Azerbaijan Journal of Mathematics
V. 10, No 2, 2020, July
ISSN 2218-6816

Elementary Proof of Nagell's Theorem

R.R. Andruszkiewicz*, N. Andruszkiewicz

Abstract. We give an elementary proof of the fact that the only solutions of the Diophantine equation $x^2 + 2 = y^n$ for $n > 1$ are $x \pm 5$, $y = 3$, $n = 3$.

Key Words and Phrases: Diophantine equation, Pell equation, Higher degree equations.

2010 Mathematics Subject Classifications: 11D41

---

1. Introduction

The Diophantine equation $x^2 + 2 = y^3$ was studied by Fermat, who claimed, that it had exactly two solutions: $x = \pm 5$ and $y = 3$. The first complete proof of this hypothesis was given by Euler in the second volume of his *Algebra*. Then in 1923, T. Nagell provided incomplete proof of the following theorem:

Theorem 1. *For any integer $n > 3$ the Diophantine equation $x^2 + 2 = y^n$ has no solution.*

The first full proof of this theorem was given by W. Ljunggren [2] in 1943. Then, T. Nagell [4] in 1954 gave another proof, which, like W. Ljunggren's proof, was not elementary and was based on K. Mahler's results concerning binary quadratic forms. Therefore the equation

$$x^2 + 2 = y^n \tag{1}$$

is called **the Nagell's equation**, and Theorem 1 is called **the Nagell's Theorem**.

In 2000 B. Sury [6] attempted to present the first elementary proof of the Nagell's theorem. An important achievement of the author was to show that if for

*Corresponding author.

some integer $n > 1$ the Nagell equation has a solution, then $n \equiv 3 \pmod 4$. Then Sury applied the identity he had discovered and arrived at the contradiction claim that for some integer $n > 3$ the Nagell's equation has a solution. Unfortunately, at the end of his reasoning there is a factual mistake. Namely, he considered an element $\beta = 1 + \sqrt{-2}$ of the ring $\mathbb{Z}[\sqrt{-2}]$ and he stated that for positive integers a and b, according to the binomial theorem, $\beta^{2^a b} = 1 + 2^a b\beta + 2^{a+1}\mu$ for some $\mu \in \mathbb{Z}[\sqrt{-2}]$. However, $\beta^2 = -3 + 2\beta$, so $\beta^4 = -3 - 4\beta$, which shows that this is not the case even for $a = 2$ and $b = 1$.

In this paper we will present the elementary proof of Nagell's theorem based on three things: the analysis of this equation in the Euclidean ring $\mathbb{Z}[\sqrt{-2}]$, the analysis of the binomial coefficients and on the description of all solutions of the Diophantine equations $x^2 - (a^2+2)y^2 = -2$ for $a \in \mathbb{N}$. It is worth noting that all means used by us are natural techniques used in solving Diophantine equations of the form $x^2 + C = y^n$ (cf. [1], [3]). A significant part of the results was presented in [6], so our proof is in fact a correction of a mistake that was committed in there. However, for the sake of completeness, we have decided to give reasons for these results, and our goal is not to detract Sury's achievements.

2. The analysis in the ring $\mathbb{Z}[\sqrt{-2}]$

It is well-known that the subring $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$ of the field of complex numbers is an Euclidean ring with the norm N, where $N(a+b\sqrt{-2}) = a^2 + 2b^2$ for $a, b \in \mathbb{Z}$. Hence, that ring is a unique factorization domain and its group of units is $(\mathbb{Z}[\sqrt{-2}])^* = \{1, -1\}$.

Lemma 1. *Let $x^2 + 2 = y^n$ for some $x, y, n \in \mathbb{Z}$, $n \geq 2$. Then x, y, n are odd, $n \geq 3$, and in the ring $\mathbb{Z}[\sqrt{-2}]$: $x + \sqrt{-2} = (a + \sqrt{-2})^n$ for some odd $a \in \mathbb{Z}$. In particular $y = a^2 + 2$ and*

$$1 = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} a^{n-2j-1} \quad \text{and} \quad x = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j} a^{n-2j}.$$

Proof. Suppose that n is even. Then $a^2 + 2 = b^2$ for some $a, b \in \mathbb{N}$ and the integers a and b have the same parity. Thus, the integers $b - a$ and $b + a$ are even and $4 \mid (b - a)(b + a) = 2$, a contradiction. Therefore n is odd. But $n \geq 2$, so $n \geq 3$.

