O podzielności rozwiązań równania Pella

Adam Barański

1 Wprowadzenie

Równanie Pella to równanie diofantyczne postaci

$$x^2 - dy^2 = 1, \tag{1}$$

gdzie d jest dodatnią liczbą całkowitą. Oczywistymi rozwiązaniami tego równania są $x = 1, y = 0$ oraz $x = -1, y = 0$. Wszystkie pozostałe rozwiązania (gdzie $x \neq 0, y \neq 0$) można podzielić na czwórki różniące się jedynie znakiem przy x, y. Będziemy zajmować się tak zwanymi dodatnimi rozwiązaniami, kiedy $x, y > 0$. Łatwo wykazać, że dla d będącego kwadratem liczby całkowitej takich rozwiązań nie ma. Wiemy również, że jeśli d nie jest kwadratem liczby całkowitej, to rozwiązań takich jest nieskończenie wiele. Każdą taką parę rozwiązań będziemy oznaczać przez (x_n, y_n) i możemy ją zapisać w postaci

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \tag{2}$$

gdzie (x_1, y_1) jest pierwszą nietrywialną parą rozwiązań równania (1), to znaczy $x_1 \neq 1$ oraz dla każdej liczby naturalnej k zachodzi $x_k \geqslant x_1$ (więcej możemy przeczytać na przykład w [1, rozdział XI] oraz w [2]).

W niniejszej pracy udowodnimy kilka twierdzeń dotyczących podzielności współrzędnych (x_n, y_n) tego równania przez różne liczby naturalne. Praca podzielona jest na sześć rozdziałów. W rozdziałach 2–4 będziemy przyjmować, że d jest daną dowolną liczbą naturalną, nie będącą kwadratem liczby całkowitej. W rozdziale 5 rozważamy sytuację, gdy $d = 2$. W ostatnim rozdziale rozpatrywane będą oba wyżej wymienione przypadki.

W drugim rozdziale przedstawimy podstawowe własności ciągów (x_n), (y_n) i ich okresów modulo różne liczby naturalne. W trzecim zajmiemy się dzielnikami pierwszymi w ogólności, a więc rozważymy podstawowe własności zbiorów $\mathbb{P}(x_n)$, $\mathbb{P}(y_n)$, zbiorów liczb pierwszych, dla których istnieją wyrazy odpowiednio ciągów (x_n), (y_n) podzielne przez tę liczbę. W rozdziale czwartym przyjrzymy się liczbom pierwszym oraz złożonym jako dzielnikom wyrazów ciągu (x_n), badając problem dla jakich liczb pierwszych (bądź złożonych) istnieje wyraz ciągu (x_n) podzielny przez tę liczbę. W kolejnym, piątym rozdziale dokładniej rozważymy przykład podzielności elementów ciągu (x_n) przez liczby pierwsze, dla ustalonego $d = 2$. W ostatnim zaś przedstawimy proponowane tematy dalszych badań oraz rozwiązane problemy, które trudno zakwalifikować do którejś z powyższych grup, a mimo to warte są opisania.

2 Podstawowe własności

Najpierw pokażemy, że ciąg (x_n) jest rekurencyjny. A mianowicie spełnia taką samą rekurencję jak ciąg

$$x_1 + y_1\sqrt{d}, (x_1 + y_1\sqrt{d})^2, (x_1 + y_1\sqrt{d})^3, \ldots$$

Mamy

$$g = x_1+y_1\sqrt{d} \Rightarrow (g-x_1)^2 = (y_1\sqrt{d})^2 \iff g^2 = g\cdot 2x_1-(x_1^2-dy_1^2) \iff g^{n+2} = g^{n+1}\cdot 2x_1-g^n,$$

to znaczy, że ciąg (x_n) spełnia rekurencję

$$x_{n+2} = 2x_1 \cdot x_{n+1} - x_n. \tag{3}$$

Ponadto przyjmujemy $x_0 = 1$.

Lemat 1. *Niech $m \geqslant 2$. Istnieje takie $t \in \mathbb{N}$, że*

$$x_t \equiv 1 \mod m \quad i \quad x_{t+1} \equiv x_1 \mod m.$$

Dowód. Niech $f_m \colon \mathbb{Z} \to \mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ będzie dane wzorem

$$f_m(x) = r \iff x \equiv r \mod m.$$

Dla każdej liczby $k \in \mathbb{N}$ mamy

$$(f_m(x_k), f_m(x_{k+1})) \in \mathbb{Z}_m \times \mathbb{Z}_m.$$

Zbiór $\mathbb{Z}_m \times \mathbb{Z}_m$ ma m^2 elementów. Zatem istnieje takie $k < l$, że

$$\begin{gathered}(f_m(x_k), f_m(x_{k+1})) = (f_m(x_l), f_m(x_{l+1})), \text{ czyli} \\ x_k \equiv x_l \mod m \text{ oraz } x_{k+1} \equiv x_{l+1} \mod m.\end{gathered}$$

Z (3) wynika wówczas, że

$$\begin{gathered}x_{k-1} \equiv x_{l-1} \mod m, \\ \vdots \\ x_0 \equiv x_{l-k} \mod m,\end{gathered}$$

wtedy $t = l - k$. □

Najmniejsze takie $t \in \mathbb{N}$ będziemy nazywać okresem ciągu $(x_n) \mod m$. Ponieważ ciąg (y_n) spełnia taką samą rekurencję, mamy

$$y_t \equiv y_0 \equiv 0 \mod m$$

Lemat 2. *Niech $m \geqslant 2$ oraz t – okres ciągu $(x_n) \mod m$. Wtedy dla dowolnej liczby $k \in \mathbb{N}$ mamy*

$$x_k \equiv x_{t+k} \mod m.$$

Dowód. Zauważmy, że z (2) wynika

$$x_{t+k} + y_{t+k}\sqrt{d} = (x_t + y_t\sqrt{d})(x_k + y_k\sqrt{d}),$$

czyli

$$x_{t+k} = x_t x_k + y_t y_k d.$$

Lecz z Lematu 1 $x_t \equiv 1 \mod m$ oraz $y_t \equiv 0 \mod m$. Podstawiając, otrzymujemy

$$x_{t+k} \equiv 1 \cdot x_k + 0 \equiv x_k \mod m.$$

□

Bezpośrednio z Lematu 2 mamy

$$t|k \iff x_k \equiv x_t \equiv x_0 \mod m. \tag{4}$$

W ten sposób udowodniliśmy, że ciąg $(x_n) \mod m$ jest okresowy. Możemy teraz udowodnić podstawowe własności jego okresów. Najpierw jednak zdefiniujmy pojęcie reszty kwadratowej.

