MINUT 2021 (3), s. 17–30
ISSN 2719-3063

Michał RÓŻAŃSKI[1], Barbara SMOLEŃ-DUDA[1], Roman WITUŁA[1]

[1]Katedra Matematyki, Politechnika Śląska, ul. Kaszubska 23, 44-100 Gliwice

O rozkładzie liczb naturalnych na sumę kwadratów liczb naturalnych

Streszczenie. Praca ta porusza temat rozkładu liczb naturalnych na sumę kwadratów liczb naturalnych. Szczególną uwagę poświęcono twierdzeniu Fermata, dotyczącemu rozkładu liczb pierwszych postaci $4n + 1$ na sumę kwadratów dwóch liczb naturalnych. Szczegółowo przedstawiony został jeden z najmłodszych dowodów tego twierdzenia. Przytoczono również elementarny dowód twierdzenia Eulera mówiącego o tym, że jeżeli daną liczbę nieparzystą można zapisać w postaci sumy kwadratów dwóch liczb naturalnych na dwa sposoby, to liczba ta jest liczbą złożoną. Natomiast w ostatnim rozdziale przedstawiono twierdzenia dotyczące mocy zbiorów liczb pierwszych zawartych w ciągach liczb naturalnych stanowiących wartości pewnych wielomianów kwadratowych.

Słowa kluczowe: sumy kwadratów liczb naturalnych, rozkłady liczb naturalnych, liczby pierwsze

1. Wstęp

Gdy słyszymy o sumie kwadratów dwóch liczb naturalnych, to najczęściej przychodzi nam do głowy twierdzenie Pitagorasa i słynne trójki pitagorejskie np. $(3, 4, 5)$ czy $(5, 12, 13)$. Jednak nie jest to jedyne słynne twierdzenie nawiązujące do takich sum. Na przestrzeni lat, wielu matematyków starało się odpowiedzieć na pytania: *Kiedy daną liczbę naturalną można przedstawić w postaci sumy kwadratów dwóch liczb naturalnych* i *kiedy rozkład taki jest jednoznaczny?*. Dzisiaj znamy wiele twierdzeń zawierających, przynajmniej częściowo, odpowiedzi na te pytania. Jednym z najsłynniejszych twierdzeń w tej tematyce jest, bez wątpienia, twierdzenie Fermata o sumach kwadratów.

2. Fermat i jego twierdzenie

W 1640 roku Pierre de Fermat zakomunikował ojcu Mersennowi następujące twierdzenie:

Twierdzenie 1 (Fermata o sumach kwadratów). *Każda liczba pierwsza postaci* $4n+1$, $n \in \mathbb{N}$, *może być zapisana jednoznacznie w postaci sumy kwadratów dwóch liczb naturalnych.*

Autor korespondencyjny: B. Smoleń-Duda (Barbara.Smolen-Duda@polsl.pl).
Data wpłynięcia: 30.10.2020.

Jak podaje Mollin [10] twierdzenie to sformułował wcześniej Albert Girard (1595-1632). Jednak, ani Girard, ani Fermat nie opublikowali dowodu tego twierdzenia. Uczynił to dopiero Euler w 1754 roku. Dzisiaj znanych jest wiele dowodów tego twierdzenia, m.in. podanych przez takie sławy świata matematyki jak Lagrange, Gauss czy Dedekind. Jednym z najmłodszych dowodów jest tak zwany „dowód w jednym zdaniu" (ang. „one-sentence proof") zaprezentowany przez Zagiera[1] [18] w 1990r. Przedstawimy tutaj „pełną wersję" tego dowodu. O ile sam dowód rzeczywiście jest stosunkowo zwięzły i krótki, to wymaga on pewnego, wcześniejszego przygotowania. Zacznijmy od udowodnienia następującego twierdzenia:

Twierdzenie 2. *Niech $X \neq \emptyset$ będzie zbiorem skończonym, $f : X \to X$ oraz istnieje liczba pierwsza p, taka że $f^p = id_X$. Jeśli X_0 oznacza zbiór punktów stałych odwzorowania f, to znaczy $X_0 = \{x \in X : f(x) = x\}$, to wtedy zachodzi:*

$$|X| \equiv |X_0| \ (mod\ p).$$

Dowód. Dla dowolnego $x \in X$ symbolem $\mathrm{orb}(x)$ oznaczymy orbitę elementu x, to jest zbiór:

$$\mathrm{orb}(x) := \left\{x, f(x), \ldots, f^{p-1}(x)\right\}.$$

Zauważmy, że orbity elementów $x \in X$ stanowią klasy abstrakcji względem relacji równoważności ρ na X określonej wzorem:

$$(\forall x, z \in X)\left(x \rho z \Leftrightarrow \text{ istnieje } k \in \mathbb{N}_0, k < p, \text{ takie, że } z = f^k(x)\right).$$

Zauważmy, że $|\mathrm{orb}(x)| = 1$, gdzie $x \in X$ wtedy i tylko wtedy, gdy $x = f(x)$, to jest gdy $x \in X_0$. Pokażemy, że jeśli $x \in X$ oraz $|\mathrm{orb}(x)| > 1$, to $|\mathrm{orb}(x)| = p$. W tym celu przypuśćmy, że dla pewnego takiego $x \in X$ mamy $|\mathrm{orb}(x)| < p$. Oznacza to, że istnieją $i, j \in \mathbb{N}_0$, $i < j < p$, dla których $f^i(x) = f^j(x)$, czyli $x = f^{(p-i)+i}(x) = f^{(p-i)+j}(x) = f^{j-i}\left(f^p(x)\right) = f^{j-i}(x)$. Ponieważ $f^p(x) = x$ oraz $\mathrm{NWD}(j-i, p) = 1$, więc istnieją $a, b \in \mathbb{N}$, takie że $ap = b(j-i) + 1$ lub $a(j-i) = bp + 1$, czyli $f(x) = x$. Stąd $|\mathrm{orb}(x)| = 1$, czyli istotnie, jeśli $x \in X$, to albo $|\mathrm{orb}(x)| = 1$, albo $|\mathrm{orb}(x)| = p$.