Next, the integers x and y have the same parity. If both of these numbers are even, then $4 \mid x^2$ and $4 \mid y^n$, since $n \geq 2$. Hence $4 \mid y^n - x^2 = 2$, a contradiction. Therefore x and y are odd.

We claim that in the ring $\mathbb{Z}[\sqrt{-2}]$ the elements $x+\sqrt{-2}$ are $x-\sqrt{-2}$ are coprime. Assume otherwise. By the uniqueness assumption, there exists a prime element π being a common divisor of these elements. Then $\pi \mid (x+\sqrt{-2})-(x-\sqrt{-2}) = 2\sqrt{-2} = -(\sqrt{-2})^3$. Since $2 = (-\sqrt{-2})\cdot\sqrt{-2}$, we have $\pi \mid \sqrt{-2}$ and $\pi \mid 2$. But $\pi \mid x+\sqrt{-2}$, so $\pi \mid x$. As we have shown $x = 2k+1$ for some $k \in \mathbb{Z}$ and $\pi \mid 2$, so $\pi \mid 1$, a contradiction. Therefore the elements $x+\sqrt{-2}$ and $x-\sqrt{-2}$ are coprime.

Moreover, in the ring $\mathbb{Z}[\sqrt{-2}]$ we have: $(x+\sqrt{-2})\cdot(x-\sqrt{-2}) = y^n$, so by the uniqueness assumption, $x+\sqrt{-2} = u\cdot\alpha^n$ for some $u \in (\mathbb{Z}[\sqrt{-2}])^* = \{1,-1\}$, and for some $\alpha \in \mathbb{Z}[\sqrt{-2}]$. But n is odd, so $x+\sqrt{-2} = (a+b\sqrt{-2})^n$ for some $a,b \in \mathbb{Z}$. Hence $x^2+2 = |x+\sqrt{-2}|^2 = |a+b\sqrt{-2}|^{2n} = (a^2+2b^2)^n$, this means that $y^n = (a^2+2b^2)^n$ and since n is odd, we have $y = a^2+2b^2$. But y is also odd, so a is odd.

By the binomial theorem $(a+b\sqrt{-2})^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k(\sqrt{-2})^k$, so

$$(a+b\sqrt{-2})^n =$$

$$\sum_{j=0}^{\frac{n-1}{2}}(-2)^j\binom{n}{2j}a^{n-2j}b^{2j} + \sqrt{-2}\cdot\sum_{j=0}^{\frac{n-1}{2}}(-2)^j\binom{n}{2j+1}a^{n-2j-1}b^{2j+1}.$$

Therefore

$$x = \sum_{j=0}^{\frac{n-1}{2}}(-2)^j\binom{n}{2j}a^{n-2j}b^{2j} \tag{2}$$

and

$$1 = b\cdot\sum_{j=0}^{\frac{n-1}{2}}(-2)^j\binom{n}{2j+1}a^{n-2j-1}b^{2j}. \tag{3}$$

By (3), $b \mid 1$, so $b = \pm 1$. Multiplying both sides of the latter equation by b we find that $b = \sum_{j=0}^{\frac{n-1}{2}}(-2)^j\binom{n}{2j+1}a^{n-2j-1}$. Hence $b \equiv na^{n-1} - 2\binom{n}{3}a^{n-3} \pmod 4$. But the two integers n and a are odd, so $a^{n-1} \equiv 1 \pmod 4$ and $a^{n-3} \equiv 1 \pmod 4$. Thus $b \equiv n - 2\binom{n}{3} \pmod 4$ and $3b \equiv 3n - n(n-1)(n-2) \pmod 4$. Since n is odd, $n^2 \equiv 1 \pmod 4$. Hence $3b \equiv 3n - (1-n)(n-2) = n^2+2 \equiv 3 \pmod 4$, so $3b \equiv 3 \pmod 4$ and $b \equiv 1 \pmod 4$. Moreover $b = \pm 1$, so finally $b = 1$. Hence $y = a^2+2$, $x+\sqrt{-2} = (a+\sqrt{-2})^n$ and by (2) and (3) the result follows. ◄

