FOLIA 65

Annales Universitatis Paedagogicae Cracoviensis
Studia ad Didacticam Mathematicae Pertinentia II (2009)

Jan Górowski, Adam Łomnicki

O nieskończonych ciągach liczb naturalnych, parami względnie pierwszych

Abstract. In the first part of the paper the authors, using general formulas, determine and describe a class of infinite series of natural numbers pairs of which are relatively prime. The second part of the paper contains – as a proposition – a set of problems concerning prime numbers and pairs of relatively prime numbers suggested for use during the process of work with Mathematics students, as well as some didactic comments concerning these problems.

W procesie kształcenia nauczycieli matematyki w Polsce teoria liczb wraca do łask. Ponad 30 lat temu, na nauczycielskich studiach matematycznych przedmiot „Arytmetyka teoretyczna" został wchłonięty przez przedmiot „Algebra ogólna" (nazywany też „Algebrą abstrakcyjną" czy krócej – „Algebrą") i w konsekwencji wiedza z teorii liczb w nim zawarta była zmarginalizowana. Absolwenci studiów matematycznych dopiero w czasie pracy w szkołach podstawowych i średnich starali się uzupełniać swoje wykształcenie z tego działu matematyki na podstawie literatury popularnonaukowej (z lat 1950-1970, Sierpiński, 1959a; Sierpiński, 1959b; Sierpiński, 1964). Obecnie znajdujemy elementy teorii liczb wśród standardów nauczania na kierunku matematyka oraz w programach nauczania przedmiotu „Algebra z teorią liczb". Pojawiło się kilka pięknie napisanych książek o tematyce związanej z teorią liczb (Ribenboim, 1997; Yan, 2006; Marzantowicz, Zarzycki, 2006; Graham, Knuth, Patashnik, 2002).

Song Y. Yan podkreślał w 2000 roku:

> Obecnie teoria liczb znajduje zastosowania w tak odległych dziedzinach, jak fizyka, chemia, akustyka, biologia, informatyka, kryptografia, transmisja cyfrowa, a nawet muzyka i biznes.
>
> (Yan, 2006, s. XII)

Martin E. Hellman pisał w 2001 roku we wstępie do książki Song Y. Yana (Yan, 2006, s. IX):

> To było bardzo satysfakcjonujące obserwować, jak w ciągu ostatnich dwudziestu pięciu lat kryptografia i teoria liczb wpływały na siebie. Teoria liczb stała się źródłem wielu błyskotliwych pomysłów stosowanych

> w systemach kryptograficznych i protokołach, a kryptografia z kolei okazała się pomocna w zdobywaniu funduszy na badania w teorii liczb nazywanej często „królową matematyki" bez zastosowań w rzeczywistości. Jak bardzo mało wiedzieli ci, którzy tak myśleli!

Wacław Marzantowicz i Piotr Zarzycki uważają, że:

> Teoria liczb, jedna z dwóch (obok geometrii) najstarszych dziedzin matematyki, to ogromny, budowany od ponad dwóch tysięcy lat dział matematyki, pełen pięknych rezultatów i różnorodnych metod.
>
> (Marzantowicz, Zarzycki, 2006)

To spojrzenie na teorię liczb jest dla dydaktyków matematyki niemniej ważne od uznawania wagi jej zastosowań. Przed dydaktykami matematyki stoi zadanie wykorzystania zmian w standardach nauczania dla ulepszenia procesu kształcenia nauczycieli matematyki. Wyróżnić należy te treści (rezultaty i metody), które są nauczane lub stanowić mogłyby horyzont dla matematyki nauczanej w szkołach niższych szczebli, zaproponować ich ujęcie w formie sprzyjającej aktywizowaniu studiujących, jak też ułatwiającej wyzwalanie różnych aktywności matematycznych.

W pierwszej części artykułu przedstawiamy kilka uzyskanych przez nas twierdzeń o nieskończonych ciągach liczb naturalnych, parami względnie pierwszych. Chcemy w ten sposób pokazać, że klasyczny, znany od setek lat materiał może być źródłem wyzwalającym twórczość matematyczną na poziomie dostępnym dla uzdolnionych matematycznie absolwentów szkół średnich. Poznawanie i obserwacje znanych od lat zależności, analiza różnych dowodów znanych twierdzeń prowadzić może do poszukiwań podobnych zależności, do stawiania hipotez, prób ich weryfikacji, do poszukiwania dowodów.

W drugiej części artykułu zamieszczamy propozycję serii zadań opracowanych do zajęć ze studentami matematyki na temat liczb pierwszych i liczb parami względnie pierwszych. Wykorzystujemy pomysły zadań problemowych, które układaliśmy, pisząc skrypt *Arytmetyka i algebra* na początku lat 90. dla studentów Kolegiów Nauczycielskich (Górowski, Łomnicki, 1993), jak również zadań, które egzemplifikują rezultaty z części pierwszej tego artykułu.

1. Nieskończone ciągi liczb naturalnych, parami względnie pierwszych

Bardzo znanym nieskończonym ciągiem liczb naturalnych, parami względnie pierwszych, który można określić wzorem, jest ciąg (F_n) liczb Fermata[1]. O liczbach Fermata, czyli o liczbach postaci $F_n = 2^{2^n} + 1$, gdzie $n \in \mathbb{N}$ wiadomo i dużo, i mało, np. F_0, F_1, F_2, F_3, F_4 są liczbami pierwszymi, F_5 jest liczbą złożoną, podzielną przez 641, liczby pierwsze Fermata występują w twierdzeniu Gaussa o konstruowalności n-kąta foremnego. Nie wiemy natomiast, ile jest

[1]Dowód tego faktu można znaleźć m.in. w książce (Sierpiński, 1969, s. 87).

liczb pierwszych wśród wyrazów ciągu (F_n) (zob. Yan, 2006, s. 35; Narkiewicz, 2003, s. 16).

Oczywiście każdy nieskończony podciąg ciągu kolejnych liczb pierwszych (lub potęg kolejnych liczb pierwszych) jest nieskończonym ciągiem liczb naturalnych, parami względnie pierwszych. „Mankamentem" tego ciągu jest to, że nie można podać wzoru na jego n-ty wyraz oraz, iż wcześniej trzeba wiedzieć, że liczb pierwszych jest nieskończenie wiele.