Reszta kwadratowa $\mod p$, dla liczby pierwszej p, to taka liczba całkowita a, że istnieje całkowite rozwiązanie kongruencji

$$x^2 \equiv a \mod p.$$

Dla dowolnych liczb $a \in \mathbb{N}$, $p \in \mathbb{P}$, gdzie $\mathbb{P}$ jest zbiorem wszystkich liczb pierwszych, przez $\left(\frac{a}{p}\right)$ oznaczamy symbol Legendre'a. Definiujemy go następująco

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{jeśli } p|a \\ 1 & \text{jeśli } a \text{ jest resztą kwadratową} \mod p \\ -1 & \text{jeśli } a \text{ nie jest resztą kwadratową} \mod p \end{cases}.$$

Lemat 3. *Przez t oznaczmy okres ciągu $(x_n) \mod p$, gdzie p jest dowolną liczbą pierwszą większą od 2. Zachodzą wtedy równoważności*

$$\left(\frac{d}{p}\right) = 1 \iff t|p-1, \tag{5}$$

$$\left(\frac{d}{p}\right) = -1 \iff t|p+1. \tag{6}$$

Dowód. Z (2) mamy

$$x_p + y_p\sqrt{d} = (x_1 + y_1\sqrt{d})^p = \sum_{k=0}^{p} \binom{p}{k} x_1^k (y_1\sqrt{d})^{p-k}.$$

To znaczy, że

$$x_p = \sum_{2|k}^{p} \binom{p}{k} x_1^k (y_1\sqrt{d})^{p-k}, \quad y_p\sqrt{d} = \sum_{2|k}^{p} \binom{p}{k} x_1^k (y_1\sqrt{d})^{p-k}.$$

Jednakże dla $p > k > 0$, $p|\binom{p}{k}$, gdyż $p \in \mathbb{P}$, a więc

$$x_p \equiv x_1^p \mod p \text{ oraz } y_p \equiv y_1^p d^{\frac{p-1}{2}} \mod p,$$

co na mocy Małego Twierdzenia Fermata (patrz [1, rozdział IV, Twierdzenie 4]) jest równoważne z

$$x_p \equiv x_1 \mod p \text{ oraz } y_p \equiv y_1 \left(\frac{d}{p}\right) \mod p.$$

Czyli z (2) mamy

$$x_{p+1} + y_{p+1}\sqrt{d} = (x_p + y_p\sqrt{d})(x_1 + y_1\sqrt{d}),$$

tym samym $x_{p+1} \equiv x_p x_1 + y_p y_1 d \mod p$, co oznacza, że zachodzi

$$x_{p+1} \equiv x_1^2 + y_1^2 d \left(\frac{d}{p}\right) \mod p.$$

Jeśli $\left(\frac{d}{p}\right) = 1$, to $x_{p+1} \equiv x_1^2 + y_1^2 d \mod p$, czyli korzystając z (1) otrzymujemy

$$x_{p+1} \equiv 2x_1^2 - (x_1^2 - y^2 d) \equiv 2x_1^2 - 1 \mod p.$$

Ale z rekurencji (3) mamy $x_{p-1} = 2x_1 x_p - x_{p+1}$, tym samym

$$x_{p-1} \equiv 2x_1^2 - (2x_1^2 - 1) \equiv 1 \mod p,$$

więc na podstawie (4)

$$t|p-1.$$

Jeśli zaś $\left(\frac{d}{p}\right) = -1$, to $x_{p+1} \equiv x_1^2 - y_1^2 d \mod p$, więc korzystając z (1),

$$x_{p+1} \equiv 1 \mod p,$$

czyli

$$t|p+1.$$

□

Lemat 4. *Niech $m \in \mathbb{N}$, $m > 2$, t będzie okresem ciągu $(x_n) \mod m$. Wtedy*

$$\exists_{k\in\mathbb{N}}\ m|x_k \iff 4|t.$$

Dowód. 1) Uznajmy, że istnieje takie k, że $m|x_k$. Możemy przyjąć, że jest to najmniejsza taka liczba naturalna. Wtedy z (2)

$$(x_k + y_k\sqrt{d})^2 = x_{2k} + y_{2k}\sqrt{d}.$$

Czyli $x_{2k} \equiv x_k^2 + y_k^2 d \mod m$. Zachodzą następujące równoważności

$$x_{2k} \equiv x_k^2 + y_k^2 d \mod m \iff x_{2k} \equiv 2x_k^2 - (x_k^2 - y_k^2 d) \mod m \iff x_{2k} \equiv -1 \mod m,$$

bowiem $x_k \equiv 0 \mod m$. Analogicznie

$$(x_{2k} + y_{2k}\sqrt{d})^2 = x_{4k} + y_{4k}\sqrt{d}.$$

Mamy

$$x_{4k} \equiv x_{2k}^2 + y_{2k}^2 d \mod m \iff x_{4k} \equiv 2x_{2k}^2 - (x_{2k}^2 - y_{2k}^2 d) \mod m \iff x_{4k} \equiv 1 \mod m.$$

To znaczy, że z (4) mamy $t|4k$. Oprócz tego, ponieważ $x_{2k} \equiv -1 \mod m$, to $t \nmid 2k$. Ponadto $t > k$, gdyż oczywistym jest, że $t \neq k$, a w przeciwnym razie $k - t \in \mathbb{N}$, więc z Lematu 2 mamy $x_k \equiv x_{k-t} \mod m$. Czyli

$$x_{k-t} \equiv 0 \mod m,$$

jednakże $k - t < k$, a założyliśmy, że k jest najmniejszą taką liczbą naturalną. Czyli

$$t|4k,\ t \nmid 2k,\ t > k \Rightarrow t = 4k,$$

ponieważ jedynymi dzielnikami liczby $4k$ większymi od k są liczby $2k$ i $4k$.

2) Uznajmy, że $4|t$. Wtedy $t = 4k$, dla pewnego $k \in \mathbb{N}$. A więc z (2)

$$(x_{2k} + y_{2k}\sqrt{d})^2 = x_{4k} + y_{4k}\sqrt{d}.$$

Mamy

$$x_{2k}^2 + y_{2k}^2 d \equiv x_{4k} \mod m \iff 2x_{2k}^2 - (x_{2k}^2 - y_{2k}^2 d) \equiv x_{4k} \mod m \iff x_{2k}^2 \equiv 1 \mod m.$$

Lecz $4k \nmid 2k$, więc z (4) $x_{2k} \not\equiv 1 \mod m$, to znaczy, że

$$x_{2k} \equiv -1 \mod m.$$

Podobnie

$$(x_k + y_k\sqrt{d})^2 = x_{2k} + y_{2k}\sqrt{d},$$

to znaczy, że $x_k^2 + y_k^2 d \equiv x_{2k} \mod m$. Ponadto zachodzi

$$x_k^2 + y_k^2 d \equiv x_{2k} \mod m \iff 2x_k^2 - (x_k^2 - y_k^2 d) \equiv x_{2k} \mod m \iff 2x_k^2 \equiv 0 \mod m.$$

Ale $m > 2$, czyli

$$m|x_k.$$

□

Na tym zakończymy tę część. Powyższe lematy wykorzystane zostaną w następnych rozdziałach.

