3. The main theorem

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **28.04.2024**

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

$$x^2 + 7 = 2^k \tag{2.1}$$

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

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

So the next equation of interest might seem to be

$$x^2 + 11 = 3^k . \tag{2.3}$$

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 $\geqslant 5$. Then the diophantine equation

$$x^2 + D = p^k \tag{3.1}$$

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

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

Therefore,

$$p^{k/2} \pm x = u\,, \; p^{k/2} \mp x = v\,, \tag{3.3}$$

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. ∇

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 ± 1), unless $D = 3$, in which case the units are ± 1, $(1 \pm \sqrt{-3})/2$, $(-1 \pm \sqrt{-3})/2$.

Proof. See Stark [15, pp. 274-275]. ∇

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]. ∇

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

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

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 $s \leqslant t$. 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 $t \leqslant s$, 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 $x - \sqrt{-D}$. ∇

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

Proof. $a^2 - 1 = \dfrac{-[(3+D)/2] + \sqrt{-D}}{2}$. 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 $u = -3$, $v = -1$. ∇

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, $a^{k-1} = \pm 2 \pmod{b}$, 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 $\left(\dfrac{m-n}{2}\right)\left(\dfrac{m+3n}{2}\right)^{2z}$ $\pm 2\,(z=0, 1, \dots, p-1)$. ∇