Paulo Ribenboim (Ribenboim, 1997, s. 22), omawiając różne dowody twierdzenia mówiącego, że liczb pierwszych jest nieskończenie wiele, podaje m.in. następujące rozumowanie: *wystarczy znaleźć ciąg (a_n) liczb naturalnych większych od 1, które są parami względnie pierwsze; symbolem q_i oznaczmy dzielnik pierwszy liczby a_i; oczywiście ciąg (q_i) jest nieskończonym i różnowartościowym ciągiem liczb pierwszych; to dowodzi, że liczb pierwszych jest nieskończenie wiele.*

Ribenboim podaje przykład ciągu liczb parami względnie pierwszych, określonego rekurencyjnie i zauważa:

> Chciałoby się znaleźć inne ciągi nieskończone o wyrazach parami względnie pierwszych, nie zakładając istnienia nieskończenie wielu liczb pierwszych.
>
> (Ribenboim, 1997, s. 23)

Referuje wyniki uzyskane na ten temat, podaje przykłady takich ciągów, są one jednak zawsze określone rekurencyjnie (zob. Edwards, 1964).

W tej części artykułu podejmujemy próbę opisania pewnej klasy ciągów nieskończonych o wyrazach parami względnie pierwszych, określonych wzorami ogólnymi (tak, jak ciąg liczb Fermata), które udało się nam uzyskać.

Będziemy dalej mówili krótko, że **nieskończony ciąg liczb naturalnych ma własność *wp*, gdy każde dwa jego różne wyrazy są liczbami względnie pierwszymi**.

Wymieniony powyżej ciąg (F_n) ma własność *wp* i dodatkowo można go określić wzorem.

Oczywiście ciąg (a_n) taki, że $a_n = 3^{2^n} + 1$ dla $n \in \mathbb{N}$ (i ogólnie $a_n = b^{c^n} + 1$ dla $n \in \mathbb{N}$, gdzie b jest ustaloną liczbą naturalną nieparzystą, a c ustaloną liczbą naturalną dodatnią), jest ciągiem o wyrazach parzystych, a więc nie ma własności *wp*.

Rozważmy teraz ciąg (c_n) taki, że $c_n = 6^{2^n} + 1$ dla $n \in \mathbb{N}$. Wyrazy tego ciągu są liczbami nieparzystymi (bo dodatnia potęga szóstki jest liczbą parzystą). Przypuśćmy, że ciąg (c_n) nie ma własności *wp*, czyli $\mathrm{NWD}(c_n, c_m) \neq 1$ dla pewnych $n, m \in \mathbb{N}$ takich, że $m > n$. Stąd dla pewnych $\alpha_n, \alpha_m \in \mathbb{N} \setminus \{0\}$ oraz pewnej nieparzystej liczby pierwszej q mamy:

$$6^{2^n} + 1 = q\alpha_n \quad \text{oraz} \quad 6^{2^m} + 1 = q\alpha_m,$$

$$\begin{aligned} 6^{2^m}+1 &= \left(6^{2^n}\right)^{2^{m-n}}+1 \\ &= (q\alpha_n-1)^{2^{m-n}}+1 \\ &= \sum_{k=0}^{2^{m-n}} \binom{2^{m-n}}{k} (q\alpha_n)^k (-1)^{2^{m-n}-k}+1 \\ &= \sum_{k=1}^{2^{m-n}} \binom{2^{m-n}}{k} (q\alpha_n)^k (-1)^{2^{m-n}-k}+2. \end{aligned}$$

Otrzymana suma w dzieleniu przez q daje resztę 2, gdyż jej składnik

$$\sum_{k=1}^{2^{m-n}} \binom{2^{m-n}}{k} (q\alpha_n)^k (-1)^{2^{m-n}-k}$$

jest podzielny przez q. Otrzymaliśmy sprzeczność z tym, że $6^{2^m}+1$ jest podzielne przez nieparzystą liczbę pierwszą q.

Udowodniliśmy zatem

Twierdzenie 1
Ciąg (c_n) określony wzorem $c_n = 6^{2^n}+1$ dla $n \in \mathbb{N}$ ma własność wp.

Zauważmy, że prowadząc analogiczne rozumowanie, można udowodnić ogólniejsze

Twierdzenie 2
Ciąg (a_n) określony wzorem $a_n = a^{s^n}+1$, gdzie a oraz s są ustalonymi liczbami parzystymi dodatnimi, ma własność wp.

Warto odnotować, że występujące w twierdzeniu 2 założenie parzystości liczby s jest istotne. Np. kolejnymi wyrazami ciągu (e_n), takiego że $e_n = 2^{3^n}+1$ dla $n \in \mathbb{N}$ są $3, 9, 513$, a więc ciąg ten nie ma własności *wp* (ponieważ np. $\mathrm{NWD}(9, 513) \neq 1$).

Od tego miejsca literą $\mathbb{P}$ oznaczać będziemy zbiór liczb pierwszych. Analiza przeprowadzonego dowodu twierdzenia 1 podpowiada następujące

Twierdzenie 3
Jeżeli $p \in \mathbb{P}\setminus\{2\}$, to ciąg (a_n) określony wzorem $a_n = \frac{1}{2}(p^{2^n}+1)$ dla $n \in \mathbb{N}\setminus\{0\}$ ma własność wp.

Dowód. Najpierw pokażemy – na dwa sposoby – że wyrazy ciągu (a_n) są liczbami nieparzystymi.

I sposób:

Symbolem $cjlx$ oznaczmy cyfrę jedności liczby naturalnej x, zapisanej w systemie dziesiątkowym. Poniższa tabela może stanowić źródło wiadomości o cyfrach jedności wielu liczb naturalnych.

$cjln$	0	1	2	3	4	5	6	7	8	9
$cjln^2$	0	1	4	9	6	5	6	9	4	1
$cjln^3$	0	1	8	7	4	5	6	3	2	9
$cjln^4$	0	1	6	1	6	5	6	1	6	1
$cjln^5$	0	1	2	3	4	5	6	7	8	9

Łatwo zauważyć, że $cjln^4 = cjln^{4k}$ dla $n \in \mathbb{N}$ i $k \in \mathbb{N} \setminus \{0\}$.