Podsumowując, zbiór X jest sumą mnogościową $|X_0|$ orbit długości 1 oraz pewnej liczby, powiedzmy n, parami rozłącznych orbit długości p. Zatem $|X| = |X_0| + np$, co implikuje tezę twierdzenia. □

Wniosek 1. *Jeśli S jest zbiorem niepustym, skończonym, odwzorowanie $f : S \to S$ jest inwolucją[2], to moc zbioru S i moc zbioru punktów stałych odwzorowania f mają tę samą parzystość.*

Idąc za uwagą Zagiera z artykułu [18] nadmienimy, że wniosek ten jest kombinatorycznym odpowiednikiem i przypadkiem szczególnym, następującego wyniku topologicznego:

Twierdzenie 3. *Charakterystyka Eulera danej przestrzeni topologicznej i moc zbioru punktów stałych dowolnej ciągłej inwolucji na tej przestrzeni mają tę samą parzystość.*

Zainteresowanym tym faktem Czytelnikom proponujemy jako literaturę uzupełniającą następujące prace [7, 9, 11, 15].

[1] Don Zagier, matematyk niemiecko-amerykański, na stałe związany z uniwersytetem w Bonn w Niemczech, wybitny współczesny specjalista teorii liczb.

[2] Przypomnijmy, że odwzorowanie $f : X \to X$ nazywamy inwolucją jeżeli $f \circ f = \mathrm{id}_X$.

Niech teraz $p \in \mathbb{N}$ będzie liczbą pierwszą, $p \equiv 1 \pmod 4$. Oznaczmy przez S następujący zbiór:

$$S = \left\{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\right\}.$$

Oczywiście S jest zbiorem skończonym (jak na razie nie wiadomo, czy S jest zbiorem niepustym). Pokażemy, że odwzorowanie $f : S \to S$ określone wzorem:

$$S \ni (x, y, z) \overset{f}{\mapsto} \begin{cases} (x + 2z, z, y - x - z) & \text{gdy } x < y - z, \\ (2y - x, y, x - y + z) & \text{gdy } y - z < x < 2y, \\ (x - 2y, x - y + z, y) & \text{gdy } x > 2y, \end{cases} \tag{1}$$

jest inwolucją.
Najpierw sprawdzimy, że jeśli $(x, y, z) \in S$ oraz $x < y - z$, to trójka uporządkowana $(x + 2z, z, y - x - z)$ również należy do S. Faktycznie, mamy: $(x + 2z, z, y - x - z) \in \mathbb{N}^3$ oraz

$$(x + 2z)^2 + 4z(y - x - z) = x^2 + 4xz + 4z^2 + 4zy - 4zx - 4z^2 = x^2 + 4zy \in S.$$

Podobnie weryfikujemy pozostałe dwa przypadki, które redukują się do sprawdzenia, że:

$$\begin{cases} (2y - x, y, x - y + z) \in \mathbb{N}^3, & \text{gdy } y - z < x < 2y, \\ (x - 2y, x - y + z, y) \in \mathbb{N}^3, & \text{gdy } x > 2y \end{cases}$$

oraz

$$(2y - x)^2 + 4y(x - y + z) = 4y^2 - 4xy + x^2 + 4xy - 4y^2 + 4yz = x^2 + 4yz \in S.$$

W kolejnym kroku udowodnimy, że f jest inwolucją. I tak, jeśli $(x, y, z) \in S$ oraz $x < y - z$, to:

$$\begin{aligned} f \circ f(x, y, z) &= f(\underbrace{x + 2z}_{=x_1}, \underbrace{z}_{=y_1}, \underbrace{y - x - z}_{=z_1}) = (\text{mamy } x_1 > 2y_1) \\ &= (x_1 - 2y_1, x_1 - y_1 + z_1, y_1) = (x, y, z), \end{aligned}$$

jeśli $(x, y, z) \in S$ oraz $y - z < x < 2y$, to:

$$\begin{aligned} f \circ f(x, y, z) &= f(\underbrace{2y - x}_{=x_2}, \underbrace{y}_{=y_2}, \underbrace{x - y + z}_{=z_2}) = (\text{mamy } y_2 - z_2 < x_2 < 2y_2) \\ &= (2y_2 - x_2, y_2, x_2 - y_2 + z_2) = (x, y, z), \end{aligned}$$

i wreszcie jeśli $(x, y, z) \in S$ oraz $x > 2y$, to:

$$\begin{aligned} f \circ f(x, y, z) &= f(\underbrace{x - 2y}_{=x_3}, \underbrace{x - y + z}_{=y_3}, \underbrace{y}_{=z_3}) = (\text{mamy } x_3 < y_3 - z_3) \\ &= (x_3 + 2z_3, z_3, y_3 - x_3 - z_3) = (x, y, z), \end{aligned}$$

Zatem odwzorowanie f jest inwolucją.

Teraz przedstawimy zapowiadany wcześniej dowód Twierdzenia Fermata o sumach kwadratów.

