

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

Autor(en): **Cohen, Edward L.**

Objektyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Persistenter Link: <https://doi.org/10.5169/seals-46907>

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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

by Edward L. COHEN <sup>1</sup>

## 1. INTRODUCTION

Numerous authors have proved the following theorem:

*Theorem 1.1.* There are only finitely many solutions of the equation

$$(1.1) \quad x^2 + D = r^k,$$

$D, r$  positive fixed integers;  $k = 1, 2, 3, \dots$

This has been shown mainly through the theorem of Thue [16] or Landau-Ostrowski [6] which states

*Theorem 1.2.* The equation

$$(1.2) \quad ax^2 + bx + c = dy^n$$

with  $n$  (fixed)  $\geq 3$ ,  $ad \neq 0$ ,  $b^2 - 4ac \neq 0$  (all letters denoting rational integers) has at most a finite number of solutions.

*Proof of Theorem 1.1.* Let  $a = 1$ ,  $b = 0$ ,  $c = D$ . Then equation (1.2) can be transformed into

$$(1.3) \quad x^2 + D = dy^n.$$

Now let  $y = r^v$ ,  $v = [k/3]$ , and  $d = 1, r, r^2$  if  $k \equiv 0, 1, 2 \pmod{3}$ , respectively. Then equation (1.3) becomes three equations of the type (1.2) when  $n = 3$ .  $\nabla$

Mordell [9] proved Theorem 1.2 when  $n = 3$ . This is obviously sufficient for our purposes.

Henceforth,  $r$  will be a prime  $p$  and  $D \equiv 3 \pmod{4}$  [unless explicitly stated otherwise]. Under the conditions that  $r$  be a prime, Apéry proved [1], [2] that equation (1.1) has at most two solutions unless  $D = 7$  and  $p = 2$ .

---

<sup>1</sup> This research was supported in part by the National Research Council of Canada, Grant A-7164.

## 2. HISTORICAL BACKGROUND: $D = 7, p = 2$ and $D = 11, p = 3$

Ramanujan in 1913 [12], [13] asked whether there were other solutions to the diophantine equation

$$(2.1) \quad x^2 + 7 = 2^k$$

besides the known ones, namely when  $k = 3, 4, 5, 7, 15$ . This problem was again posed by Ljunggren [7] in 1943, and it was finally shown by Nagell [10] that the  $k$  above were the only five solutions. Nagell's paper was written in Norwegian and few knew about its existence although he had posed it shortly afterwards as an exercise in his book [11] on elementary number theory. Hence, thereafter, there were a large number of papers proving the same result (see [5] for an up-to-date list).

It is also interesting to note that equation (2.1) has interesting applications to binary error-correcting codes [3], [14].

Equation (2.1) is of the form

$$(2.2) \quad x^2 + D = [(D+1)/4]^k.$$

So the next equation of interest might seem to be

$$(2.3) \quad x^2 + 11 = 3^k.$$

This equation was solved by Ljunggren and the author [5]. Its only solution occurs when  $k = 3$ .

## 3. THE MAIN THEOREM

*Theorem 3.1.* Let  $D \equiv 3 \pmod{8}$ . Let  $p = (D+1)/4$  be a prime  $\geq 5$ . Then the diophantine equation

$$(3.1) \quad x^2 + D = p^k$$

has no solutions.

The remainder of this section will be devoted to a proof of this theorem, a sketch of which was presented in [4]. The last section will be devoted to corollaries and other related results.

*Lemma 3.2.* There are no solutions to the equation (3.1) when  $k$  is even.

*Proof.* When  $k$  is even, the equation can be written as

$$(3.2) \quad (p^{k/2})^2 - x^2 = D.$$

Therefore,

$$(3.3) \quad p^{k/2} \pm x = u, \quad p^{k/2} \mp x = v,$$

where  $u$  and  $v$  are integers,  $uv = D$  and  $u + v \equiv 0 \pmod{4}$ . But then  $p^{k/2} = (u+v)/2$ . This is impossible because  $(u+v)/2$  is even.  $\nabla$

We present two lemmas which are well known in the elementary theory of numbers. They are introduced only for the case when  $D \equiv 3 \pmod{4}$ .

*Lemma 3.3.* When  $D \equiv 3 \pmod{4}$ ,  $Q(\sqrt{-D})$  has exactly two units (namely  $\pm 1$ ), unless  $D = 3$ , in which case the units are  $\pm 1, (1 \pm \sqrt{-3})/2, (-1 \pm \sqrt{-3})/2$ .

*Proof.* See Stark [15, pp. 274-275].  $\nabla$

*Lemma 3.4.* The odd prime  $p$  ( $p \nmid D$ ) decomposes in  $Q(\sqrt{-D})$  as follows:

1.  $(p)$  is the product of two distinct prime ideals if  $-D$  is a quadratic residue modulo  $p$ .
2.  $(p)$  is a prime ideal if  $-D$  is not a quadratic residue modulo  $p$ .