Symbolem $\mathbb{N}_r$ oznaczać będziemy zbiór liczb naturalnych większych lub równych r. Ustalmy dowolnie liczbę pierwszą p, większą od 2. Zatem p nie jest parzysta, a więc jej cyfrą jedności jest 1 lub 3, lub 5, lub 7, lub 9. Stąd i z faktu, że 2^n dla $n \in \mathbb{N}_2$ jest liczbą podzielną przez 4, otrzymujemy iż $cjlp^{2^n}$ jest 1 lub 5 dla $n \in \mathbb{N}_2$ i z kolei $cjl(p^{2^n}+1)$ jest 2 lub 6. Dla rozstrzygnięcia jaka jest $cjl\frac{1}{2}(p^{2^n}+1)$ wystarczy zauważyć, że cyfra dziesiątek liczby p^{2^n} jest zawsze parzysta (istotnie: p^{2^n} jest liczbą kwadratową nieparzystą, a liczba kwadratowa nieparzysta w dzieleniu przez 4 daje resztę 1, a więc jej cyfra dziesiątek jest parzysta). Stąd, uwzględniając przypadek $n = 1$, otrzymujemy, że wszystkie wyrazy ciągu (a_n) mają cyfrę jedności 1 lub 3, lub 5.

II sposób (uzasadnienia, że wyrazy ciągu (a_n) są liczbami nieparzystymi):

Wykorzystując wzór Newtona, mamy:

$$\begin{aligned}\frac{1}{2}\left(p^{2^n}+1\right) &= \frac{1}{2}\left[((p-1)+1)^{2^n}+1\right] \\ &= \frac{1}{2}\left[\sum_{k=0}^{2^n}\binom{2^n}{k}(p-1)^k+1\right] \\ &= \frac{1}{2}\left[\sum_{k=1}^{2^n}\binom{2^n}{k}(p-1)^k+2\right] \\ &= \frac{1}{2}\sum_{k=1}^{2^n}\binom{2^n}{k}(p-1)^k+1.\end{aligned}$$

Zauważmy, że dla $n \in \mathbb{N} \setminus \{0\}$ i $p \in \mathbb{P} \setminus \{2\}$ liczba $\frac{1}{2}\sum_{k=1}^{2^n}\binom{2^n}{k}(p-1)^k$ jest parzysta, a więc liczba $\frac{1}{2}(p^{2^n}+1)$ jest nieparzysta.

Pokażemy teraz, że $\mathrm{NWD}(a_n, a_m) = 1$ dla $n, m \in \mathbb{N} \setminus \{0\}$ i $n \neq m$. Przypuśćmy, że tak nie jest, tzn. $\mathrm{NWD}(a_n, a_m) > 1$ dla pewnych $n, m \in \mathbb{N} \setminus \{0\}$ i takich, że $n < m$. Stąd wynika, że znajdzie się liczba pierwsza q, taka że $q|a_n$ i $q|a_m$. Ponadto z pierwszej części przeprowadzonego dowodu wynika, że q jest

liczbą nieparzystą. Mamy zatem $\frac{1}{2}(p^{2^n}+1) = q\alpha_n$, $\frac{1}{2}(p^{2^m}+1) = q\alpha_m$, gdzie α_n, α_m są pewnymi liczbami naturalnymi. Stąd

$$p^{2^n}+1 = 2q\alpha_n, \quad p^{2^m}+1 = 2q\alpha_m,$$

$$\begin{aligned} p^{2^m}+1 &= (p^{2^n})^{2^{m-n}}+1 \\ &= (2q\alpha_n - 1)^{2^{m-n}}+1 \\ &= \sum_{k=0}^{2^{m-n}} \binom{2^{m-n}}{k} (2q\alpha_n)^k (-1)^{2^{m-n}-k} + 1 \\ &= \sum_{k=1}^{2^{m-n}} \binom{2^{m-n}}{k} (2q\alpha_n)^k (-1)^{2^{m-n}-k} + 2, \end{aligned}$$

a więc resztą z dzielenia liczby $p^{2^m}+1$ przez q jest 2, co przeczy równości $p^{2^m}+1 = 2q\alpha_m$. Zatem $\mathrm{NWD}(a_n, a_m) = 1$ dla każdych $n, m \in \mathbb{N}\setminus\{0\}$ i $n \neq m$. Twierdzenie 3 zostało tym samym udowodnione.

Symbolem $\triangle_{(a_n)}$ będziemy w dalszym tekście oznaczać zbiór wartości ciągu (a_n).
Związek między ciągami określonymi jak w twierdzeniu 3 ujmuje (łatwe do udowodnienia)

Twierdzenie 4
Jeśli $a_n = \frac{1}{2}(p^{2^n}+1)$ *dla* $n \in \mathbb{N}\setminus\{0\}$, $b_n = \frac{1}{2}(q^{2^n}+1)$ *dla* $n \in \mathbb{N}\setminus\{0\}$, *gdzie* $p \neq q$ *i* $p, q \in \mathbb{P}\setminus\{2\}$, *to* $\triangle_{(a_n)} \cap \triangle_{(b_n)} = \emptyset$.

Prawdziwe jest twierdzenie ogólniejsze od twierdzenia 3, a mianowicie

Twierdzenie 5
Jeśli m *jest liczbą nieparzystą większą od* 1, *a* s *jest liczbą parzystą dodatnią, to ciąg* (c_n) *określony wzorem* $c_n = \frac{1}{2}(m^{s^n}+1)$ *dla* $n \in \mathbb{N}\setminus\{0\}$ *ma własność wp.*

Dowód tego twierdzenia niczym nie różni się od dowodu twierdzenia 3 (sposób II). Wystarczy w dowodzie twierdzenia 3 liczbę pierwszą p zastąpić liczbą nieparzystą m, większą od 1, a liczbę 2 liczbą parzystą s.

Zauważmy też, że prawdziwe jest ogólniejsze od twierdzenia 4

Twierdzenie 6
Jeśli $c_n = \frac{1}{2}(m^{s^n}+1)$ *dla* $n \in \mathbb{N}\setminus\{0\}$, $d_n = \frac{1}{2}(r^{t^n}+1)$ *dla* $n \in \mathbb{N}\setminus\{0\}$, *gdzie* m, r *są liczbami nieparzystymi większymi od* 1 *takimi, że* $NWD(m, r) = 1$, *zaś* s, t *– liczbami parzystymi dodatnimi, to* $\triangle_{(c_n)} \cap \triangle_{(d_n)} = \emptyset$.

Pozostaje otwarty problem — ile jest liczb pierwszych wśród wyrazów określonych w tym artykule nieskończonych ciągów liczb naturalnych, parami względnie pierwszych?