Dowód twierdzenia Fermata o sumach kwadratów, zob. [18]. Niech S będzie zbiorem opisanym powyżej, oraz niech dana będzie inwolucja $f : S \to S$ opisana wzorem (1). Odwzorowanie f ma jeden punkt stały, jest to trójka $(1, 1, k)$, taka że $p = 4k + 1$. Stąd na podstawie Wniosku 1 zbiór S jest zbiorem niepustym, o mocy będącej liczbą nieparzystą. Ponieważ również odwzorowanie:

$$S \ni (x, y, z) \overset{g}{\mapsto} (x, z, y)$$

jest inwolucją, a zbiór S ma nieparzystą ilość elementów, więc g posiada punkt stały postaci (x, y, y). Stanowi to dowód jednego tylko faktu z tezy Twierdzenia Fermata, że p jest sumą kwadratów dwóch liczb naturalnych.
Drugi fakt z tezy Twierdzenia Fermata o jednoznaczności takiego rozkładu udowodnimy poniżej w Twierdzeniu 4. Ważnym uzupełnieniem Twierdzenia 4 jest Twierdzenie 6 Wacława Sierpińskiego, które dla autorów artykułu stanowiło odkrycie historyczne - zob. Uwagę 4. □

Teraz rozważmy następujące przykłady rozkładów liczb pierwszych na sumę kwadratów dwóch liczb naturalnych:

$$5 = 1^2 + 2^2, \qquad 13 = 2^2 + 3^2, \qquad 29 = 2^2 + 5^2, \qquad 53 = 2^2 + 7^2, \qquad 173 = 2^2 + 13^2.$$

Wszystkie te przykłady odpowiadają wzorowi:

$$4(n^2 - n + 1) + 1 = 2^2 + (2n - 1)^2, \tag{2}$$

w przypadku gdy liczba $4(n^2 - n + 1) + 1$ jest liczbą pierwszą (przedstawione rozkłady odpowiadają wartościom $n = 1, 2, 3, 4$ oraz $n = 7$). Gdy $n = 5$, to mamy rozkłady:

$$85 = 2^2 + 9^2 = 6^2 + 7^2,$$

a dla $n = 6$ mamy:

$$125 = 2^2 + 11^2 = 5^2 + 10^2,$$

co odpowiada przypadkom, gdy liczba $4(n^2-n+1)+1$ ze wzoru (2) nie jest liczbą pierwszą. Sytuacja ta jest ujęta ogólnie w odkrytym przez Eulera twierdzeniu (około 100 lat po sformułowanym na początku pracy twierdzeniu znalezionym przez Fermata, [17]). Twierdzenie to podamy wraz z elementarnym dowodem.

Twierdzenie 4. *Jeśli N jest liczbą nieparzystą, którą można na dwa sposoby zapisać jako sumę kwadratów liczb naturalnych przy czym nie zwracamy uwagi na porządek składników, to N jest liczbą złożoną.*

Dowód. Niech $N = a^2 + b^2 = c^2 + d^2$, gdzie a, b, c, d są liczbami naturalnymi, takimi że a oraz c są nieparzyste, natomiast b oraz d są parzyste. Mamy:

$$(a - c)(a + c) = (d - b)(d + b). \tag{3}$$

Niech $r = \mathrm{NWD}(a - c, b - d)$, oczywiście r jest parzyste. Niech $a - c := rs$, $d - b := rt$, gdzie $s, t \in \mathbb{N}$, $\mathrm{NWD}(s, t) = 1$. Wtedy z (3) wynika równość:

$$s(a + c) = t(d + b),$$

przy czym $s|(d+b)$ oraz $t|(a+c)$. Stąd mamy:

$$\mathrm{NWD}(a+c, d+b) = u,$$

gdzie u jest parzyste. Pokażemy, że:

$$N = \left[\left(\frac{r}{2}\right)^2 + \left(\frac{u}{2}\right)^2\right] \cdot (s^2+t^2).$$

Mamy:

$$\left[\left(\frac{r}{2}\right)^2 + \left(\frac{u}{2}\right)^2\right] \cdot (s^2+t^2) = \frac{1}{4}\left[(rs)^2 + (rt)^2 + (us)^2 + (ut)^2\right] =$$
$$= \frac{1}{4}\left[(a-c)^2 + (d-b)^2 + (d+b)^2 + (a+c)^2\right] = \frac{1}{2}\left(a^2+b^2+c^2+d^2\right) = N.$$

Zatem N jest liczbą złożoną. □

Wniosek 2. *Jeśli $k \in \mathbb{N}$, $k \geq 2$, to liczba $N = 4k^4 + 1$ jest liczbą złożoną.*

Dowód. Na podstawie Twierdzenia 4 teza wynika wprost z rozkładu:

$$1 + 4k^4 = (2k^2-1)^2 + 4k^2. \tag{4}$$

□

Na przykład, następujące liczby (odpowiadają $k = 5$ i $k = 100$ we wzorze (4)) są złożone:

$$2501 = 1 + 50^2 = 49^2 + 10^2,$$
$$40001 = 1 + 200^2 = 199^2 + 20^2.$$

Przedstawimy jeszcze ważną tożsamość nawiązującą do Wniosku 2..

Lemat 1. *Jeśli $k \in \mathbb{N}$, $k \geq 2$, to mamy rozkład:*

$$N = 4k^4 + 1 = (2k^2+1)^2 - 4k^2 = (2k^2-2k+1)(2k^2+2k+1),$$

czyli N jest liczbą złożoną.

Wacław Sierpiński w książce [13] zauważył, że liczby N z powyższego lematu stanowią jedynie przypadek szczególny ogólniejszej rodziny liczb złożonych $N(n,m) = m^4 + 4n^4$, $m, n \in \mathbb{N}$, gdzie $m \neq 1$ lub $n \neq 1$ o podobnych własnościach, gdyż

$$N(n,m) = (m^2)^2 + (2n^2)^2 = (m^2-2n^2)^2 + (2mn)^2 =$$
$$= (m^2+2n^2)^2 - 4m^2n^2 = (m^2-2mn+2n^2)(m^2+2mn+2n^2).$$

Uwaga 1. Tytułem uzupełnienia podkreślmy, że liczby naturalne postaci $4n+3$ nie mogą być rozłożone na sumę kwadratów dwóch liczb naturalnych, albowiem mamy:

$$\big(2k\big)^2 + \big(2l-1\big)^2 = 4\big(k^2+l^2-l\big)+1,$$

dla dowolnych $k, l \in \mathbb{N}$.