3 Zbiory $\mathbb{P}(x_n)$, $\mathbb{P}(y_n)$

Oznaczmy przez

- $\mathbb{P}(y_n)$ zbiór takich liczb pierwszych, że istnieje $i \in \mathbb{N}$, że $y_i \equiv 0 \mod p$,
- $\mathbb{P}(x_n)$ zbiór takich liczb pierwszych, że istnieje $i \in \mathbb{N}$, że $x_i \equiv 0 \mod p$.

Udowodnimy, że

Twierdzenie 1. $\mathbb{P}(y_n) = \mathbb{P}$.

Twierdzenie 2. $\#\mathbb{P}(x_n) = \infty$.

Twierdzenie 3. $\#\mathbb{P} \setminus \mathbb{P}(x_n) = \infty$.

Dowód Twierdzenia 1. Istnienie okresu ciągu (x_n) oznacza, że również ciąg (y_n) jest okresowy. Oznaczmy okres ciągu (y_n) przez t. Analogicznie dla ciągu (y_n), z Lematu 2

$$y_0 \equiv y_t \mod p \iff y_t \equiv 0 \mod p.$$

Tym samym znaleźliśmy $t \in \mathbb{N}$, że $y_t \equiv 0 \mod p$. □

Dowód Twierdzenia 2. Uznajmy nie wprost, że $\#\mathbb{P}(x_n) = k$, dla pewnego $k \in \mathbb{N}$. Oznaczmy wszystkie liczby pierwsze należące do $\mathbb{P}(x_n)$, jako $p_1, p_2, \ldots, p_k$. Niech

$$t_i \text{ to okres ciągu } (x_n) \mod p_i, \text{ dla } i \in \{1, 2, \ldots, k\}.$$

Niech

$$T = \prod_{i \in \{1,2,\ldots,k\}} t_i.$$

Z (4)

$$\forall_{i \in \{1,2,\ldots,k\}}\ x_T \equiv x_0 \mod p,$$

tym samym

$$\forall_{i \in \{1,2,\ldots,k\}}\ x_T \equiv 1 \mod p_i.$$

A więc żadna z liczb $p_1, p_2, \ldots, p_k$ nie dzieli x_T. Jednakże wtedy dla $q \in \mathbb{P}$ i $q | x_T$ mamy

$$q \in \mathbb{P}(x_n), \quad q \neq p_1, p_2, \ldots, p_k,$$

więc otrzymaliśmy sprzeczność. □

Dowód Twierdzenia 3. Załóżmy, że zbiór $\mathbb{P} \setminus \mathbb{P}(x_n)$ jest skończony. To znaczy, że od pewnej liczby naturalnej m dla każdego $p \in \mathbb{P}$, $p > m$ istnieje takie k naturalne, że

$$p | x_k,$$

Jednakże z (1)

$$x_k \equiv 0 \mod p \iff -y_k^2 d \equiv 1 \mod p.$$

Więc

$$-d \equiv \frac{1}{y_k^2} \mod p,$$

co oznacza

$$\left(\frac{-d}{p}\right) = 1.$$

A więc dla każdej liczby $p > m$ mamy

$$\left(\frac{-d}{p}\right) = 1.$$

Jest to jednak niemożliwe, co zaraz udowodnimy. Rozłóżmy d na czynniki pierwsze, a więc

$$d = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_s^{\alpha_s},$$

gdzie $q_1,\ q_2,\ \ldots,\ q_s \in \mathbb{P}$. Dla porządku przyjmijmy

$$q_1 < q_2 < \cdots < q_s.$$

Rozważmy przypadki:

I) $q_1 > 2$

Wiemy, że istnieje $x \in \{1, 2, \ldots, s\}$, że $\alpha_x \equiv 1 \mod 2$ – wynika to z założenia, że d nie jest kwadratem liczby całkowitej. Ponieważ liczby $8, q_1, q_2, \ldots, q_s$ są parami względnie pierwsze, to na podstawie Chińskiego Twierdzenia o Resztach (patrz [3, Twierdzenie 5.8]) istnieje taka liczba całkowita k, że

$$\begin{cases} k \equiv 1 \mod 8 \\ k \equiv r_i \mod q_i \text{ dla } i \in \{1, 2, \ldots, s\} \setminus \{x\} \\ k \equiv n_x \mod q_x \end{cases},$$

gdzie $r_1, r_2, \ldots, r_s$ to reszty kwadratowe odpowiednio $\mod q_1, q_2, \ldots, q_s$ (bez q_x), zaś n_x to niereszta kwadratowa $\mod q_x$. Zauważmy, że jeśli $\mathrm{NWD}(k, 8d) > 1$ to jedna z liczb $2, q_1, q_2, \ldots, q_s$ musi dzielić $\mathrm{NWD}(k, 8d)$ – wynika to wprost z rozkładu liczby $8d$ na czynniki pierwsze. Jednak z drugiej strony żadna z tych liczb nie dzieli k, bowiem k jest nieparzyste oraz $r_1, r_2, \ldots, n_x, \ldots, r_s$ są względnie pierwsze odpowiednio z $q_1, q_2, \ldots, q_s$, gdyż są resztami (i w jednym przypadku niereszą) kwadratowymi. Czyli mamy

$$k \perp 8d.$$

A więc na mocy Twierdzenia Lejeune-Dirichleta o liczbach pierwszych w postępie arytmetycznym (patrz [1, str. 79]), istnieje liczba całkowita a, taka że

$$8d \cdot a + k = p \in \mathbb{P} \qquad \text{oraz} \qquad p > m.$$

Zatem

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q_1}{p}\right)^{\alpha_1}\cdots\left(\frac{q_s}{p}\right)^{\alpha_s}.$$

Ale

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1, \text{ ponieważ } p \equiv 1 \mod 8.$$

(patrz [1, rozdział XIV, własność II, IV]). Ponadto mamy $p \equiv k \mod 8d$.

1) Dla $i \in \{1, 2, \ldots, s\} \setminus \{x\}$

$$p \equiv k \equiv r_i \mod q_i \Rightarrow \left(\frac{p}{q_i}\right) = \left(\frac{r_i}{q_i}\right) = 1,$$

ale z Prawa Wzajemności Reszt Kwadratowych (patrz [1, rozdział XIV, własność V]

$$\left(\frac{q_i}{p}\right)\left(\frac{p}{q_i}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q_i-1}{2}} = 1,$$

z czego wynika

$$\left(\frac{q_i}{p}\right) = 1.$$

2) Podobnie

$$p \equiv k \equiv n_x \mod q_x \Rightarrow \left(\frac{p}{q_x}\right) = \left(\frac{n_x}{q_x}\right) = -1,$$

więc

$$\left(\frac{q_x}{p}\right)\left(\frac{p}{q_x}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q_x-1}{2}} = 1 \Rightarrow \left(\frac{q_x}{p}\right) = -1.$$

To znaczy, że

$$\left(\frac{-d}{p}\right) = 1 \cdot 1^{\alpha_1} \cdots (-1)^{\alpha_x} \cdots 1^{\alpha_s} = -1,$$

otrzymaliśmy sprzeczność.