2. Materiały do zajęć ze studentami matematyki na temat liczb pierwszych i liczb parami względnie pierwszych (w ramach przedmiotu „Algebra z teorią liczb")

Poniżej przedstawiamy zestaw 9 zadań na ćwiczenia z przedmiotu „Algebra z teorią liczb" dla studentów matematyki (głównie z myślą o studentach kierunków nauczycielskich). Celem tych zajęć jest ugruntowanie i pogłębienie wiadomości studiujących o liczbach pierwszych i liczbach względnie pierwszych, jak również pogłębienie umiejętności analizowania tekstu matematycznego, prowadzenia rozumowań, stworzenie sytuacji do stawiania hipotez, uogólniania twierdzeń, rozumowania przez analogię. Staramy się na przykładzie proponowanych zajęć potwierdzić opinie dydaktyków matematyki, którzy uważają, że rozwijanie różnych aktywności matematycznych jest ważniejsze od przekazywania przyszłym nauczycielom matematyki obszernych porcji wiadomości „gotowej" matematyki.

Zadanie 1
a) Przypomnieć definicje – liczby pierwszej i liczby złożonej, a następnie zilustrować je przykładami.
b) Czy liczba 0 *jest pierwsza (złożona)?*
c) Czy liczba 1 *jest pierwsza (złożona)?*
d) Zbadać, która z liczb 251, 112351467, $641 \cdot 113$, $7777 + 21 \cdot 2008$ *jest pierwsza, a która złożona.*
e) Zaproponować plan badania, czy liczba $2^{2^5} + 1$ *jest pierwsza. Wyjaśnić, jakie mogłyby zaistnieć trudności przy realizacji tego planu.*
f) Uzasadnić, że następująca wypowiedź nie może być przyjęta za definicję liczby pierwszej: „Liczbą pierwszą nazywamy liczbę naturalną, która jest podzielna tylko przez 1 *i przez samą siebie".*

Zadanie 2 (wg Górowski, Łomnicki, 1993)
a) Sprawdzić, że są liczbami pierwszymi sumy:
$2 + 1$,
$2 \cdot 3 + 1$,
$2 \cdot 3 \cdot 5 + 1$,
$2 \cdot 3 \cdot 5 \cdot 7 + 1$.
b) Jak powstały te liczby? Określić kolejne liczby według tej zasady.
c) Zasadę odkrytą w rozwiązaniu zadania b), oznaczmy ją przez (Z), można sformułować tak:
wyraz a_s, *gdzie* $s \in \mathbb{N} \setminus \{0\}$, *tworzonego ciągu otrzymujemy, zwiększając iloczyn kolejnych* s *liczb pierwszych (poczynając od liczby* 2*) o* 1.

Uzasadnić, że prawdziwe jest zdanie:
jeśli tworzone według zasady (Z) liczby są zawsze pierwsze, to liczb pierwszych jest nieskończenie wiele.

Uzasadnić też, że ze zdania tego nie wynika, że liczb pierwszych jest nieskończenie wiele.
d) Uzasadnić, że $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1$ *nie jest liczbą pierwszą.*

Zadanie 3
Od 2000 lat wiadomo, że liczb pierwszych jest nieskończenie wiele.
a) Uzupełnić luki w następującym rozumowaniu (tzw. dowodzie Euklidesa).

Przypuśćmy, że $p_1, p_2, \ldots, p_r$, *gdzie* $p_1 = 2 < p_2 = 3 < p_3 < \ldots < p_r$, *są wszystkimi liczbami pierwszymi. Utwórzmy liczbę* $p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$. *Literą* p *oznaczmy jeden z dzielników liczby* $p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$ *będący liczbą pierwszą. Stąd* p *jest jedną z liczb* $p_1, p_2, \ldots, p_r$, *zatem* $p | p_1 \cdot p_2 \cdot \ldots \cdot p_r$, *a skoro* $p | p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$, *więc* $p | 1$. *Otrzymaliśmy sprzeczność. Liczb pierwszych jest zatem nieskończenie wiele.*
b) Udowodnić twierdzenie:

$$\forall_{a,b,c \in \mathbb{Z}} \; a | (b + c) \Longrightarrow (a | b \Leftrightarrow a | c).$$

Jaki jest związek tego twierdzenia z dowodem podanym w zadaniu a)?

Zadanie 4
a) Przypomnieć definicję liczb względnie pierwszych, a następnie zilustrować ją przykładami.
b) Zaproponować definicję ciągu skończonego liczb parami względnie pierwszych, a następnie zilustrować ją przykładami.
c) Zaproponować definicję ciągu nieskończonego liczb parami względnie pierwszych, a następnie zilustrować ją przykładami.
d) Uzasadnić, że ciąg (a_n) *określony wzorem* $a_n = n!$ *dla* $n \in \mathbb{N} \setminus \{0\}$ *nie jest nieskończonym ciągiem liczb parami względnie pierwszych?*
e) Podać przykłady ciągów nieskończonych, które nie są ciągami liczb parami względnie pierwszych. Które z tych ciągów są określone rekurencyjnie, a które wzorami ogólnymi?

Zadanie 5 (wg Ribenboim, 1997; Graham, Knuth, Patashnik, 2002)
Rozważmy ciąg (w_n) *określony rekurencyjnie:* $w_1 = 2$, $w_{n+1} = w_1 \cdot w_2 \cdot \ldots \cdot w_n + 1$ *dla* $n \geqslant 1$.
a) Wymienić sześć początkowych wyrazów ciągu (w_n).
b) Czy wszystkie wyrazy ciągu (w_n) *są liczbami pierwszymi?*
c) Uzasadnić, że (w_n) *jest nieskończonym ciągiem liczb parami względnie pierwszych, uzupełniając luki w następującym rozumowaniu:*

Dla dowolnie ustalonych liczb $n, m \in \mathbb{N} \setminus \{0\}$ *takich, że* $n < m$, *mamy:*

$$NWD(w_n, w_m) = NWD(w_n, aw_n + 1) \text{ dla pewnego } a \in \mathbb{N} \setminus \{0\}$$

i dalej

$$NWD(w_n, aw_n + 1) = NWD(w_n, 1).$$

Zatem $NWD(w_n, w_m) = 1$.