Problem 1. *Czy istnieje nieskończenie wiele liczb pierwszych postaci (2)?*

Uwaga 2. Ponieważ iloczyn liczb naturalnych będących sumami kwadratów dwóch liczb naturalnych również jest sumą kwadratów dwóch liczb naturalnych[3], więc nie zaskakuje następujący wynik ogólny na temat rozkładów liczb naturalnych na sumę kwadratów dwóch liczb naturalnych:

Twierdzenie 5 (zobacz Twierdzenie 6.2 w monografii [10]). *Niech $N \in \mathbb{N}$, przy czym $N = m^2 n$ i n nie jest podzielna przez kwadrat żadnej liczby pierwszej. Wówczas N jest sumą kwadratów dwóch liczb naturalnych wtedy i tylko wtedy, gdy każdy dzielnik pierwszy p liczby n przystaje do jedynki modulo cztery.*

Uwaga 3. Już po otrzymaniu recenzji naszej pracy odkryliśmy w odrobinę historycznej książce Wacława Sierpińskiego z 1961 roku [13] twierdzenie ogólniejsze aniżeli Twierdzenie 4, które przytoczymy tu bez dowodu.

Twierdzenie 6 (W. Sierpiński). *Jeżeli a i b są danymi liczbami naturalnymi, to żadna liczba pierwsza p nie daje się dwoma różnymi sposobami przedstawić w postaci*

$$p = ax^2 + by^2,$$

gdzie x i y są liczbami naturalnymi, o ile, w razie $a = b = 1$, nie zwracamy uwagi na kolejność składników.

Przedstawimy teraz przykłady zastosowania tego twierdzenia do sprawdzenia, czy dana liczba naturalna jest złożona. Mamy:

$$\begin{aligned}
57 &= 2\cdot 4^2 + 5^2 = 2\cdot 2^2 + 7^2,\\
91 &= 9^2 + 10\cdot 1^2 = 1^2 + 10\cdot 3^2,\\
493 &= 21^2 + 13\cdot 2^2 = 13\cdot 6^2 + 5^2,\\
1073 &= 32^2 + 7^2 = 28^2 + 17^2 = 2\cdot 22^2 + 105\cdot 1^2 = 2\cdot 8^2 + 105\cdot 3^2,
\end{aligned}$$

co oznacza, że wszystkie cztery liczby $57, 91, 493$ oraz 1073 są złożone. Autorom artykułu wydaje się, że wykorzystane tu twierdzenie Sierpińskiego chyba jest „nieznane", a na pewno „ma moc"! Po odkryciu książki Sierpińskiego dotarliśmy do jeszcze jednej historycznej książki, tym razem szwajcarskiego matematyka Ernsta Trosta [16] z 1953 roku. Pożółkła czekała na reaktywację w stosie złożonym z wielu innych zapomnianych, sędziwych koleżanek m. in. dwóch monografii Edmunda Landaua z teorii liczb. Trost na stronie 33 wspomnianej książki pokazuje jak z rozkładów liczby N na sumy postaci:

$$N = x_1^2 + dy_1^2 = x_2^2 + dy_2^2 \tag{5}$$

[3]Mamy: $\big(a^2+b^2\big)\big(c^2+d^2\big) = \big(ac+bd\big)^2 + \big(ad-bc\big)^2$.

można otrzymać rozkład liczby N na iloczyn dwóch czynników. I tak, z powyższych równości otrzymujemy:

$$x_1^2 - x_2^2 = d(y_2^2 - y_1^2)$$

lub

$$\frac{x_1 - x_2}{y_2 - y_1} = d\frac{y_2 + y_1}{x_1 + x_2}.$$

Stąd wynika, że istnieją liczby $u, v, s, t \in \mathbb{N}$, gdzie $\mathrm{NWD}(u, v) = 1$, takie że spełniony jest jeden z dwóch następujących układów czterech równań:[4]

$$\begin{array}{llll} \text{a)} & |x_1 - x_2| = dut, & \text{b)} & |y_2 - y_1| = vt, \\ \text{c)} & y_2 + y_1 = us, & \text{d)} & x_1 + x_2 = vs, \end{array} \tag{6}$$

albo

$$\begin{array}{llll} \text{a}_1) & |x_1 - x_2| = ut, & \text{b}_1) & |y_2 - y_1| = vt, \\ \text{c}_1) & y_2 + y_1 = us, & \text{d}_1) & x_1 + x_2 = dvs, \end{array} \tag{7}$$

Szczegółowo rozważymy poniżej jedynie układ a), b), c) i d). Wykonując działania a)$\pm$d) oraz c)$\mp$b) w zależności od tego czy $x_1 - x_2 > 0$ czy też $x_1 - x_2 < 0$, znajdujemy:

$$x_1 = \frac{1}{2}(dut + vs), \qquad y_1 = \frac{1}{2}(us - vt),$$

albo

$$x_1 = \frac{1}{2}(vs - dut), \qquad y_1 = \frac{1}{2}(us + vt)$$

gdyż $(x_1 - x_2)(y_2 - y_1) > 0$, skąd dostajemy:

$$N = \frac{1}{4}(dut \pm vs)^2 + \frac{1}{4}d(us \mp vt)^2 = \frac{1}{4}(v^2 + du^2)(s^2 + dt^2). \tag{8}$$

Ciekawą rolę pełni tu mnożnik $\frac{1}{4}$. Otóż z warunku $\mathrm{NWD}(u, v) = 1$ wynika, że tylko jedna z liczb u lub v może być parzysta. Nie naruszając ogólności rozważań załóżmy najpierw, że $2|u$. Wówczas z opisu

$$y_1 = \frac{1}{2}(us - vt) \tag{9}$$

wynika, że również $2|t$, a ponieważ

$$x_1 = \frac{1}{2}(dut + vs),$$

więc również $2|s$. Stąd w rozkładzie (8) mamy:

$$4|(s^2 + dt^2). \tag{10}$$

W przypadku, gdy liczby u oraz v są nieparzyste, to z (9) wynika, że s oraz t są tej samej parzystości. Gdy są to liczby parzyste, to zachodzi (10), a gdy są to liczby nieparzyste, to z (8) wynika, że również d jest nieparzyste, czyli:

$$2|(v^2 + du^2) \qquad \text{i} \qquad 2|(s^2 + dt^2).$$

[4]W tym miejscu Trost popełnia błąd rozważając tylko układ 6. Co ciekawe właśnie ta opcja nie obejmuje rozważanego poniżej przykładu liczby 493.