Using Lemma 1 for $n = 3$ one gets the equation: $1 = 3a^2 - 2$, hence $y = 3$ and $x^2 = 25$, and consequently $x = \pm 5$. From what has already been proved, we deduce the following Euler theorem:

Theorem 2. *The only solutions of the Diophantine equation* $x^2 + 2 = y^3$ *are* $x = \pm 5$, $y = 3$.

Lemma 2. *If* $\beta = 1 + \sqrt{-2}$, *then* $\beta^2 = -3 + 2\beta$, $\beta^3 = -6 + \beta$, *and for any* $a, b \in \mathbb{N}$, $a \geq 2$*:*

$$\beta^{2^a b} = (1 + 2^a b) + 2^a b\beta + 2^{a+1}\mu \text{ for some } \mu \in \mathbb{Z}[\sqrt{-2}]. \tag{4}$$

Proof. Note that $\beta^2 = (1+\sqrt{-2})^2 = 1 + 2\sqrt{-2} + (-2) = -3 + 2(1+\sqrt{-2}) = -3 + 2\beta$. Hence $\beta^3 = \beta(-3+2\beta) = -3\beta + 2\beta^2 = -3\beta + 2(-3+2\beta) = -6+\beta$. Therefore $\beta^4 = \beta(-6+\beta) = -6\beta + \beta^2 = -6\beta + (-3+2\beta) = -3 - 4\beta \equiv (1+2^2) + 2^2\beta \pmod{2^3}$. Suppose that $\beta^{2^a} \equiv (1+2^a) + 2^a\beta \pmod{2^{a+1}}$ for some integer $a \geq 2$. Then $\beta^{2^a} = (1+2^a) + 2^a\beta + 2^{a+1}\mu$ for some $\mu \in \mathbb{Z}[\sqrt{-2}]$. Hence $\beta^{2^{a+1}} = [(1+2^a) + 2^a\beta + 2^{a+1}\mu]^2 = (1+2^a)^2 + 2^{2a}\beta^2 + 2^{2a+2}\mu^2 + 2^{a+1}(1+2^a)\beta + 2^{a+2}(1+2^a)\mu + 2^{2a+1}\beta\mu$. But $a \geq 2$, so $2a+1 > 2a \geq a+3$ and $\beta^{2^{a+1}} \equiv (1+2^a)^2 + 2^{a+1}\beta = 1 + 2^{a+1} + 2^{2a} + 2^{a+1}\beta \equiv (1+2^{a+1}) + 2^{a+1}\beta \pmod{2^{a+2}}$. The principle of induction allows us to conclude that $\beta^{2^a} \equiv (1+2^a) + 2^a\beta \pmod{2^{a+1}}$ for every integer $a \geq 2$.

Now, let $a, b \in \mathbb{N}$ and $a \geq 2$. By the first part of the proof we have $\beta^{2^a} = 1 + 2^a(1+\beta) + 2^{a+1}\mu$ for some $\mu \in \mathbb{Z}[\sqrt{-2}]$. Hence, by the binomial theorem $\beta^{2^a b} = [1 + 2^a(1+\beta) + 2^{a+1}\mu]^b \equiv [1 + 2^a(1+\beta)]^b \equiv 1 + b\cdot 2^a(1+\beta) \equiv (1+2^a b) + 2^a b\beta \pmod{2^{a+1}}$, which ends the proof. ◀

Lemma 3. *Let* $n, t \in \mathbb{N}$, $n > 3$ *and* $t \geq 2$ *are such that* $2^t \mid n-3$ *and* $2^{t+1} \nmid n-3$. *Then*

$$\sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} \equiv 1 + 2^t \pmod{2^{t+1}}.$$