ZADANIE 6

Liczby postaci $2^{2^n}+1$, *gdzie* $n \in \mathbb{N}$, *nazywamy liczbami Fermata. Przyjmujemy oznaczenie* $F_n = 2^{2^n} + 1$, *gdzie* $n \in \mathbb{N}$.

a) Dlaczego zbadanie, czy ciąg (F_n) *jest ciągiem liczb pierwszych, jest zadaniem trudnym?*

b) Uzasadnić, że ciąg (F_n) *jest nieskończonym ciągiem liczb parami względnie pierwszych, uzupełniając luki w następującym rozumowaniu:*

Oczywiście każda liczba Fermata jest nieparzysta. Przypuśćmy, że $NWD(F_m, F_n) \neq 1$ *dla pewnych* $m, n \in \mathbb{N}$ *takich, że* $m > n$. *Stąd dla pewnych* $\alpha_n, \alpha_m \in \mathbb{N}$ *oraz pewnej nieparzystej liczby pierwszej* q *mamy:* $2^{2^n} + 1 = q\alpha_n$ *oraz* $2^{2^m} + 1 = q\alpha_m$,

$$\begin{aligned} 2^{2^m} + 1 &= \left(2^{2^n}\right)^{2^{m-n}} + 1 \\ &= (q\alpha_n - 1)^{2^{m-n}} + 1 \\ &= \sum_{k=0}^{2^{m-n}} \binom{2^{m-n}}{k} (q\alpha_n)^k (-1)^{2^{m-n}-k} + 1 \\ &= \sum_{k=1}^{2^{m-n}} \binom{2^{m-n}}{k} (q\alpha_n)^k (-1)^{2^{m-n}-k} + 2. \end{aligned}$$

Otrzymana suma w dzieleniu przez q *daje resztę 2, gdyż jej składnik*

$$\sum_{k=1}^{2^{m-n}} \binom{2^{m-n}}{k} (q\alpha_n)^k (-1)^{2^{m-n}-k}$$

jest podzielny przez q. *Otrzymaliśmy sprzeczność z tym, że* $2^{2^m} + 1$ *jest podzielne przez nieparzystą liczbę pierwszą* q.

c) W 1640 roku w liście do Mersenne'a Fermat postawił hipotezę, że wszystkie liczby F_n *są pierwsze, chociaż sprawdził to tylko dla* $n = 0, 1, 2, 3, 4$. *W 1732 roku Euler wykazał, że liczba* F_5 *nie jest pierwsza, jest podzielna przez* 641. *Czy, używając kalkulatora, można sprawdzić, że* $641|F_5$? *Uzasadnić każdy krok w następującym dowodzie tego, że liczba* F_5 *jest złożona.*

Oczywiście $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$. *Zatem* $641|(5^4 + 2^4) \cdot 2^{28}$ *oraz* $641|(5 \cdot 2^7)^4 - 1$, *czyli* $641|5^4 \cdot 2^{28} + 2^{32}$ *oraz* $641|5^4 \cdot 2^{28} - 1$, *a więc* $641|[(5^4 \cdot 2^{28} + 2^{32} - (5^4 \cdot 2^{28} - 1)]$. *Stąd* $641|2^{32} + 1$.

d) (wg Graham, Knuth, Patashnik, 2002, s. 157)
Wniosek, że F_5 nie jest liczbą pierwszą, można wyciągnąć z twierdzenia Fermata (które mówi, że $n^{p-1} \equiv 1 (mod\, p)$, jeśli p jest liczbą pierwszą oraz $NWD(n, p) = 1$). Przypuśćmy, że F_5 jest liczbą pierwszą.
Uzasadnić, że wtedy $3^{2^{32}} \equiv 3029026160 (mod\, F_5)$, a więc że uzyskujemy sprzeczność.

Zadanie 7
Rozwiązując zadanie 6, poznaliśmy ciąg (F_n) liczb Fermata, nieskończony ciąg liczb parami względnie pierwszych.
a) Zbadać, czy ciąg (a_n), taki że $a_n = 3^{2^n} + 1$ dla $n \in \mathbb{N}$, jest ciągiem liczb parami względnie pierwszych.
b) Rozważmy ciąg (c_n), taki że $c_n = 6^{2^n} + 1$ dla $n \in \mathbb{N}$. Uzasadnić, że (c_n) jest ciągiem liczb parami względnie pierwszych, prowadząc rozumowanie podobne do dowodu tego, że ciąg (F_n) liczb Fermata jest ciągiem liczb parami względnie pierwszych.
c) Sformułować i rozwiązać zadanie analogiczne do zadania b).
d) Czy prawdziwa jest hipoteza:

> *Ciąg (d_n) określony wzorem $d_n = a^{s^n} + 1$, gdzie a jest ustaloną liczbą naturalną parzystą dodatnią, a s – ustaloną liczbą naturalną dodatnią, jest nieskończonym ciągiem liczb względnie pierwszych?*

e) Jak wzmocnić założenia podane w hipotezie postawionej w zadaniu d), by uzyskać twierdzenie ogólniejsze od twierdzenia „ukrytego" w zadaniu b)? Sformułować i udowodnić to twierdzenie.

Zadanie 8
Rozważmy ciąg (a_n) określony wzorem $a_n = \frac{1}{2}\left(p^{2^n} + 1\right)$ dla $n \in \mathbb{N} \setminus \{0\}$, gdzie p jest ustaloną liczbą pierwszą nieparzystą.
a) Podać cztery początkowe wyrazy ciągu określonego wzorem $b_n = \frac{1}{2}\left(3^{2^n} + 1\right)$.
b) Podać cztery początkowe wyrazy ciągu określonego wzorem $c_n = \frac{1}{2}\left(5^{2^n} + 1\right)$.
c) Czy dla każdej liczby pierwszej p, różnej od 2, wyrazy ciągu (a_n) są liczbami nieparzystymi?
d) Prowadząc rozumowanie podobne do przedstawionego w zadaniu 6b), wykazać, że (a_n) jest ciągiem liczb parami względnie pierwszych.
e) Sformułować twierdzenie, którego dowodem mogłoby być rozumowanie postulowane w zadaniu d).
f) Podjąć próby uogólnienia twierdzenia, będącego tematem zadania e).

Zadanie 9
Czy można wykazać równoważność zdań:
(1) istnieje nieskończenie wiele liczb pierwszych,
(2) istnieje nieskończony ciąg liczb parami względnie pierwszych,
nie znając wartości logicznej żadnego z nich?

Uwagi natury dydaktycznej o zadaniu 1

Nauczyciel matematyki powinien już na studiach (a nie dopiero w trakcie pracy zawodowej) poznać wiele wiadomości o liczbach pierwszych dla dobrej realizacji programów nauczania matematyki, a zwłaszcza dla przygotowania się do rozbudzania zainteresowania matematyką uczniów uzdolnionych. Poznawanie elementów teorii liczb, nasyconych różnymi ciekawostkami, też natury historycznej, może stanowić dla uczniów szkół średnich (a nawet gimnazjów) wspaniałą zachętę do studiowania matematyki.