Podkreślmy jeszcze, że w przypadku, gdy spełniony jest układ a_1), b_1), c_1) i d_1), to odpowiednio, w zależności od znaku liczby $x_1 - x_2$, dostajemy:

$$x_1 = \frac{1}{2}(dvs \pm ut), \qquad y_1 = \frac{1}{2}(us \mp vt),$$

a rozkład liczby N wygląda następująco:

$$N = \frac{1}{4}(u^2 + dv^2)(t^2 + ds^2).$$

Pora na przykład. Rozważmy liczbę 493, mamy:

$$x_1 = 5, \quad y_1 = 6, \quad d = 13, \quad x_2 = 21, \quad y_2 = 2.$$

Dostajemy układ a_1), b_1), c_1) i d_1), ściślej układ postaci

$$\begin{array}{llll} a_1) & x_1 - x_2 = 16, & b_1) & y_1 - y_2 = 4, \\ c_1) & y_2 + y_1 = 8, & d_1) & x_1 + x_2 = 26 = 13 \cdot 2 \cdot 1, \end{array}$$

skąd wynika, że:

$$u = 4, \quad v = 1, \quad t = 4, \quad s = 2$$

i ostatecznie:

$$493 = \frac{1}{4}(16 + 13)(16 + 52) = 29 \cdot 17.$$

Rozkład liczby 1073 wykonamy następująco. Wiemy, że:

$$1073 = 105 + 2 \cdot 22^2 = 105 \cdot 9 + 2 \cdot 8^2,$$

skąd

$$105 \cdot 8 = 2(22^2 - 8^2),$$

to jest

$$105 = 11^2 - 16.$$

Zatem

$$1073 = 11^2 - 16 + 8 \cdot 11^2 = 9 \cdot 11^2 - 16 = (3 \cdot 11 - 4)(3 \cdot 11 + 4) = 29 \cdot 37.$$

3. Suma więcej niż dwóch kwadratów

Rozważmy jeszcze sytuację, gdy szukamy rozkładu liczby całkowitej nieujemnej na sumę n kwadratów i dopuścimy dodatkowo aby w tym rozkładzie pojawiała się również liczba 0. Możemy wówczas zapytać: *Jaka jest najmniejsza liczba naturalna n, taka że dowolną liczbę całkowitą nieujemną można przedstawić w postaci sumy n kwadratów liczb całkowitych nieujemnych?* Odpowiedzi na to pytanie, jak wynika z przykładów przedstawionych w dziele *Arithemtica*, świadom był już jego autor Diofantos z Aleksandrii (ok. 200/214 n.e. - ok. 284/298 n.e.). Nie sformułował on jednak, ani nie udowodnił odpowiedniego twierdzenia. W 1621 roku francuski matematyk Claude Gaspard Bachet de Méziriac (1581-1638) w swoich notatkach do tłumaczenia na język łaciński dzieła Diofantosa zawarł bez dowodu następujące twierdzenie:

Twierdzenie 7. *Każda liczba całkowita nieujemna jest sumą kwadratów czterech liczb całkowitych nieujemnych.*

Twierdzenie to udowodnił dopiero Joseph Louis Lagrange w 1770 roku. Stąd też, jest współcześnie znane jako *Twierdzenie Lagrange'a o rozkładach liczb naturalnych* lub szerzej pod anglojęzyczną nazwą *Lagrange's four-square theorem.* Co ciekawe pierwszą osobą, która utrzymywała, że udowodniła powyższe twierdzenie był Fermat (zob. [4]). Jednak, jak to miał w zwyczaju, dowodu tego twierdzenia ani nie opublikował ani nie pozostawił w notatkach - to drugie w czasach Fermata było normą. Pełen dowód tego twierdzenia można znaleźć np. w [8,12]. Zauważmy jedynie, że ponieważ prawdziwa jest następująca tożsamość czterech kwadratów Eulera:

$$\begin{aligned}&\left(a^2+b^2+c^2+d^2\right)\left(x^2+y^2+z^2+t^2\right)=\\&\quad=(ax+by+cz+dt)^2+(ay-bx+ct-dz)^2+(az-cx+bt-dy)^2+(at-dx+bz-cy)^2,\end{aligned}\tag{11}$$

gdzie $a,b,c,d,x,y,z,t\in\mathbb{R}$ oraz ponieważ $x^2=(-x)^2$, więc dowód Twierdzenia 7 sprowadza się do udowodnienia następującego lematu:

Lemat 2. *Każda liczba pierwsza jest sumą kwadratów czterech liczb całkowitych.*

W istocie, z tożsamości (11) dostajemy, że iloczyn dwóch liczb, z których każda jest sumą kwadratów czterech liczb całkowitych, jest również taką sumą. Łatwo zauważyć, że tożsamość tę można uogólnić na dowolną liczbę składników. Ponieważ każdą liczbę naturalną większą od 1 można rozłożyć na iloczyn skończonej ilości czynników pierwszych oraz mamy $0=0^2+0^2+0^2+0^2$ i $1=1^2+0^2+0^2+0^2$, więc z Lematu 2 dostajemy tezę Twierdzenia 7.

Wiadomo jednak, że istnieje nieskończenie wiele liczb naturalnych, które nie mogą zostać przedstawione w postaci sumy czterech liczb naturalnych, czyli takich w których rozkładzie na sumę czterech kwadratów liczb całkowitych nieujemnych musi pojawić się również 0. Takimi liczbami są na przykład wszystkie nieparzyste potęgi liczby dwa, [12].

Dla uatrakcyjnienia tego rozdziału proponujemy na jego zakończenie pewien problem natury diofantycznej. Rozpocznijmy od pomocniczego pojęcia.