*Proof.* See Mann [8, pp. 66-67].  $\nabla$

From Lemma 3.4 (for  $p$  odd), it is obvious that solutions could occur only if  $(-D/p) = +1$ ; since for this case we have

$$(3.4) \quad \begin{aligned} x^2 + D &= (x + \sqrt{-D})(x - \sqrt{-D}) = p^k \\ &= [(m + n\sqrt{-D})/2]^k [(m - n\sqrt{-D})/2]^k, \end{aligned}$$

$m$  and  $n$  nonzero integers. Henceforth, in this section, let  $D > 3$ ,  $p$  be an odd prime,  $m$  and  $n$  be nonzero integers. Also, from Lemma 3.3 and Lemma 3.4 we obtain immediately:

*Corollary 3.5.* If  $(-D/p) = +1$ , then  $p$  can be expressed uniquely as

$$p = \pm \left( \frac{m + n\sqrt{-D}}{2} \right) \cdot \mp \left( \frac{m - n\sqrt{-D}}{2} \right).$$

By standard norm arguments, the following is obtained:

*Corollary 3.6.*  $p^k$  can be uniquely expressed (to within units  $= \pm 1$ ) as

$$p^k = \left( \frac{m + n\sqrt{-D}}{2} \right)^k \left( \frac{m - n\sqrt{-D}}{2} \right)^k.$$

In the context above, we have as a unique expression (with  $m$  and  $n$  fixed)

*Lemma 3.7.*  $x \pm \sqrt{-D} = [(m \pm n\sqrt{-D})/2]^k$  when  $D \equiv 3 \pmod{4}$ ,  $D > 3$ .

*Proof.* By Corollary 3.6, any prime factor of  $x \pm \sqrt{-D}$  can have as factors only  $(m \pm n\sqrt{-D})/2$ . Suppose

$$x + \sqrt{-D} = \left(\frac{m + n\sqrt{-D}}{2}\right)^s \left(\frac{m - n\sqrt{-D}}{2}\right)^t$$

and let  $s \leq t$ . Then  $x + \sqrt{-D} = p^s \left(\frac{m - n\sqrt{-D}}{2}\right)^{t-s}$ . Therefore,

$x + \sqrt{-D} = p^s \left(\frac{a + b\sqrt{-D}}{2}\right)$  or  $1 = p^s (b/2)$ . This is impossible unless  $s = 0$ . Similarly, if  $t \leq s$ , then  $t = 0$ . We conclude that

$$x + \sqrt{-D} = \left(\frac{m + n\sqrt{-D}}{2}\right)^k \text{ or } \left(\frac{m - n\sqrt{-D}}{2}\right)^k.$$

The same argument applies for  $x - \sqrt{-D}$ .  $\nabla$

*Lemma 3.8.* Let  $a = (1 + \sqrt{-D})/2$ ,  $b = (1 - \sqrt{-D})/2$ . Then  $a^2 \equiv 1 \pmod{b}$ .

*Proof.*  $a^2 - 1 = \frac{-[(3+D)/2] + \sqrt{-D}}{2}$ . Solve

$$a^2 - 1 = \frac{b(u + v\sqrt{-D})}{2}. \text{ Then,}$$

$$-[(3+D)/2] + \sqrt{-D} = (1 - \sqrt{-D}) \frac{(u + v\sqrt{-D})}{2};$$

or

$$\begin{aligned} u + vD &= -(3+D) \\ -u + v &= 2, \end{aligned}$$

yielding  $u = -3$ ,  $v = -1$ .  $\nabla$

*Lemma 3.9.* There are no solutions to the equation (3.1) when  $k$  is odd. (This completes the proof of Theorem 3.1).

*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,  $a^{k-1} \equiv \pm 2 \pmod{b}$ , 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  $p \geq 5$ .  $\nabla$

#### 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  $x^2 + D = p^k$  ( $k \geq 1$ ) has no solutions. (See [4] for details.)  $\nabla$

*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  $nm^z \pm 2$ ,  $\left(\frac{m+n}{2}\right) \left(\frac{m-3n}{2}\right)^{2z} \pm 2$  and  $\left(\frac{m-n}{2}\right) \left(\frac{m+3n}{2}\right)^{2z} \pm 2$  ( $z = 0, 1, \dots, p-1$ ).  $\nabla$

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  $D > 3$ ,  $n^2 + m^2D = 4p$  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.

- [16] THUE, A. Über die Unlösbarkeit der Gleichung  $ax^2 + bx + c = dy^n$  in grossen ganzen Zahlen  $x$  und  $y$ . *Archiv for Mathematik og Naturvidenskab* (Kristiania), 34 (1916), No. 16.

Edward L. Cohen

Department of Mathematics  
University of Ottawa  
Ottawa, Ontario, Canada  
K1N 6N5

(Reçu le 2 juillet 1974)



**Vide-leer-empty**