IIa) $q_1 = 2$ oraz istnieje $q_x \neq 2$, że $\alpha_x \equiv 1 \mod 2$. Skoro $k \equiv 1 \mod 8$, to $\left(\frac{k}{2}\right) = 1$ – mimo, że liczby $(8, q_1 = 2)$ nie są względnie pierwsze, to istnieje k spełniające układ modulo z (I). Pozostała część dowodu przebiega analogicznie.

IIb) $q_1 = 2$ oraz nie istnieje $q_x \neq 2$, że $\alpha_x \equiv 1 \mod 2$. Wtedy mamy

$$d = 2r^2,$$

dla pewnego r całkowitego. Więc

$$\left(\frac{-d}{p}\right) = \left(\frac{-2}{p}\right)\cdot\left(\frac{r^2}{p}\right) = \left(\frac{-2}{p}\right).$$

Ale wtedy wystarczy wziąć np. $p \equiv -1 \mod 8$ oraz $p > m$ i mamy

$$\left(\frac{-d}{p}\right) = -1,$$

czyli sprzeczność z wcześniejszym założeniem na m.

We wszystkich przypadkach I, IIa, IIb uzyskaliśmy sprzeczność, więc niemożliwe jest by dla każdej liczby $p > m$

$$\left(\frac{-d}{p}\right) = 1,$$

co oznacza, że zbiór $\mathbb{P} \setminus \mathbb{P}(x_n)$ jest nieskończony. □

4 Liczby pierwsze i złożone jako dzielniki

Najpierw sprawdźmy podzielność wyrazów ciągu (x_n) przez różne potęgi dwójki. Niech

$$v_2(c) = \alpha \iff 2^\alpha | c \text{ oraz } 2^{\alpha+1} \nmid c,$$

$v_2(c)$ będziemy nazywać wykładnikiem 2-adycznym liczby c. Udowodnimy następujący lemat

Lemat 5. *Dla dowolnej liczby $k \in \mathbb{N}$,*

$$v_2(x_{2k}) = 0, \qquad v_2(x_{2k-1}) = v_2(x_1).$$

Dowód Lematu 5. Z (2)

$$x_{2k} + y_{2k}\sqrt{d} = (x_k + y_k\sqrt{d})^2.$$

To oznacza, że $x_{2k} = x_k^2 + y_k^2 d$, czyli

$$x_{2k} = x_k^2 + y_k^2 d = 2x_k^2 - (x_k^2 - dy_k^2) = 2x_k^2 - 1$$

A więc $v_2(x_{2k}) = 0$, dla każdego k naturalnego.

Udowodnimy indukcyjnie, że $v_2(x_{2k-1}) = v_2(x_1)$ dla każdego $k \in \mathbb{N}$. Dla $k = 1$ mamy $v_2(x_1) = v_2(x_1)$. Załóżmy, że dla pewnego $k \geqslant 1$ mamy

$$v_2(x_{2k-1}) = v_2(x_1) = \alpha,$$

dla pewnej liczby całkowitej α. Wykażemy, że

$$v_2(x_{2k+1}) = v_2(x_1) = \alpha.$$

Czyli z założenia indukcyjnego mamy

$$x_1 = 2^\alpha \cdot r, \; x_{2k-1} = 2^\alpha \cdot r',$$

dla pewnych $r,\ r'$ nieparzystych. Z rekurencji (3)

$$v_2(x_{2k+1}) = v_2(2x_1 \cdot x_{2k} - x_{2k-1}) = v_2(2^\alpha \cdot 2x_{2k}r - 2^\alpha \cdot r') = v_2(2^\alpha(2x_{2k}r - r')).$$

Jednak skoro r' jest nieparzyste, to $2x_{2k}r - r'$ również, a więc $v_2(2^\alpha(2x_{2k}r - r')) = \alpha$, czyli

$$v_2(x_{2k+1}) = \alpha,$$

co chcieliśmy wykazać. □

Teraz możemy zająć się pozostałymi liczbami pierwszymi, większymi od 2. Zauważmy, że bezpośrednio z Lematów 3, 4 otrzymujemy

$$\exists_i\ x_i \equiv 0 \mod p \Rightarrow \left(\left(\frac{d}{p}\right) = 1,\ p \equiv 1 \mod 4 \vee \left(\frac{d}{p}\right) = -1,\ p \equiv 3 \mod 4\right), \qquad (7)$$

bowiem w przeciwnym razie, w obydwu przypadkach otrzymalibyśmy $4|2$, co jest oczywiście niemożliwe.

Ujemne równanie Pella to równanie diofantyczne postaci

$$a^2 - db^2 = -1,$$

gdzie d jest dodatnią liczbą całkowitą. Udowodnimy, że

Twierdzenie 4. *Niech $p \in \mathbb{P}$, $p > 2$. Dla takiego d, że ujemne równanie Pella ma rozwiązanie, zachodzi*

$$\left(\frac{d}{p}\right) = -1, p \equiv 3 \mod 4 \Rightarrow \exists_i\ x_i \equiv 0 \mod p.$$

Dowód Twierdzenia 4. Przez (a, b) oznaczmy pierwszą parę rozwiązań ujemnego równania Pella. Znanym faktem jest, że zachodzi

$$(a + b\sqrt{d})^2 = x_1 + y_1\sqrt{d}.$$

Czyli

$$(a + b\sqrt{d})^{p+1} = x_{\frac{p+1}{2}} + y_{\frac{p+1}{2}}\sqrt{d},$$

więc

$$x_{\frac{p+1}{2}} = \sum_{2|k}^{p+1} \binom{p+1}{k} a^k (b\sqrt{d})^{p+1-k},$$

jednak dla $p > k > 1$, $p|\binom{p+1}{k}$, gdyż $p \in \mathbb{P}$, oznacza to, że

$$x_{\frac{p+1}{2}} \equiv a^{p+1} + b^{p+1}d^{\frac{p+1}{2}} \equiv a^2 + b^2\left(\frac{d}{p}\right)d \equiv a^2 - b^2 d \equiv -1 \mod p.$$

Niech t to okres ciągu $(x_n) \mod p$. Wtedy

$$t \nmid \frac{p+1}{2},$$

ponadto z Lematu 3

$$t|p+1,$$

a więc z tych dwóch własności otrzymujemy

$$v_2(p+1) = v_2(t).$$

Ale $p \equiv 3 \mod 4$, czyli

$$v_2(p+1) \geqslant 2 \iff v_2(t) \geqslant 2 \iff 4|t,$$

więc z Lematu 4

$$\exists_i \; x_i \equiv 0 \mod p.$$

□

Co ciekawe dla d takiego, że istnieje rozwiązanie ujemnego równania Pella, nie zawsze wystarczy $\left(\frac{d}{p}\right) = 1,\ p \equiv 1 \mod 4$, aby $\exists_i \; x_i \equiv 0 \mod p$ – przykładem są $d = 5, p = 29$.