Definicja 1. *Powiemy, że liczby $m,n\in\mathbb{N}$ są w relacji ρ wtedy i tylko wtedy, gdy $m=n$ lub $m\neq n$ oraz istnieje $k\in\mathbb{N}$, takie, że każdą z tych liczb można zapisać jako sumę tej samej liczby k kwadratów różnych liczb naturalnych i żadnej z liczb m oraz n nie można zapisać jako sumy większej liczby kwadratów różnych liczb naturalnych.*

Łatwo stwierdzamy, że zdefiniowana powyżej relacja ρ jest relacją równoważności, a dla klas abstrakcji względem tej relacji, oznaczenie $[n]_\rho$ dla każdego $n\in\mathbb{N}$, mamy m. in.

$$29\in[14]_\rho,\qquad\text{ale}\qquad 30\notin[14]_\rho.$$

Problem 2. *Czy wszystkie zbiory* $\left[\sum_{k=1}^{n}k^2\right]_\rho$, $n\in\mathbb{N}$ *są skończone?*

4. Uzupełnienia

Aby lepiej naświetlić Problem 1 sformułowany w rozdziale drugim przypomnimy kilka znanych w tym temacie wyników. Rozpoczniemy od klasycznego wyniku.

Twierdzenie 8 (Sierpiński [14]). *Dla każdego $M \in \mathbb{N}$ istnieje $c \in \mathbb{N}$ takie, że ciąg $\{n^2+c\}_{n=1}^{\infty}$ zawiera co najmniej M liczb pierwszych.*

4.1. Wzmocnienie twierdzenia Ageeva

Ageev w pracy [3] wzmocnił powyższe twierdzenie rozważając zbiory $\mathcal{P}_k$ wszystkich liczb pierwszych w ciągach

$$\left\{(2l)^2+(2k-1)^2\right\}_{l=1}^{\infty}$$

dla każdego $k \in \mathbb{N}$.

Twierdzenie 9 (Ageev [3]). *Dla dowolnych $k_0 \in \mathbb{N}$, $M \in (0,\infty)$ oraz $\delta \in [0,1)$ istnieje $k \in \mathbb{N}$, $k \geq k_0$, takie że*

$$|\mathcal{P}_k| > M(2k-1)^{\delta}.$$

Naszym celem będzie uogólnienie tego wyniku. Udowodnimy mianowicie, następujące twierdzenie.

Twierdzenie 10. *Jeśli $\mathcal{K} \subseteq \mathbb{N}$ jest podzbiorem, dla którego mamy:*

$$\sum_{k\in\mathcal{K}}\sum_{p\in\mathcal{P}_k}\frac{1}{p}=\infty, \tag{12}$$

to dla dowolnego $k_0 \in \mathcal{K}$, $M \in (0,\infty)$ oraz $\delta \in [0,1)$ istnieje $k \in \mathcal{K}$, $k \geq k_0$, takie że:

$$|\mathcal{P}_k| > M(2k-1)^{\delta}.$$

Dowód. Oznaczmy przez $\mathcal{P}$ zbiór wszystkich liczb pierwszych postaci $4n+1$, gdzie $n \in \mathbb{N}$. Na mocy twierdzenia Fermata mamy:[5]

$$\mathcal{P} \subsetneq \left\{(2l)^2+(2k-1)^2 : k,l \in \mathbb{N}\right\}. \tag{13}$$

Ponadto zbiory $\mathcal{P}_k$, $k \in \mathbb{N}$, tworzą podział zbioru $\mathcal{P}$. Istotnie, równość $\mathcal{P} = \bigcup_{k\in\mathbb{N}} \mathcal{P}_k$ jest oczywista, natomiast rozłączność zbiorów $\mathcal{P}_k$, $k \in \mathbb{N}$, wynika na podstawie twierdzenia Fermata, z jednoznaczności rozkładu liczb $4n+1$, $n \in \mathbb{N}$, na sumę kwadratów liczb naturalnych postaci $(2l)^2+(2k-1)^2$, $l,k \in \mathbb{N}$. Stąd, dla każdego $k \in \mathbb{N}$ otrzymujemy:

$$\sum_{p\in\mathcal{P}_k}\frac{1}{p} < \sum_{l=1}^{\infty}\frac{1}{4l^2+1} < \infty. \tag{14}$$

[5] Inkluzja (13) jest ostra np. $6^2+3^2 = 45$. Liczba 45 jest najmniejszą liczbą złożoną należącą do zbioru $\left\{(2l)^2+(2k-1)^2 : k,l \in \mathbb{N}\right\}$.

Ustalmy zbiór $\mathcal{K} \subseteq \mathbb{N}$, taki że:

$$\sum_{k\in\mathcal{K}} \sum_{p\in\mathcal{P}_k} \frac{1}{p} = \infty \tag{15}$$

i przypuśćmy, przeciwnie aniżeli w tezie dowodzonego twierdzenia, że istnieją $k_0 \in \mathcal{K}$, $M \in (0,\infty)$ oraz $\delta \in [0,1)$, takie że dla każdego $k \in \mathcal{K}$ jeśli $k \geq k_0$, to

$$|\mathcal{P}_k| \leq M(2k-1)^\delta.$$

Zatem[6]

$$\sum_{k\in\mathcal{K}} \sum_{p\in\mathcal{P}_k} \frac{1}{p} \leq \sum_{\substack{k\in\mathcal{K}\\ k\geq k_0}} \frac{|\mathcal{P}_k|}{4+(2k-1)^2} \leq \sum_{\substack{k\in\mathcal{K}\\ k\geq k_0}} \frac{M(2k-1)^\delta}{4+(2k-1)^2} \leq \sum_{\substack{k\in\mathcal{K}\\ k\geq k_0}} \frac{M}{(2k-1)^{2-\delta}} < \infty, \tag{16}$$

co wobec (14) jest sprzeczne z (15). Otrzymana sprzeczność kończy dowód twierdzenia. □

Przypomnijmy teraz twierdzenie Dirichleta o szeregach liczb pierwszych (zob. [2]).