Zbyt często absolwenci szkół średnich podają błędną definicję liczby pierwszej oraz błędną definicję liczby złożonej. Dobrym odruchem jest ilustrowanie definicji przykładami i kontrprzykładami. W zadaniu b) oczywiście należy uzasadnić, że liczba 0 (podobnie liczba 1) ani nie jest pierwsza, ani nie jest złożona. Liczba 1 nie jest pierwsza, mimo że spełnia warunek: „jest podzielna tylko przez 1 i przez samą siebie" (zob. zadanie f)). Warto podjąć dyskusję ze studentami, jakie byłyby konsekwencje „poszerzenia" zbioru liczb pierwszych o liczbę 1.

Zadanie d) „prowokuje" do korzystania bądź z definicji liczby pierwszej (liczby złożonej), bądź z cech podzielności liczb, bądź z twierdzeń podających warunki wystarczające na podzielność iloczynu lub sumy liczb naturalnych.

W zadaniu e) wcale nie jest najważniejsze, by rozstrzygnąć, czy liczba Fermata $2^{2^5}+1$ (którą „poznamy" bliżej w zadaniu 6) jest pierwsza. Ważne, by zdać sobie sprawę z trudności, jakie trzeba pokonać, by uzyskać wynik takiego badania (pozwoli to łatwiej zrozumieć, dlaczego Fermat w 1640 roku pomylił się, a Euler dopiero w 1732 roku uzasadnił, że liczba $2^{2^5}+1$ nie jest pierwsza).

Uwagi natury dydaktycznej o zadaniu 2

Oczywiście zadania a) oraz b) nie są trudne. Paradoksalnie, znajomość dowodu Euklidesa tego, że liczb pierwszych jest nieskończenie wiele (zob. zadanie 3) może być źródłem błędnego sądu, że liczby tworzone na wzór sum wymienionych w zadaniu a) są zawsze pierwsze. Oczywiście zrozumienie tego dowodu nie implikuje takiego błędu; w dowodzie tym tworzy się liczbę $p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$, której postać przypomina liczby z zadania 2 a), ale nie twierdzi się, że jest ona pierwsza.

Ostatnie polecenie zadania c) byłoby trudne dla studentów I roku matematyki, którzy jeszcze nie opanowali elementów logiki (które zniknęły z większości programów nauczania matematyki w szkołach średnich), ale nie jest trudne dla studentów wyższych lat, zgłębiających elementy teorii liczb.

W zadaniu d) podano sucho i kategorycznie, że liczba $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1$ nie jest pierwsza. Można ten fakt uzasadnić, korzystając np. z kalkulatora oraz listy liczb pierwszych mniejszych od 1000.

Zauważmy, że studenci mogą postawić hipotezę, że ciąg (a_s) jest nieskończonym ciągiem liczb parami względnie pierwszych. Nie wiemy, czy hipoteza

ta jest prawdziwa i wydaje się, że jest to trudne do rozstrzygnięcia. Ważne, by student matematyki zdawał sobie sprawę, że wielu problemów nie można od razu rozwiązać, a szczególnie inspirujące są te pytania, na które całymi latami nie ma odpowiedzi.

Uwagi natury dydaktycznej o zadaniu 3

Będąc nauczycielem matematyki, nie tylko trzeba wiedzieć, że liczb pierwszych jest nieskończenie wiele, ale wypada znać dowód Euklidesa podany w tym zadaniu. Dobrym sposobem na poznanie dowodu jest uzupełnianie luk w jego redakcji.

Rozwiązując zadania a) i b), uświadamiamy sobie, z czego w istocie korzystamy w tym dowodzie. W szczególności korzystamy z tego, że liczba naturalna większa od 1 ma dzielnik będący liczbą pierwszą.

Uwagi natury dydaktycznej o zadaniu 4

Pojęcie liczb względnie pierwszych nie jest powszechnie znane absolwentom szkół średnich. Nawet ci studenci, którzy po raz pierwszy usłyszą odpowiednią definicję, nie będą mieć trudności ze zilustrowaniem jej przykładami. Zadanie b) powinno okazać się łatwe (choć wymaga sprecyzowania zwrotu „parami").

W zadaniu c) pojawia się konieczność zaproponowania definicji nowego pojęcia. Rosnący ciąg kolejnych liczb pierwszych jest oczywiście nieskończonym ciągiem liczb parami względnie pierwszych. Każdy nieskończony podciąg tego ciągu jest też nieskończonym ciągiem liczb parami względnie pierwszych.

d) Dla uzasadnienia, że ciąg (a_n) nie jest nieskończonym ciągiem liczb parami względnie pierwszych, wystarczy zauważyć, że np. $\mathrm{NWD}(2!, 3!) = 2 \neq 1$.

Zadanie e) jest łatwe. Mogą paść przykłady ciągów określonych wzorami ogólnymi (np. $a_n = 2^n$, $b_n = 3^n$ dla $n \in \mathbb{N}$) lub określonych rekurencyjnie (np. $c_1 = 4$, $c_{n+1} = 3c_n + 2$ dla $n \in \mathbb{N} \setminus \{0\}$).

Uwagi natury dydaktycznej o zadaniu 5

a) Natychmiast otrzymujemy:

$$\begin{aligned} w_1 &= 2, \\ w_2 &= 2 + 1 = 3, \\ w_3 &= 2 \cdot 3 + 1 = 7, \\ w_4 &= 2 \cdot 3 \cdot 7 + 1 = 43, \\ w_5 &= 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807, \\ w_6 &= 2 \cdot 3 \cdot 7 \cdot 43 \cdot 1807 + 1 = 3263443. \end{aligned}$$

b) Nietrudno sprawdzić, że w_5 jest liczbą złożoną; $1807 = 13 \cdot 139$. Tu można podać studentom „ciekawostki" z literatury: w_6 jest liczbą pierwszą, natomiast $w_7, w_8, \ldots, w_{17}$ są liczbami złożonymi (Graham i inni, 2002, s. 132). Znanymi liczbami pierwszymi w ciągu (w_n) są: 2,3,7,43,3263443.

c) Pierwsza równość wynika wprost z określenia ciągu (w_n), druga z lematu: $\mathrm{NWD}(a, b) = \mathrm{NWD}(a, a - b)$ dla $a, b \in \mathbb{N}$, $a > b$.