Ponownie zajmujemy się tylko równaniem Pella postaci (1). Skoro wiemy już, dla jakich liczb pierwszych istnieje rozwiązanie x_n tego równania podzielne przez tę liczbę, od razu narzuca się pytanie, dla jakich liczb złożonych m jest to możliwe. Warto więc rozważyć dwa prostsze przypadki, które posłużą nam do rozwiązania ogólnego.

Lemat 6. *Niech t_α – okres ciągu $(x_n) \mod p^\alpha$. Dla każdej liczby pierwszej $p > 2$ nie będącej dzielnikiem d i dowolnej $\alpha \in \mathbb{N}$ zachodzi*

$$v_2(t_1) = v_2(t_\alpha).$$

Lemat 7. *Niech p, q to dowolne względnie pierwsze liczby nieparzyste, takie że dla pewnych $i, j \in \mathbb{N}$, $p|x_i$ i $q|x_j$. Oznaczmy odpowiednio przez t, s okresy ciągu (x_n) modulo p, q. Wtedy*

$$v_2(t) = v_2(s) \iff \exists_{k \in \mathbb{N}} \quad pq|x_k.$$

Dowód Lematu 6. Dowód tego lematu przeprowadzimy za pomocą indukcji. Dla $\alpha = 1$ jest to prawda. Załóżmy więc, że dla pewnej $\alpha \geqslant 1$

$$v_2(t_\alpha) = v_2(t_1).$$

Wykażemy, że

$$v_2(t_{\alpha+1}) = v_2(t_1).$$

Zauważmy, że z (2)

$$x_{t_\alpha p} + y_{t_\alpha p}\sqrt{d} = (x_{t_\alpha} + y_{t_\alpha}\sqrt{d})^p \iff x_{t_\alpha p} + y_{t_\alpha p}\sqrt{d} = \sum_{k=0}^{p} \binom{p}{k} x_{t_\alpha}^k (y_{t_\alpha}\sqrt{d})^{p-k}.$$

Jednak skoro $x_{t_\alpha} \equiv 1 \mod p^\alpha$, to z (1) $y_{t_\alpha}^2 d \equiv 0 \mod p^\alpha$. Czyli dla nieparzystych $k \in \{1, 2, \dots p-2\}$ mamy

$$p \mid \binom{p}{k} \text{ oraz } p^\alpha \mid (y_{t_\alpha}\sqrt{d})^{p-k},$$

czyli $p^{\alpha+1} \mid \binom{p}{k}(y_{t_\alpha}\sqrt{d})^{p-k}$, gdy k nieparzyste, a więc

$$x_{t_\alpha p} \equiv \sum_{2\nmid k}^{p} \binom{p}{k} x_{t_\alpha}^k (y_{t_\alpha}\sqrt{d})^{p-k} \equiv x_\alpha^p \mod p^{\alpha+1} \Rightarrow x_{t_\alpha p} \equiv x_\alpha^p \mod p^{\alpha+1}.$$

Ponieważ $p^\alpha | x_{t_\alpha} - 1$, to z LTE (Lifting The Exponent Lemma) (patrz [3, Twierdzenie 2.18])

$$v_p(x_{t_\alpha}^p - 1) = v_p(x_{t_\alpha} - 1) + v_p(p) \geqslant \alpha + 1,$$

czyli

$$p^{\alpha+1} | x_{t_\alpha}^p - 1 \iff x_{t_\alpha}^p \equiv 1 \mod p^{\alpha+1} \iff x_{t_\alpha p} \equiv 1 \mod p^{\alpha+1}.$$

Lecz z Lematu 2 oznacza to, że $t_{\alpha+1} | t_\alpha p$, z czego wynika

$$v_2(t_{\alpha+1}) \leqslant v_2(t_\alpha p) = v_2(t_\alpha).$$

Jednak oczywistym jest, że jeśli $x_{t_{\alpha+1}} \equiv 1 \mod p^{\alpha+1}$, to tym bardziej $x_{t_{\alpha+1}} \equiv 1 \mod p^\alpha$, czyli $t_\alpha | t_{\alpha+1}$, więc

$$v_2(t_{\alpha+1}) \geqslant v_2(t_\alpha).$$

To oznacza zaś, że otrzymujemy

$$v_2(t_\alpha) \geqslant v_2(t_{\alpha+1}) \geqslant v_2(t_\alpha) \iff v_2(t_{\alpha+1}) = v_2(t_\alpha),$$

co kończy dowód. □

Do dowodu Lematu 7 będziemy potrzebowali następującej własności

Lemat 8. *Niech m będzie dowolną liczbą nieparzystą, dla której istnieje taka liczba i, że $m | x_i$. Przez $4t$ oznaczmy okres ciągu $(x_n) \mod m$. Dla dowolnej dodatniej liczby całkowitej k zachodzi wtedy*

$$x_k \equiv 0 \mod m \iff k \equiv t \mod 2t.$$

Dowód Lematu 8. Z Lematu 4 wynika, że t jest liczbą naturalną. Niech $k' \in \{1, 2, \dots, 4t\}$ i $m | x_{k'}$. Mamy więc

$$x_{2k'} + y_{2k'}\sqrt{d} = (x_{k'} + y_{k'}\sqrt{d})^2 \Longrightarrow \begin{cases} x_{2k'} \equiv x_{k'}^2 + y_{k'}^2 d \equiv 2x_{k'}^2 - 1 \equiv -1 \mod m \\ y_{2k'} \equiv 2x_{k'}y_{k'} \equiv 0 \mod m \end{cases}.$$

Czyli

$$x_{4k'} + y_{4k'}\sqrt{d} = (x_{2k'} + y_{2k'}\sqrt{d})^2 \Longrightarrow \begin{cases} x_{4k'} \equiv x_{2k'}^2 + y_{2k'}^2 d \equiv 2x_{2k'}^2 - 1 \equiv 1 \mod m \\ y_{4k'} \equiv 2x_{2k'}y_{2k'} \equiv 0 \mod m \end{cases}.$$