Twierdzenie 11 (Dirichleta o szeregach liczb pierwszych). *Niech $a, b \in \mathbb{N}$ będą względnie pierwsze. Wówczas zbiór*[7] $\{ak+b : k \in \mathbb{N}\} \cap \mathbb{P}$ *jest nieskończony, natomiast szereg:*

$$\sum_{\substack{ak+b\in\mathbb{P}\\ k\in\mathbb{N}}} \frac{1}{ak+b}$$

jest rozbieżny.

Jeśli $\mathcal{K} = \mathcal{P}$, to na mocy powyższego twierdzenia zachodzi warunek (12) dla $a = 4$ oraz $b = 1$. W konsekwencji z Twierdzenia 10 otrzymujemy Twierdzenie 9 Ageeva.

4.2. Twierdzenie Abela-Sieberta

Istnieje jeszcze jeden typ twierdzeń uogólniających Twierdzenie 8 Sierpińskiego. Przedstawimy jedynie jedno z tego grona wyników, twierdzenie Urlicha Abela i Hartmuta Sieberta [1].

Twierdzenie 12. *Niech $\{a_n\}_{n=1}^\infty$ będzie różnowartościowym ciągiem liczb naturalnych i niech $A(x)$ będzie funkcją zliczającą tego ciągu, to jest:*

$$A(x) := |\{n \in \mathbb{N} : a_n \leq x\}| \qquad \textit{dla } x \in \mathbb{N}.$$

[6]Końcowe oszacowanie w (14) i (16) wynika wprost ze standardowej własności szeregów $\sum_{n=1}^{\infty} \frac{1}{n^s}$, gdzie $s \in \mathbb{R}, s > 0$, a mianowicie, że szeregi te są zbieżne wtedy i tylko wtedy, gdy $s > 1$ (zob. [2]).

[7]Symbolem $\mathbb{P}$ oznaczamy tutaj zbiór wszystkich liczb pierwszych.

Jeśli[8]

$$\limsup_{x\to\infty}\frac{A(x)}{\ln x}=\infty, \tag{17}$$

to dla każdego $N\in\mathbb{N}$ *istnieje liczba naturalna* $c=c(N)$*, taka że w ciągu* $\{a_n+c\}_{n=1}^{\infty}$ *znajduje się co najmniej* N *liczb pierwszych.*
Natomiast, jeśli zachodzi warunek:

$$\limsup_{x\to\infty}\frac{A(2x)-A(x)}{\ln x}=\infty, \tag{18}$$

to dla każdego $N\in\mathbb{N}$ *istnieje liczba naturalna* $d=d(N)$*, taka że w ciągu* $\{a_n-d\}_{n=1}^{\infty}$ *znajduje się co najmniej* N *liczb pierwszych.*

Natychmiastowo otrzymujemy stąd wniosek - uogólnienie Twierdzenia 8.

Wniosek 3. *Niech* P *będzie wielomianem o współczynnikach całkowitych stopnia* $\deg P\geq 1$ *i dodatnim współczynniku przy najwyższej potędze. Wówczas dla każdego* $N\in\mathbb{N}$ *istnieją* $c=c(N)\in\mathbb{N}$ *oraz* $d=d(N)\in\mathbb{N}$*, takie że suma* $P(n)+c$ *jest liczbą pierwszą dla więcej niż* N *liczb naturalnych* n *oraz różnica* $P(n)-d$ *jest liczbą pierwszą dla więcej niż* N *liczb naturalnych* n*.*

Dowód. Z założenia, że $(\deg P)>0$ wynika, że istnieją dodatnie $\beta\in\mathbb{R}$ oraz $n_0\in\mathbb{N}$, dla których:

1. $P|_{[n_0,\infty)}$ jest funkcją rosnącą,
2. $\beta x^{\deg P}\leq P(x+n_0)\leq\frac{3}{2}\beta x^{\deg P}$, dla $x\in\mathbb{R}_+$.

Przyjmując $a_n=P(n+n_0)$, $n\in\mathbb{N}$, potrafimy udowodnić, że

$$\left(\frac{2}{3}\frac{x}{\beta}\right)^{\frac{1}{\deg P}}\leq A(x)\leq\left(\frac{x}{\beta}\right)^{\frac{1}{\deg P}},\qquad\text{dla } x\in\mathbb{N},$$

skąd:

$$\limsup_{x\to\infty}\frac{A(x)}{\ln x}\geq\limsup_{x\to\infty}\frac{\left(\frac{2x}{3\beta}\right)^{\frac{1}{\deg P}}}{\ln x}=\infty$$

oraz

$$\limsup_{x\to\infty}\frac{A(2x)-A(x)}{\ln x}\geq\limsup_{x\to\infty}\frac{\left(\frac{4x}{3\beta}\right)^{\frac{1}{\deg P}}-\left(\frac{x}{\beta}\right)^{\frac{1}{\deg P}}}{\ln x}=\limsup_{x\to\infty}\frac{\left(\left(\frac{4}{3}\right)^{\frac{1}{\deg P}}-1\right)\left(\frac{x}{\beta}\right)^{\frac{1}{\deg P}}}{\ln x}=\infty,$$

co oznacza, że tak określony ciąg $\{a_n\}_{n=1}^{\infty}$ spełnia warunki (17) oraz (18) twierdzenia 12 i w konsekwencji kończy dowód wniosku 3. □

