symbols. *Information and Control, 7* (1964), pp. 381-384. MR 29 #5656.

[4] —— Sur certaines équations diophantiennes quadratiques. *C. R. Acad. Sc. Paris, 274* (1972), pp. 139-140. MR 45 #169.

[5] —— Sur l'équation diophantienne $x^2 + 11 = 3^k$. *C. R. Acad. Sc. Paris, 275* (1972), pp. 5-7. MR 46 #3445.

[6] Landau, E. and A. Ostrowski. On the diophantine equation $ay^2 + by + c = dx^n$. *Proceedings of the London Mathematical Society, (2), 19* (1921), pp. 276-280.

[7] Ljunggren, W. *Norsk Matematisk Tidsskrift, 25* (1943), p. 29.

[8] Mann, H. B. *Introduction to Algebraic Number Theory.* Graduate School Studies, Mathematics Series No. 1, The Ohio State University Press, Columbus, Ohio, 1955. MR 17-240.

[9] Mordell, L. J. Indeterminate equations of the third and fourth degree. *Quarterly Journal of Pure and Applied Mathematics, 45* (1914), pp. 170-186.

[10] Nagell, T. Løsning til oppgave nr 2 (1943, s. 29), *Norsk Matematisk Tidsskrift, 30* (1948), pp. 62-64.

[11] —— *Introduction to Number Theory.* John Wiley & Sons, New York, 1951. Problem 165, p. 272. MR 13-207.

[12] Ramanujan, S. Question 464. *The Journal of the Indian Mathematical Society, 5* (1913), p. 120.

[13] —— *Collected Papers.* Cambridge University Press, 1927. p. 327.

[14] Shapiro, H. S. and D. L. Slotnick. On the mathematical theory of error-correcting codes. *IBM Journal of Research and Development, 3* (1959), pp. 25-34. MR 20 #5092.

[15] Stark, H. M. *An Introduction to Number Theory.* Markham Publishing Company, Chicago 1970. MR 40 #7186.