Proof. By the assumptions $n = 2^t b + 3$ for some $t, b \in \mathbb{N}$, where $t \geq 2$ and $2 \nmid b$. In the ring $\mathbb{Z}[\sqrt{-2}]$ for $\beta = 1 + \sqrt{-2}$, by Lemma 2 and the fact that b is odd, we have $\beta^{2^t b} \equiv (1+2^t b) + 2^t b\beta \equiv (1+2^t) + 2^t\beta \pmod{2)^{t+1}}$. But $\beta^3 = \beta - 6$, so $\beta^n \equiv (\beta - 6)[(1+2^t) + 2^t\beta] \equiv (1+2^t)\beta + 2^t\beta^2 - 6 \equiv (1+2^t)\beta + 2^t(-3 + 2\beta) - 6 \equiv (2^t - 6) + (1+2^t)\beta \pmod{2^{t+1}}$. Thus $\beta^n = (2^t - 6) + (1+2^t)\beta + 2^{t+1}\mu$ for some $\mu \in \mathbb{Z}[\sqrt{-2}]$. Hence $\overline{\beta}^n = (2^t - 6) + (1+2^t)\overline{\beta} + 2^{t+1}\overline{\mu}$. Therefore $\beta^n - \overline{\beta}^n = (1+2^t)(\beta - \overline{\beta}) + 2^{t+1}(\mu - \overline{\mu})$. But $\mu = u + v\sqrt{-2}$ for some $u, v \in \mathbb{Z}$ and $\beta - \overline{\beta} = 2\sqrt{-2}$, so $\mu - \overline{\mu} = 2v\sqrt{-2}$. Consequently

$$\frac{\beta^n - \overline{\beta}^n}{2\sqrt{-2}} = 1 + 2^t + 2^{t+1}v. \tag{5}$$

By the binomial theorem

$$\beta^n = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j} + \sqrt{-2} \cdot \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1},$$

so

$$\overline{\beta}^n = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j} - \sqrt{-2} \cdot \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1}.$$

Hence $\frac{\beta^n - \overline{\beta}^n}{2\sqrt{-2}} = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1}$, and the assertion follows from (5). ◄

3. The analysis of the binomial coefficients

Next important lemma was proved by Sury in [6]. For completeness, we present the original proof of Sury in a slightly modified form.

Lemma 4. *If for every integer $n > 3$ the equation $x^2 + 2 = y^n$ has a solution, then $n \equiv 3 \pmod 4$.*

Proof. From Lemma 1 it follows that n is odd and there exists an odd integer a such that $y = a^2 + 2$ and

$$1 = \sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} a^{n-2j-1}. \tag{6}$$

Assume that $n \not\equiv 3 \pmod 4$. Then $n \equiv 1 \pmod 4$. Hence there exists a greatest integer t such that $2^t \mid n-1$. But $4 \mid n-1$, so $t \geq 2$ and $2^{t+1} \nmid n-1$. Hence $n-1 = 2^t(2S+1)$ for some $S \in \mathbb{N}_0$ and, in a consequence, $n \equiv 1 + 2^t \pmod{2^{t+1}}$. Consider any integer $k \geq 3$ such that $2k+1 \leq n$. Then

$$2^k \binom{n}{2k+1} = \frac{2^k}{2k} \cdot (n-1) \cdot \frac{n}{2k+1} \cdot \binom{n-2}{2k-1}. \tag{7}$$

There exist $s \in \mathbb{N}_0$ and odd $u \in \mathbb{N}$ such that $k = 2^s u$. If $k \leq s+1$, then $2^k \mid 2k$. Hence $2^k \leq 2k$ and $2^{k-1} \leq k$. Next, $k \geq 3$, so $k-1 \geq 2$ by binomial theorem, $2^{k-1} = (1+1)^{k-1} \geq 1 + (k-1) + \binom{k-1}{2} > k$, a contradiction. Hence $k \geq s+2$, that is $\frac{2^k}{2k} = \frac{2c}{2v-1}$ for some $c, v \in \mathbb{N}$. Moreover $n-1 = 2^t(2S+1)$ and the integers $2k+1$ and n are odd, so by (7) we have

$$2^k\binom{n}{2k+1} \equiv 0 \pmod{2^{t+1}} \text{ for all } k \geq 3,\ k \leq \frac{n-1}{2}. \tag{8}$$