Uwagi natury dydaktycznej o zadaniu 6

a) Za trudne do natychmiastowego rozstrzygnięcia wydaje się nawet pytanie, czy liczba F_5 jest pierwsza (postawione wcześniej w zadaniu 1 e)). Głównym powodem trudności jest to, że dla $n \geqslant 5$ liczby F_n są tak duże (wielocyfrowe), że znalezienie ich dzielników właściwych (gdyby takie istniały) graniczy z cudem. Powstaje naturalne pytanie: na jakiej drodze wykazać, że liczba F_5 jest złożona? Jeszcze większe trudności wystąpią zapewne przy rozważaniu liczb F_6, F_7 itd.

A co wiadomo z literatury, do której warto odesłać studentów? Z literatury wiemy, że znanymi dotychczas liczbami pierwszymi Fermata są: F_0, F_1, F_2, F_3, F_4. O wielu liczbach Fermata wiadomo, że są złożone. Znane są rozkłady kanoniczne niektórych z nich (Yan, 2006, s. 34, 35). Nie wiadomo, czy istnieje nieskończenie wiele liczb pierwszych Fermata, ani czy istnieje nieskończenie wiele liczb złożonych Fermata. Wszystkie te wiadomości uczą pokory, uczą szacunku dla tych, którzy zmagają się z problemami teorii liczb.

b) W. Narkiewicz poinformował P. Ribenboima, że już w 1730 roku Goldbach w liście do Eulera zawarł dowód tego, że liczby Fermata są parami względnie pierwsze, by wyciągnąć wniosek, że liczb pierwszych jest nieskończenie wiele (zob. Ribenboim, 1997, s. 22). Interesujące jest, że w podobny sposób wiele lat później różni matematycy (może niezależnie od siebie) dowodzili, że liczb pierwszych jest nieskończenie wiele. Dowody tego, że (F_n) jest nieskończonym ciągiem liczb parami względnie pierwszych, można znaleźć w wielu podręcznikach akademickich (Ribenboim, 1997; Sierpiński, 1969; Graham i inni, 2002). Paulo Ribenboim (1997, s. 22) podaje takie rozumowanie:

> Łatwo pokazać przez indukcję ze względu na m, że $F_m - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{m-1}$; stąd, jeżeli $n < m$, to F_n dzieli $F_m - 2$. Gdyby liczba pierwsza p dzieliła zarówno F_n, jak i F_m, to dzieliłaby $F_m - 2$ i F_m, dzieliłaby więc 2 i mielibyśmy $p = 2$. Jednak każda liczba F_n jest nieparzysta, a więc nie jest podzielna przez 2. Dowodzi to, że liczby Fermata są parami względnie pierwsze.

W przedstawionym w temacie zadania b) rozumowaniu korzystamy m.in. z twierdzenia o potęgowaniu potęgi oraz ze wzoru na dwumian Newtona.

c) Korzystając z kalkulatora, łatwo sprawdzić, że $F_5 = 2^{32} + 1 = ((16^2)^2)^2 + 1 = 4294967297 = 641 \cdot 6700417$. Warto zwrócić uwagę, ile lat minęło od pomyłki Fermata do rezultatu Eulera, o których mowa w temacie zadania 6 c).

Mogliśmy tak łatwo sprawdzić, że F_5 jest liczbą złożoną, bo podany został jej dzielnik. W rozumowaniu cytowanym w temacie zadania c) korzystamy m.in. z lematów:
(1) $a^4 - 1 = (a+1)(a-1)(a^2+1)$ dla $a \in \mathbb{R}$,
(2) $a|b \Rightarrow a|bc$ dla $a, b, c \in \mathbb{N}$,
(3) $a|b \wedge a|c \Rightarrow a|b-c$ dla $a, b, c \in \mathbb{N}$.

d) Uzupełnienie istotnych luk w dowodzie naszkicowanym w temacie zadania 6d) wymaga m.in. podnoszenia kolejnych liczb do kwadratu, poczynając od liczby 3. Wystarczy brać pod uwagę jedynie reszty z dzielenia modulo F_5, czyli modulo $2^{32}+1$. Dowód kończy zauważenie, że $3029026160 \not\equiv 1 (mod\, F_5)$.

Uwagi natury dydaktycznej o zadaniu 7

W zadaniu a) określony jest wzorem ogólnym ciąg, którego kolejnymi wyrazami są $4, 10, 82, \ldots$. Oczywiście np. $\mathrm{NWD}(4, 10) \neq 1$. Ciąg (a_n) nie jest więc ciągiem liczb parami względnie pierwszych.

b) Oczywiście wyrazy ciągu (c_n) są liczbami nieparzystymi, w dzieleniu przez 2 dają bowiem resztę 1. Rozwiązanie zadania b) uzyskamy natychmiast, zamieniając w podanym w zadaniu 6 b) dowodzie twierdzenia o liczbach Fermata liczbę 2^{2^n} na liczbę 6^{2^n} i uzasadniając, że zamiana ta nie zmienia (nie psuje) rozumowania.

Zadanie c) mogłoby dotyczyć ciągu (e_n) określonego wzorem $e_n = 8^{2^n} + 1$ dla $n \in \mathbb{N}$. Już teraz można byłoby się pokusić o odkrycie twierdzenia ogólniejszego (ku któremu zmierzamy, proponując zadania d) i e)).

W zadaniu d) proponujemy zbadanie prawdziwości postawionej tam hipotezy. Szczególnym przypadkiem ciągu (d_n) jest np. ciąg (t_n) określony wzorem $t_n = 2^{3^n} + 1$ dla $n \in \mathbb{N}$, a nietrudno zauważyć, że $\mathrm{NWD}(t_1, t_2) = \mathrm{NWD}(3, 9) \neq 1$. Hipoteza podana w zadaniu d) zostałaby w ten sposób obalona.

Do rozwiązania zadania e) wystarczyłoby wzmocnić założenia w hipotezie podanej z zadaniu d) następująco: zarówno a jak i s są ustalonymi liczbami parzystymi dodatnimi. Dowód w istocie niczym się nie różni od przeprowadzonego w rozwiązaniu zadania b).