A więc z Lematu 2 mamy $4t|4k'$, tym samym

$$t|k'.$$

Ale to znaczy, że $k' \in \{t, 2t, 3t, 4t\}$, jednak $x_{2t} \equiv -1 \mod m$, $x_{4t} \equiv 1 \mod m$, więc $k' = t$ lub $k' = 3t$. Ale ze wzoru (2)

$$x_{3t} + y_{3t}\sqrt{d} = (x_t + y_t\sqrt{d})(x_{2t} + y_{2t}\sqrt{d}),$$

czyli

$$x_{3t} \equiv x_t x_{2t} + y_t y_{2t} d \equiv -x_t \mod m,$$

bowiem z (2) mamy $x_{2t} \equiv -1$, zaś $y_{2t} \equiv 0 \mod m$. Czyli $x_t \equiv x_{3t} \equiv 0 \mod m$. A więc zachodzi

$$m|x_k \iff \exists_c\ (k = t + 4t \cdot c \vee k = 3t + 4t \cdot c),$$

ale

$$\exists_c\ (k = t + 4t \cdot c \vee k = 3t + 4t \cdot c) \iff k \equiv t \mod 2t.$$

Zatem mamy

$$m|x_k \iff k \equiv t \mod 2t.$$

□

Dowód Lematu 7. Z Lematu 4, $4|t, s$. Czyli istnieją takie $t', s' \in \mathbb{N}$, że $t = 4t'$, $s = 4s'$. Ponadto zauważmy, że z Lematu 8

$$\begin{aligned} p|x_i &\iff i \equiv t' \mod 2t', \\ q|x_i &\iff i \equiv s' \mod 2s'. \end{aligned}$$

A więc, ponieważ $\mathrm{NWD}(p, q) = 1$, to mamy

$$\exists_{k\in\mathbb{N}}\ pq|x_k \iff \exists_{k\in\mathbb{N}} \begin{cases} k \equiv t' \mod 2t' \\ k \equiv s' \mod 2s' \end{cases}.$$

Udowodnimy, że

$$\exists_{k\in\mathbb{N}} \begin{cases} k \equiv t' \mod 2t' \\ k \equiv s' \mod 2s' \end{cases} \iff v_2(t') = v_2(s').$$

Oczywiste jest, że

$$\exists_{k\in\mathbb{N}} \begin{cases} k \equiv t' \mod 2t' \\ k \equiv s' \mod 2s' \end{cases} \Rightarrow v_2(t') = v_2(s'),$$

bo wtedy

$$v_2(k) = v_2(t'), \quad v_2(k) = v_2(s'),$$

czyli

$$v(t') = v(s').$$

To znaczy, że wystarczy wykazać

$$v_2(t') = v_2(s') \Rightarrow \exists_{k\in\mathbb{N}} \begin{cases} k \equiv t' \mod 2t' \\ k \equiv s' \mod 2s' \end{cases}.$$

Niech $v_2(t') = v_2(s') = c$, dla pewnego $c \in \mathbb{N}$. A więc $2^c \cdot t'' = t'$ oraz $2^c \cdot s'' = s'$, gdzie t'', s'' są nieparzyste. Istotnie istnienie rozwiązań k, k' układów kongruencji

$$\begin{cases} k \equiv t' \mod 2t' \\ k \equiv s' \mod 2s' \end{cases}, \qquad \begin{cases} k' \equiv t'' \mod 2t'' \\ k' \equiv s'' \mod 2s'' \end{cases}$$

jest równoważne, bowiem jeśli k' spełnia drugi układ, to $2^c \cdot k'$ jest rozwiązaniem pierwszego (i odwrotnie, bo $2^c | k$, dla każdego k spełniającego pierwszu układ). Jednakże dla $k' = t'' \cdot s''$ mamy

$$t''|k', \quad s''|k' \quad \wedge \quad 2 \cdot t'' \nmid k', \quad 2 \cdot s'' \nmid k',$$

ponieważ $2 \nmid t'', s''$. Czyli

$$\begin{cases} k' \equiv t'' \mod 2t'' \\ k' \equiv s'' \mod 2s'' \end{cases},$$

co oznacza, że

$$\begin{cases} 2^c \cdot k' \equiv t' \mod 2t' \\ 2^c \cdot k' \equiv s' \mod 2s' \end{cases}.$$

A więc podsumowując

$$\begin{cases} k \equiv t' \mod 2t' \\ k \equiv s' \mod 2s' \end{cases} \iff v_2(t') = v_2(s'),$$

ale skoro $v_2(t') = v_2(s')$, to $v_2(4t') = v_2(4s')$, czyli podstawiając $4t' = t, 4s' = s$ mamy $v_2(t) = v_2(s)$. To znaczy, że wykazaliśmy

$$\exists_{k\in\mathbb{N}}\ pq|x_k \iff \exists_{k\in\mathbb{N}} \begin{cases} k \equiv t' \mod 2t' \\ k \equiv s' \mod 2s' \end{cases} \quad \text{oraz} \quad \exists_{k\in\mathbb{N}} \begin{cases} k \equiv t' \mod 2t' \\ k \equiv s' \mod 2s' \end{cases} \iff v_2(t) = v_2(s),$$

więc

$$v_2(t) = v_2(s) \iff \exists_{k\in\mathbb{N}} \quad pq|x_k.$$

□

Twierdzenie 5. *Dla danej liczby naturalnej $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, gdzie $p_1, p_2, \ldots, p_n \in \mathbb{P}$, niech $t_1, t_2, \ldots, t_n$ – okresy ciągu $(x_n) \mod p_1, p_2, \ldots, p_n$ odpowiednio. Wtedy zachodzą następujące fakty*

(1) m jest liczbą nieparzystą

$$\exists_k\ x_k \equiv 0 \mod m \iff v_2(t_1) = v_2(t_2) = \cdots = v_2(t_n) \geqslant 2.$$

(2) m jest liczbą parzystą (bez straty ogólności $p_1 = 2$)

$$\exists_k\ x_k \equiv 0 \mod m \iff \alpha_1 \leqslant v_2(x_1) \text{ oraz } v_2(t_2) = v_2(t_3) = \cdots = v_2(t_n) = 2.$$

Dowód Twierdzenia 5.
(1) m jest liczbą nieparzystą
Oczywistym jest, że

$$v_2(t_1), v_2(t_2), \ldots, v_2(t_n) \geqslant 2,$$

bowiem w przeciwnym razie z Lematu 4 któraś z liczb $p_1, p_2, \ldots, p_n$ nie należałaby do zbioru $\mathbb{P}(x_n)$, więc tym bardziej nie istniałoby i, że $m | x_i$. Ponieważ liczby $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_n^{\alpha_n}$ są parami względnie pierwsze to na podstawie Lematu 7 indukcyjnie otrzymujemy

$$\exists_k\ x_k \equiv 0 \mod p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \iff v_2(s_1) = v_2(s_2) = \cdots = v_2(s_n),$$

gdzie $s_1, s_2, \ldots, s_n$ to okresy ciągu $(x_n) \mod p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_n^{\alpha_n}$ odpowiednio. Jednakże na podstawie Lematu 6

$$v_2(t_i) = v_2(s_i),$$

dla każdego $i \in \{1, 2, \ldots, n\}$. A więc otrzymujemy

$$\exists_k\ x_k \equiv 0 \mod m \iff v_2(t_1) = v_2(t_2) = \cdots = v_2(t_n) \geqslant 2.$$