Thus by (6) it follows that

$$\binom{n}{1}a^{n-1} - 2\binom{n}{3}a^{n-3} + 4\binom{n}{5}a^{n-5} \equiv 1 \pmod{2^{t+1}}. \tag{9}$$

By Euler's theorem $a^{2^t} = a^{\varphi(2^{t+1})} \equiv 1 \pmod{2^{t+1}}$. Taking into account that $n-1 = 2^t(2S+1)$, we get the congruence $a^{n-1} \equiv 1 \pmod{2^{t+1}}$. But $n \equiv 1 + 2^t \pmod{2^{t+1}}$, so:

$$\binom{n}{1}a^{n-1} \equiv 1 + 2^t \pmod{2^{t+1}}. \tag{10}$$

Denote $D = 2\binom{n}{3}a^{n-3}$. Then $D = \frac{n(n-1)(n-2)}{3} \cdot a^{n-3}$ and $n \equiv 1+2^t \pmod{2^{t+1}}$, so $3D \equiv (1+2^t)\cdot 2^t \cdot (2^t-1)\cdot a^{n-3} \equiv 3\cdot 2^t \pmod{2^{t+1}}$, since $2 \mid (1+2^t)\cdot(2^t-1)\cdot a^{n-3}-3$ and the fact that a is odd. Therefore $D \equiv 2^t \pmod{2^{t+1}}$. By the above

$$2\binom{n}{3}a^{n-3} \equiv 2^t \pmod{2^{t+1}}. \tag{11}$$

Denote $E = 4\binom{n}{5}a^{n-5}$. Then $E = \frac{n(n-1)(n-2)(n-3)(n-4)}{2\cdot 3\cdot 5}a^{n-5}$ and $n = 1 + 2^t + 2^{t+1}S$, so $15E = (1+2^t+2^{t+1}S)(2^t+2^{t+1}S)(2^t+2^{t+1}S-1)(2^{t-1}+2^tS-1)(2^t+2^{t+1}S-3)\cdot a^{n-5}$. But $t \geq 2$, so $(1+2^t+2^{t+1}S)(2^t+2^{t+1}S-1)(2^{t-1}+2^tS-1)(2^t+2^{t+1}S-3)a^{n-5} = 2g+1$ for some $g \in \mathbb{Z}$. Hence $15E \equiv 2^t(2g+1) \equiv 2^t \equiv 15 \cdot 2^t \pmod{2^{t+1}}$. Thus $E \equiv 2^t \pmod{2^{t+1}}$. By the above

$$4\binom{n}{5}a^{n-5} \equiv 2^t \pmod{2^{t+1}}. \tag{12}$$

By congruences (10)-(12) and (9) it follows that $(1+2^t) - 2^t + 2^t \equiv 1 \pmod{2^{t+1}}$. Consequently $2^{t+1} \mid 2^t$, a contradiction. Finally $n \equiv 3 \pmod 4$. ◄

4. The analysis of the Pell's equation

Lemma 5. *If $a, x, y \in \mathbb{N}$ and $x^2 - (a^2+2)y^2 = 1$, then $x \equiv 1 \pmod a$ and $y \equiv 0 \pmod a$.*