[8]Przypomnijmy pojęcie granicy górnej danego ciągu liczb rzeczywistych, oznaczenie $\limsup_{n\to\infty}a_n$ lub $\overline{\lim_{n\to\infty}}a_n$. Przyjmujemy:

$$\limsup_{n\to\infty}a_n=\begin{cases}\infty, & \text{gdy ciąg } \{a_n\}_{n=1}^{\infty} \text{ nie jest ograniczony z góry,}\\ -\infty, & \text{gdy } \lim_{n\to\infty}a_n=-\infty,\\ G\in\mathbb{R}, & \text{gdy ciag } \{a_n\}_{n=1}^{\infty} \text{ jest ograniczony z góry, posiada podciąg zbieżny w } \mathbb{R} \text{ a w zbiorze } \mathcal{G}\\ & \text{granic wszystkich podciągów zbieżnych ciągu } \{a_n\}_{n=1}^{\infty} \text{ liczba } G \text{ jest liczbą największą.}\\ & \text{Istnienie takiej liczby największej wynika stąd, że } \sup\mathcal{G}\in\mathcal{G} \text{ - co jednak wymaga oddzielnego}\\ & \text{dowodu. Oczywiście mamy } G=\sup\mathcal{G}.\end{cases}$$

Uwaga 4. Ani warunku (17), ani warunku (18), nie spełniają elementy szybko rosnących[9] liniowych ciągów rekurencyjnych liczb naturalnych $\{r_n\}_{n=1}^{\infty}$ albowiem, jak wynika z jawnej postaci wzoru opisującego elementy takich ciągów (chodzi o wzór Bineta, zob. [5]), istnieją $\alpha \in \mathbb{C}$, $|\alpha| > 1$ oraz wielomian β zmiennej n o współczynnikach zespolonych, takie że:

$$r_n \sim \beta \cdot \alpha^n \qquad \text{gdy } n \to \infty,$$

to znaczy, że $\lim\limits_{n\to\infty} \frac{r_n}{\beta\cdot\alpha^n} = 1$. Dla przykładu, jeśli $\{F_n\}_{n=1}^{\infty}$ jest ciągiem liczb Fibonacciego, to:

$$F_n \sim \frac{1}{\sqrt{5}}\varphi^n \qquad \text{gdy } n \to \infty,$$

natomiast dla liczb Lucasa L_n, $n \in \mathbb{N}$, zachodzi:

$$L_n \sim \varphi^n \qquad \text{gdy } n \to \infty.$$

Stąd otrzymujemy kolejne naturalne pytanie:

Problem 3. *Czy dla każdego $N \in \mathbb{N}$ istnieją $c = c(N), d = d(N) \in \mathbb{N}$, takie że każdy z ciągów $\{F_n+c\}_{n=1}^{\infty}$ oraz $\{F_n - d\}_{n=1}^{\infty}$ zawiera co najmniej N liczb pierwszych?*

Analogiczne pytanie nasuwa się, gdy rozważamy ciągi $\{r_n + c\}_{n=1}^{\infty}$ oraz $\{r_n - d\}_{n=1}^{\infty}$, gdzie $\{r_n\}_{n=1}^{\infty}$ jest rosnącym ciągiem rekurencyjnym liniowym liczb naturalnych.

Uwaga 5. Twierdzenia typu Twierdzenie 12 znajdziemy też w pracy Formana [6].

Podziękowania

Autorzy pracy wyrażają głęboką wdzięczność jej Recenzentowi za wnikliwe uwagi i cenne sugestie. Z całą pewnością pozwoliło to nadać pracy lepszą, ale i jeszcze ciekawszą formę.

Literatura

1. U. Abel, H. Siebert, *Sequences with large numbers of prime values*, Amer. Math. Monthly 100 (1993), pp. 167–169.
2. M. Adam i in., *Szeregi liczbowe w analizie matematycznej i w teorii liczb.*, Wyd. Pol. Śl., Gliwice 2021.
3. A.A. Ageev, *Sierpinski's Theorem is Deducible from Euler and Dirichlet*, Amer. Math. Monthly 101 (1994), pp. 659–660.
4. J. Boucard, *Lagrange and the four-square theorem*, Lett. Mat. Int. 2 (2014), pp. 59–66.
5. S. Elaydi, *An Introduction to Difference Equations*, Springer, 2005.

[9]Powiemy, że ciąg $\{r_n\}_{n=1}^{\infty} \subset \mathbb{N}$ jest szybko rosnący jeśli jest rosnący oraz istnieje $\beta > 0$ takie, że $\frac{r_{n+1}}{r_n} > 1 + \beta$ dla dostatecznie dużych $n \in \mathbb{N}$.

6. R. Forman, *Sequences with Many Primes*, Amer. Math. Monthly 99 (1992), pp. 548–557.
7. P. Hajłasz, *Charakterystyka Eulera, czyli jak się uczesać* - rozdział w książce Bartol W., Sadowski W. (red.), *O twierdzeniach i hipotezach: matematyka według Delty*, Wyd. Uniwersytetu Warszawskiego, Warszawa 2016.
8. G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1980.
9. M.M. Marjanović, *Euler-Poincaré characteristic - a case of topological self-convincing*, The Teaching of Math. 17 No. 1 (2014), pp. 21–33.
10. R.A. Mollin, *Fundamental Number Theory with Applications*, Chapman & Hall/ CRC, Boca Raton 2008.
11. W. Sadowski, *Wzór Eulera i balony*, Delta, wrzesień 2005.
12. W. Sierpiński, *Arytmetyka Teoretyczna*, PWN, Warszawa 1959.
13. W. Sierpiński, *Co wiemy, a czego nie wiemy o liczbach pierwszych*, PZWS, Warszawa 1961.
14. W. Sierpiński, *Les binômes $x^2 + n$ et les nombres premiers*, Bull. Soc., Royale Sciences, Liege 33 (1964), pp. 259–260.
15. J.A. Szaszkin, *Euler Characteristic*, Moskwa 1984 (dostępna jest oryginalna wersja książki po rosyjsku i jej tłumaczenie na język angielski).
16. E. Trost, *Primzahlen*, Birkhäuser, Basel 1953.
17. V.S. Varadajan, *Euler Through Time: A New Look at Old Times*, AMS, 2006.
18. D. Zagier, *A one-sentence proof that every prime $p \equiv 1$ (mod 4) is a sum of two squares*, Amer. Math. Monthly 97 No 2 (1990), pp. 144.