(2) m jest liczbą parzystą
Z pierwszego podpunktu Twierdzenia 5 dla liczby nieparzystej $m' = p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_n^{\alpha_n}$ mamy

$$\exists_k\ x_k \equiv 0 \mod m \iff v_2(t_2) = v_2(t_3) = \cdots = v_2(t_n) \geqslant 2.$$

Z Lematu 5 otrzymujemy dodatkowe założenie na szukane k, a mianowicie $2 \nmid k$. Jednak z Lematu 8

$$k \equiv \frac{t_i}{4} \mod \frac{t_i}{2},$$

dla $i \in \{2, 3, \ldots, n\}$. Czyli

$$4 | t, \quad 2 \nmid \frac{t_i}{4} \iff v_2(t_i) = 2,$$

Ponadto z Lematu 5 zachodzi $v_2(x_1) = v_2(x_k)$ dla każdej nieparzystej k, więc na pewno $\alpha_1 \leqslant v_2(x_1)$. Podsumowując otrzymujemy

$$\exists_k\ x_k \equiv 0 \mod m \iff \alpha_1 \leqslant v_2(x_1) \text{ oraz } v_2(t_2) = v_2(t_3) = \cdots = v_2(t_n) = 2.$$

□

5 Przypadek dla $d = 2$

W tym rozdziale będziemy przyjmować $d = 2$, a więc rozważane równanie Pella przyjmuje postać

$$x^2 - 2y^2 = 1 \tag{8}$$

Udowodnimy następujące twierdzenia.

Twierdzenie 6. *Dla każdej liczby pierwszej p*

$$p \equiv 5, 7 \mod 8 \Rightarrow p \notin \mathbb{P}(x_n).$$

Twierdzenie 7. *Istnieje nieskończenie wiele liczb pierwszych p, że*

$$p \equiv 1 \mod 8 \quad \textit{oraz} \quad p \in \mathbb{P}(x_n).$$

Twierdzenie 8. *Dla każdej liczby pierwszej p*

$$p \equiv 3 \mod 8 \Rightarrow p \in \mathbb{P}(x_n).$$

Najpierw przeprowadzimy dowód Twierdzenia 6.

Dowód twierdzenia 6. Zauważmy, że dla każdego naturalnego i

$$x_i \equiv 0 \mod p \Rightarrow -2y^2 \equiv 1 \mod p,$$

co jest równoważne z

$$-2 \equiv \left(\frac{1}{y_k}\right)^2.$$

Zatem

$$\left(\frac{-2}{p}\right) = 1.$$

Jednakże

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}},$$

więc dla $p \equiv 5, 7 \mod 8$

$$\left(\frac{-2}{p}\right) = -1,$$

to znaczy, że

$$p \equiv 5, 7 \Rightarrow p \notin \mathbb{P}(x_n).$$

□

Do dowodu Twierdzenia 7 będziemy potrzebować następującego lematu

Lemat 9. *Dla każdej liczby pierwszej $p > 2$ i takich u, v, że $p \nmid u, v$, zachodzi*

$$p|u^2 + v^2 \iff p \equiv 1 \mod 4.$$

Dowód Lematu 9. Załóżmy nie wprost, że $p = 4k + 3$.

$$p|u^2 + v^2 \iff u^2 \equiv -v^2 \mod p,$$

więc skoro $\frac{p-1}{2} = \frac{4k+2}{2}$ jest liczbą nieparzystą, to

$$(u^2)^{\frac{p-1}{2}} \equiv (-v^2)^{\frac{p-1}{2}} \mod p \iff u^{p-1} \equiv -v^{p-1} \mod p,$$

z Małego Twierdzenia Fermata otrzymujemy

$$1 \equiv -1 \mod p,$$

sprzeczność. □

Dowód twierdzenia 7. Załóżmy nie wprost, że takich liczb jest skończona liczba n. Oznaczmy je przez $p_1, p_2, \ldots, p_n$. Niech

$$t_i \text{ to okres ciągu } (x_n) \mod p_i, \text{ dla } i \in \{1, 2, \ldots, n\}$$

oraz

$$T = \prod_{i \in \{1,2,\ldots,n\}} t_i.$$

Z Lematu 4 mamy $4|t_1$, więc tym bardziej

$$2|T.$$

Zauważmy, jednak, że dla dowolnej $l \in \mathbb{N}$ z (2)

$$x_{2l} = x_l^2 + 2y_l^2,$$

co jest równoważne z

$$x_{2l} = 4y_l^2 + (x_l^2 - 2y_l^2) = 4y_l^2 + 1,$$

więc x_{2l} można zapisać w postaci sumy dwóch kwadratów. Tym samym, skoro $2|T$ to x_T również możemy zapisać w postaci sumy dwóch kwadratów. A więc z Lematu 9 wszystkie dzielniki pierwsze liczby x_T są postaci $4m + 1$. Jednak z (4)

$$x_T \equiv x_0 \mod p_i,$$

dla $i \in \{1, 2, \ldots, n\}$, więc żadna z liczb $p_1, p_2, \ldots, p_n$ nie dzieli x_T. Ale na podstawie Twierdzenia 6 $p \not\equiv 5 \mod 8$. Otrzymaliśmy tym samym sprzeczność, bowiem $p \equiv 1 \mod 4 \iff p \equiv 1, 5 \mod 8$. □

Teraz udowodnimy ostatnie z twierdzeń w tym rozdziale.

Dowód twierdzenia 8. Ponieważ dla $d = 2$ istnieje rozwiązanie ujemnego równania Pella, ponadto

$$p \equiv 3 \mod 8 \Rightarrow \left(\frac{2}{p}\right) = -1.$$

A więc na podstawie Twierdzenia 4

$$p \in \mathbb{P}(x_n).$$

□

6 Proponowane tematy badań

W tym rozdziale przedstawione zostaną zadania (wraz z przykładowymi rozwiązaniami) oraz proponowane otwarte problemy związane z podzielnością wyrazów ciągów $(x_n), (y_n)$ równania Pella.

Zacznijmy od zadań. Pierwsze z nich inspirowane jest zadaniem nr 4 z zawodów finałowych LXVII Olimpiady Matematycznej.