Proof. Since $a^2 < a^2 + 2 < (a+1)^2$, we see that $D = a^2 + 2$ is not a square of an integer, and the equation $x^2 - Dy^2 = 1$ is a Pell's equation. One of the solutions of this equation is (a^2+1, a). Next, $x^2 - Dy^2 > 0$ and $D > a^2$, so $x^2 > Dy^2 > (ay)^2$ and $x > ay$. Hence $x \geq ay + 1$ and $1 = x^2 - Dy^2 \geq (ay+1)^2 - Dy^2 = (ay+1)^2 - (a^2+2)y^2 = 1 + 2ay - 2y^2$. Thus $2y^2 \geq 2ay$ and consequently $y \geq a$. Hence, the pair (a^2+1, a) is a minimal solution of this equation. Hence, by the description of all solutions of the general Pell's equation (cf. [5]) we conclude that $x + y\sqrt{D} = [(a^2+1) + a\sqrt{D}]^m$ for some $m \in \mathbb{N}$. But $(a^2+1) + a\sqrt{D} \equiv 1 \pmod{a}$ in the ring $\mathbb{Z}[\sqrt{D}]$, so $x + y\sqrt{D} \equiv 1 \pmod{a}$. Hence $x \equiv 1 \pmod{a}$ and $y \equiv 0 \pmod{a}$ in the ring $\mathbb{Z}$. ◄

Lemma 6. *Assume that the integers $a, x, y \in \mathbb{N}$ are such that $x^2 - (a^2+2)y^2 = -2$. Then $x \equiv 0 \pmod{a}$ and $y \equiv 1 \pmod{a}$.*

Proof. If $y = 1$, then $x = a$ and the assertion is clear. Let $y > 1$. Then $x^2 = (a^2+2)y^2 - 2 > a^2 + 2 - 2 = a^2$ and consequently $x > a$.

But $x^2 - (a^2+2)y^2 = -2$, so $x^2 - a^2y^2 \equiv 0 \pmod{2}$, $x^2 \equiv x \pmod{2}$, and $ay \equiv a^2y^2 \pmod{2}$. Hence $x - ay \equiv 0 \pmod{2}$ and $\frac{x-ay}{2} \in \mathbb{Z}$. Moreover $x^2 - a^2y^2 = 2y^2 - 2 > 0$, since $y > 1$ and consequently $x - ay > 0$. Hence $\frac{x-ay}{2} \in \mathbb{N}$. Next, $x \equiv ay \pmod{2}$, so $ax \equiv a^2y \equiv (a^2+2)y \pmod{2}$ and $\frac{(a^2+2)y-ax}{2} \in \mathbb{Z}$. We also have $(a^2+2)^2y^2 - a^2x^2 = (a^2+2)(x^2+2) - a^2x^2 = 2a^2 + 2x^2 + 4 > 0$, so $(a^2+2)y > ax$ and by the above, we obtain $\frac{(a^2+2)y-ax}{2} \in \mathbb{N}$. Moreover

$$\frac{x + y\sqrt{a^2+2}}{a + \sqrt{a^2+2}} = \frac{(a^2+2)y - ax}{2} + \frac{x - ay}{2}\sqrt{a^2+2}. \tag{13}$$

Denote $D = a^2 + 2$. A map $r + s\sqrt{D} \mapsto \overline{r + s\sqrt{D}} = r - s\sqrt{D}$ for $r, s \in \mathbb{Q}$ is an automorphism of the field $\mathbb{Q}(\sqrt{a^2+2})$ and $(r + s\sqrt{D}) \cdot \overline{r + s\sqrt{D}} = r^2 - Ds^2$, so by the formula (13) we get

$$\frac{\overline{x + y\sqrt{a^2+2}}}{\overline{a + \sqrt{a^2+2}}} = \frac{(a^2+2)y - ax}{2} - \frac{x - ay}{2}\sqrt{a^2+2}. \tag{14}$$

Multiplying equations (13) and (14) and taking into account that $x^2 - (a^2+2)y^2 = -2$ and $a^2 - (a^2+2) \cdot 1^2 = -2$ we obtain $1 = \frac{-2}{-2} = [\frac{(a^2+2)y-ax}{2}]^2 - (a^2+2)[\frac{x-ay}{2}]^2$. Thus by Lemma 5, $\frac{(a^2+2)y-ax}{2} \equiv 1 \pmod{a}$ and $\frac{x-ay}{2} \equiv 0 \pmod{a}$. Hence $\frac{(a^2+2)y-ax}{2} + \frac{x-ay}{2}\sqrt{D} \equiv 1 \pmod{a}$ in the ring $\mathbb{Z}[\sqrt{D}]$. By the formula (13), $x + y\sqrt{D} = (a + \sqrt{D}) \cdot [\frac{(a^2+2)y-ax}{2} + \frac{x-ay}{2}\sqrt{D}]$, so $x + y\sqrt{D} \equiv \sqrt{D} \pmod{a}$. Hence $x \equiv 0 \pmod{a}$ and $y \equiv 1 \pmod{a}$ in the ring $\mathbb{Z}$. ◄