Uwagi natury dydaktycznej o zadaniu 8

a) Korzystając z kalkulatora, natychmiast otrzymujemy:

$$b_1 = \frac{1}{2}\left(3^2 + 1\right) = 5,$$
$$b_2 = \frac{1}{2}\left(3^4 + 1\right) = 41,$$

$$b_3 = \frac{1}{2}\left(3^8+1\right) = \frac{1}{2}(81\cdot 81+1) = 3281,$$
$$b_4 = \frac{1}{2}\left(3^{16}+1\right) = 21523361.$$

b) Nietrudno otrzymać:

$$c_1 = \frac{1}{2}\left(5^2+1\right) = 13,$$
$$c_2 = \frac{1}{2}\left(5^4+1\right) = 313,$$
$$c_3 = \frac{1}{2}\left(5^8+1\right) = 195313,$$
$$c_4 = \frac{1}{2}\left(5^{16}+1\right) = 76293945313.$$

c) Rozwiązania zadań a) i b) sugerują hipotezę-odpowiedź „tak" na postawione pytanie. Wydaje się, że znalezienie dowodu na to, że wyrazy ciągu (a_n) są liczbami nieparzystymi, może sprawić istotne trudności studentom. W pierwszej części artykułu podaliśmy dwa takie dowody. Na ćwiczeniach z algebry z teorią liczb trzeba byłoby zapewne podać wskazówki lub zadać pytania prowadzące do odkrycia tych dowodów. Krótszy i łatwiejszy do zrozumienia (i zapamiętania) jest dowód przedstawiony w sposobie II, jednak do odkrycia go konieczny był pomysł (mógłby być „sprowokowany" znajomością dowodu podanego w zadaniu 6 b)). Bardziej naturalne, choć dłuższe wydaje się rozumowanie przedstawione w sposobie I (s. 55). Dla przyszłego nauczyciela matematyki zrozumienie rozważań dotyczących cyfr jedności liczby mogłoby być przydatne w pracy z uczniami uzdolnionymi szkół średnich (a nawet gimnazjów), przygotowującymi się do konkursów matematycznych.

d), e) Wskazówka podana w temacie zadania d) powoduje, że z zadania bardzo trudnego staje się zadaniem łatwym. Oczekujemy od studenta rozumowania przez analogię i redakcji dowodu, podobnej do tej, którą podaliśmy w pierwszej części artykułu (dowód twierdzenia 3, s. 5 i 6). Trywialne polecenie w zadaniu e) ma wyrabiać u studenta nawyk podsumowywania osiągnięć, sporządzania listy rezultatów badań. Oczekujemy np. takiej redakcji twierdzenia: jeżeli $p \in \mathbb{P}\setminus\{2\}$, to wyrazy ciągu (a_n) określonego wzorem $a_n = \frac{1}{2}\left(p^{2^n}+1\right)$ są parami względnie pierwsze.

f) Okazuje się, że prawdziwe jest twierdzenie:
jeżeli m jest liczbą nieparzystą większą od 1, a s jest liczbą parzystą dodatnią, to wyrazy ciągu (c_n) określonego wzorem $c_n = \frac{1}{2}\left(m^{s^n}+1\right)$ dla $n \in \mathbb{N}\setminus\{0\}$ są parami względnie pierwsze.

Twierdzenie to jest oczywiście ogólniejsze od twierdzenia podanego w zadaniu e), bo liczba pierwsza różna od 2 jest liczbą nieparzystą większą od 1, a liczba 2 jest liczbą parzystą dodatnią.

Warto może powiedzieć, że ciągi określone w zadaniu 8 udało się odkryć po próbie takiego „poprawiania" definicji ciągu podanego w zadaniu 7 a), by uzyskać ciągi liczb parami względnie pierwszych. W wyrazach ciągu z zadania 7 a) został wyeliminowany ich wspólny czynnik 2. Na ćwiczeniach ze studentami można by było podjąć wspólne próby takiego „przedłużania" zadania 7, które doprowadziłyby do sformułowania hipotez będących tematem zadania 8.

Uwagi natury dydaktycznej o zadaniu 9

Wynikanie (1) $\Rightarrow$ (2) zostało w istocie uzasadnione w zadaniu 5 d). Dowód implikacji (2) $\Rightarrow$ (1) mógłby być następujący:

Symbolem (b_n) oznaczmy nieskończony ciąg liczb parami względnie pierwszych. Niech q_j będzie dzielnikiem pierwszym liczby b_j dla $j \in \mathbb{N} \setminus \{0\}$. Oczywiście (q_n) jest nieskończonym ciągiem różnowartościowym liczb pierwszych. Istotnie, przypuszczenie, iż (q_n) nie jest ciągiem różnowartościowym prowadzi natychmiast do sprzeczności z tym, że (b_n) jest ciągiem liczb parami względnie pierwszych. Skoro (b_n) jest ciągiem nieskończonym, to i (q_n) jest ciągiem nieskończonym. Wynika stąd, że liczb pierwszych jest nieskończenie wiele.

Komentarze do zadań w tym artykule w żadnym stopniu nie powinny krępować prowadzącego zajęcia, który w szczególności może zrezygnować z niektórych zadań, zmienić kolejność ich rozwiązywania, dać więcej swobody zdolnym studentom, którzy mieliby szansę na w pełni samodzielne szukanie rozwiązań, samodzielne formułowanie kolejnych zadań, może przy niektórych zadaniach wdrażać studentów do studiowania literatury i szukania w niej nie tylko wiadomości, ale i inspiracji do formułowania pytań i stawiania hipotez.

Literatura

Edwards, A. W. F.: 1964, Infinite coprime sequences, *Math. Gazette* **48**, 416-422.

Graham, R. L., Knuth, D. E., Patashnik, O.: 2002, *Matematyka konkretna*, PWN, Warszawa.

Górowski, J., Łomnicki, A.: 1993, *Arytmetyka i algebra*, Wojewódzki Ośrodek Metodyczny w Bielsku-Białej, Bielsko-Biała.

Marzantowicz, W., Zarzycki, P.: 2006, *Elementarna teoria liczb*, PWN, Warszawa.

Ribenboim, P.: 1997, *Mała księga wielkich liczb pierwszych*, Wydawnictwo Naukowo-Techniczne, Warszawa.

Sierpiński, W.: 1959a, *O stu prostych ale trudnych zagadnieniach arytmetyki*, PZWS, Warszawa.

Sierpiński, W.: 1959b, *Teoria liczb, cz. 2*, PWN, Warszawa.

Sierpiński, W.: 1964, *200 zadań z elementarnej teorii liczb*, PZWS, Warszawa.

Sierpiński, W.: 1969, *Arytmetyka teoretyczna*, PWN, Warszawa.

Yan, S. Y.: 2006, *Teoria liczb w informatyce*, PWN, Warszawa.

Instytut Matematyki
Uniwersytet Pedagogiczny
ul. Podchorążych 2
PL-30-084 Kraków
e-mail alomnicki@poczta.fm
e-mail jangorowski@interia.pl