Zadanie 1. Rozważamy równanie (1) z danym $d \in \mathbb{N}$, nie będącym kwadratem liczby całkowitej. Wyznaczyć wszystkie takie pary różnych nieparzystych liczb naturalnych (k, l), dla których istnieje takie $a \in \mathbb{N}$, że

$$k|x_a \qquad \text{oraz} \qquad l|y_a,$$

ale także istnieje takie $b \in \mathbb{N}$, że

$$l|x_b \qquad \text{oraz} \qquad k|y_b.$$

Rozwiązanie. Na początku zauważmy, że dla dowolnego i i dowolnej naturalnej liczby m nieparzystej mamy

$$y_i \equiv 0 \mod m \Rightarrow x_i^2 \equiv 1 \mod m,$$

a więc

$$x_i \equiv \pm 1 \mod m.$$

Niech r będzie okresem ciągu $(x_n) \mod m$. Tym samym r jest okresem ciągu (y_n), bowiem obydwa te ciągi spełniają taką samą rekurencję. Czyli

(1) $x_i \equiv 1 \mod m$. Wtedy z Lematu 1 zachodzi $r|i$, więc tym bardziej $r|2i$.

(2) $x_i \equiv -1 \mod m$. Wtedy mamy z (2)

$$(x_i + y_i\sqrt{d})^2 = x_{2i} + y_{2i}\sqrt{d},$$

więc

$$x_{2i} \equiv x_i^2 + y_i^2 d \equiv 2x_i^2 - (x_i^2 - y_i^2 d) \equiv 1 \mod m.$$

Zatem $r|2i$.

A więc w obydwu przypadkach zachodzi

$$r|2i.$$

Teraz przejdziemy do głównej części rozwiązania. Udowodnimy, że nie ma takich liczb, które spełniają wymagania zadania. Uznajmy nie wprost, że istnieją takie k, l, które spełniają żądane własności. Skoro $k|x_a$ oraz $l|x_b$, to na podstawie Lematu 4 okresy ciągu $(x_n) \mod k$ i $\mod l$ są podzielne przez 4. A więc istnieją takie liczby $s,\ t$, że $4s,\ 4t$ są okresami ciągu $(x_n) \mod k,\ \mod l$ odpowiednio. Czyli skoro $k|x_a$ oraz $l|x_b$, to na podstawie Lematu 8

$$a \equiv s \mod 2s \text{ oraz } b \equiv t \mod 2t.$$

To oznacza, że

$$v_2(a) = v_2(s), \qquad v_2(b) = v_2(t).$$

Ponadto, ponieważ $l|y_a$ i $k|y_b$, to na podstawie wcześniej udowodnionego faktu

$$2a \equiv 0 \mod 4t \text{ oraz } 2b \equiv 0 \mod 4s,$$

co jest równoważne z

$$a \equiv 0 \mod 2t \text{ oraz } b \equiv 0 \mod 2s,$$

zatem

$$v_2(a) \geqslant v_2(2t), \qquad v_2(b) \geqslant v_2(2s).$$

Jednak to znaczy, że

$$v_2(a) \geqslant v_2(2t) > v_2(t) = v_2(b) \geqslant v_2(2s) > v_2(s) = v_2(a),$$

czyli

$$v_2(a) > v_2(a),$$

a więc otrzymaliśmy sprzeczność.

□

Zadanie 2. Udowodnić, że równanie

$$(a^2 + b^2)^2 - 2(c^2 + d^2)^2 = 1,$$

nie ma rozwiązań w liczbach całkowitych $a,\ b,\ c,\ d$.

Rozwiązanie. Niech

$$S = \{s^2 + t^2 : s, t \in \mathbb{Z}\}$$

Chcemy więc udowodnić, że nie istnieje taka liczba k, że

$$x_k,\ y_k \in S.$$

Uznajmy nie wprost, że istnieje takie k. Jednakże z Lematu 9, to znaczy, że

$$x_k \equiv 1 \mod 4,$$

bowiem jeśli jakaś liczba pierwsza p dzieli x_k, to albo $p \equiv 1 \mod 4$, albo $p \equiv 3 \mod 4$ dzieli x_k w parzystej potędze (zaś $3^2 \equiv 1 \mod 4$). Ponadto $2 \nmid x_k$. Rozważmy dwa przypadki

1. k jest nieparzyste. Wtedy istnieje k', takie że $k = 2k' + 1$. Korzystając z (2) otrzymujemy

$$x_k + y_k\sqrt{2} = (3 + 2\sqrt{2})(x_{2k'} + y_{2k'}\sqrt{2}).$$

Zatem

$$x_k = 3x_{2k'} + 4y_{2k'}.$$

Ale z (2) mamy $x_{2k'} = x_{k'}^2 + 2y_{k'}^2$, czyli

$$x_{2k'} \equiv 4y_{k'} + (x_{k'} - 2y_{k'}) \equiv 1 \mod 4.$$

To znaczy, że

$$x_k \equiv 3x_{2k'} + 4y_{2k'} \equiv 3 \mod 4,$$

a więc $x_k \notin S$.

2. k jest parzyste. Niech $v_2(k) = \alpha$. Zatem $k = 2^\alpha r$, gdzie $2 \nmid r$. Ze wzoru (2) wprost wynika, że dla dowolnego i

$$y_{2i} = 2x_i y_i.$$

Po α-krotnym podstawieniu tego faktu otrzymujemy

$$y_{2^\alpha r} = 2x_{2^{\alpha-1}r}y_{2^{\alpha-1}r} = 2^2 x_{2^{\alpha-1}r}x_{2^{\alpha-2}r}y_{2^{\alpha-2}r} = \cdots = 2^\alpha x_{2^{\alpha-1}r}x_{2^{\alpha-2}r}\cdots x_r y_r.$$

A więc, jeśli $y_k \in S$ to albo $x_r \in S$, albo x_r jest kwadratem liczby całkowitej. Ale w obydwu tych przypadkach mielibyśmy $x_r \equiv 1 \mod 4$, zaś z udowodnionego wcześniej faktu, skoro r nieparzyste, to $x_r \equiv 3 \mod 4$.

W obydwu przypadkach uzyskaliśmy sprzeczność, a więc nie istnieje takie k, że $x_k,\ y_k \in S$. □

Na koniec przedstawiamy proponowane nierozwiązane problemy.

Problem 1. Dla równania (8) udowodnić, że istnieje nieskończenie wiele liczb pierwszych p, takich że

$$p \equiv 1 \mod 8 \quad \text{oraz} \quad p \notin \mathbb{P}(x_n).$$

Problem 2. Rozważamy równanie (1). Scharakteryzować, dla jakich $r \in \{1, 2, \ldots, 4d-1\}$, że $\mathrm{NWD}(r, 4d) = 1$ istnieje nieskończenie wiele $p \in \mathbb{P}$, $p \equiv r \mod 4d$, takich że

$$p \in \mathbb{P}(x_n).$$

Literatura

[1] Wacław Sierpiński, *Teoria liczb*, wydanie 3 powiększone, Monografie Matematyczne, tom XIX, Warszawa–Wrocław 1950.

[2] Wacław Sierpiński, *Wstęp do teorii liczb*, wydanie 3 poprawione, Biblioteczka Matematyczna 25, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1987.

[3] Adam Neugebauer, *Algebra i Teoria Liczb*, wydanie XV (rozszerzone), Matematyka Olimpijska, Volumina.pl, Szczecin 2017.