Lemma 7. *Let $n > 3$ be an integer. If $x^2+2 = y^n$ for some $x, y \in \mathbb{Z}$, then $y = 3$.*

Proof. According to Lemma 4, $n = 4m + 3$ for some $m \in \mathbb{N}_0$. From Lemma 1, x is odd and $y = a^2 + 2$ for some odd integer a satisfing (6). Hence, without loss of generality, we can assume $a \in \mathbb{N}$. Furthermore $1 \equiv (-2)^{\frac{n-1}{2}} \pmod{a}$. In addition $\frac{n-1}{2} = 2m + 1$, so

$$2^{\frac{n-1}{2}} \equiv -1 \pmod{a}. \tag{15}$$

Moreover, x is odd, so we may assume that $x \in \mathbb{N}$ and the equality $x^2 + 2 = y^n$ can be rewritten as $x^2 - (a^2 + 2)[y^{\frac{n-1}{2}}]^2 = -2$. From Lemma 6 we get $y^{\frac{n-1}{2}} \equiv 1 \pmod{a}$. But $y \equiv 2 \pmod{a}$, so $2^{\frac{n-1}{2}} \equiv 1 \pmod{a}$. Thus by (15), $1 \equiv -1 \pmod{a}$, so $a \mid 2$. But a is odd, so $a = 1$ and $y = 3$. ◀

5. Proof of the Nagell's theorem

Now we are ready to prove the Nagell's theorem. Suppose that for some integer $n > 3$ there exist integers x and y such that $x^2 + 2 = y^n$. By Lemma 4 we get $n \equiv 3 \pmod{4}$, hence there exists an integer $t \geq 2$ such that $2^t \mid n - 3$ and $2^{t+1} \nmid n - 3$. By Lemma 7 and its proof, we have $y = 3$ and $\sum_{j=0}^{\frac{n-1}{2}} (-2)^j \binom{n}{2j+1} = 1$. Hence by Lemma 3 $1 \equiv 1 + 2^t \pmod{2^{t+1}}$, and consequently $2^{t+1} \mid 2^t$, a contradiction. Therefore the Diophantine equation (1) for $n > 3$ has no solution and the Nagell's theorem 1 is proved.

References

[1] J.H.E. Cohn, *The diophantine equation $x^2 + C = y^n$*, Acta Arithmetica **LXV(4)**, 1993, 367–381.

[2] W. Ljunggren, *Über einige Arcustangens gleichungen die auf interessante unbestimmte. Gleichungen fuhrer*, Ark. Mat. Astr. Fys., **29(13)**, 1943.

[3] T. Nagell, *The diophantine equation $x^2 + 7 = 2^n$*, Norsk. Mat. Tidsskr., **30**, 1948, 62–64.

[4] T. Nagell, *Verallgemeinerung eines Fermatschen Satzes*, Arch. Math. (Basel), **5**, 1954, 153–159.

[5] W. Sierpiński, *Elementary theory of numbers*, North-Holland, PWN - Polish Scientific Publishers, Amsterdam - New York - Oxford, 1988.

[6] B. Sury, *On the Diophantine equation* $x^2 + 2 = y^n$, Arch. Math. (Basel), **74**, 2000, 350–355.

R.R. Andruszkiewicz
Institute of Mathematics, University of Białystok, Ciołkowskiego 1M, 15-245 Bialystok, Poland
E-mail: randrusz@math.uwb.edu.pl

N. Andruszkiewicz
Institute of Mathematics, University of Białystok, Ciołkowskiego 1M, 15-245 Bialystok, Poland
E-mail: nandrusz@math.uwb.edu.pl

Received 04 June 2019
Accepted 28 January 2020