

# O liczbach Sierpińskiego

Wojciech GUZICKI\*

\*Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Historia liczb Sierpińskiego zaczyna się chyba od Pierre'a Fermata, prawnika i matematyka z Tuluzy, który około 1640 roku wyraził przypuszczenie, że wszystkie liczby naturalne postaci  $F_n = 2^{2^n} + 1$  (dzisiaj nazywane liczbami Fermata) są pierwsze. Sprawdził, że liczby

$$F_0 = 2^1 + 1 = 3, F_1 = 2^2 + 1 = 5, F_2 = 2^4 + 1 = 17,$$

$$F_3 = 2^8 + 1 = 257, F_4 = 2^{16} + 1 = 65537$$

rzeczywiście są pierwsze. Hipoteza Fermata okazała się nieprawdziwa, pierwszy kontrprzykład został znaleziony około 1747 roku przez Eulera:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Można oczywiście zapytać, jak Euler znalazł ten rozkład na czynniki pierwsze. Czy po prostu miał więcej cierpliwości niż Fermat? Otóż nie. Euler udowodnił, że każdy dzielnik pierwszy  $p$  liczby Fermata  $F_n$  ma postać

$$p = k \cdot 2^{n+1} + 1$$

dla pewnej liczby naturalnej  $k$ . Stąd wynika, że dzielnik pierwszy liczby  $F_5$  musi mieć postać  $p = 64k + 1$ . Teraz wystarczy zbadać 10 liczb (dla  $k = 1, 2, \dots, 10$ ), by znaleźć dzielnik 641.

Odkrycie Eulera i problem badania następnych liczb Fermata spowodowały naturalne zainteresowanie liczbami postaci  $k \cdot 2^n + 1$  i w szczególności pytaniem o to, czy są one pierwsze. Wacław Sierpiński udowodnił w 1960 roku następujące twierdzenie (znane w literaturze teoriolicznej jako twierdzenie Sierpińskiego).

**Twierdzenie.** *Istnieje nieskończenie wiele nieparzystych liczb naturalnych  $k$  o następującej własności:*

- liczba  $k \cdot 2^n + 1$  jest złożona dla każdej liczby naturalnej  $n$ .

Od tego czasu nieparzyste liczby  $k$ , dla których wszystkie liczby postaci  $k \cdot 2^n + 1$  są złożone, zaczęto nazywać liczbami Sierpińskiego. Przedstawię teraz dowód twierdzenia Sierpińskiego. Wcześniej jednak zaprezentuję pewne pojęcie.

Przypuśćmy, że mamy dane dwa ciągi skończone liczb naturalnych tej samej długości  $t$ :

$$(a_1, a_2, \dots, a_t) \quad \text{oraz} \quad (m_1, m_2, \dots, m_t),$$

oraz mamy dany pewien podzbiór zbioru liczb naturalnych  $A \subseteq \mathbb{N}$ . Mówimy, że układ kongruencji

$$\begin{cases} n \equiv a_1 \pmod{m_1}, \\ n \equiv a_2 \pmod{m_2}, \\ \dots\dots\dots \\ n \equiv a_t \pmod{m_t} \end{cases}$$

jest systemem kongruencji pokrywającym zbiór  $A$ , jeśli każda liczba naturalna  $n \in A$  spełnia co najmniej jedną z tych kongruencji. Mówimy także, że zbiór liczb naturalnych  $B \subseteq \mathbb{N}$  pokrywa zbiór  $A$ , jeśli każda liczba  $n \in A$  jest podzielna przez co najmniej jedną liczbę  $p \in B$ . Przejdźmy teraz do dowodu twierdzenia Sierpińskiego.

**Dowód.** Dla dowolnej liczby naturalnej  $k$  oznaczmy:

$$A_k = \{k \cdot 2^n + 1 : n \in \mathbb{N}\}.$$

Niech następnie

$$B = \{3, 5, 17, 257, 641, 65537, 6700417\}.$$

Udowodnię, że istnieje nieskończenie wiele liczb naturalnych  $k$  o własności:

- zbiór  $B$  pokrywa zbiór  $A_k$ .

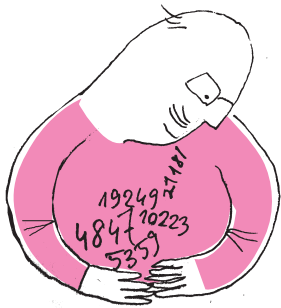
Weźmy trzy ciągi długości 7:

$$(a_1, a_2, \dots, a_7), \quad (m_1, m_2, \dots, m_7) \quad \text{oraz} \quad (p_1, p_2, \dots, p_7),$$



## Rozwiązanie zadania F 1043.

Dla zapewnienia komfortu pasażerów wartość wektorowej sumy przyspieszenia  $a$  w kierunku poziomym i pionowego przyspieszenia ziemskiego  $g$  nie może przekroczyć  $2g$ . Oznacza to, że  $a^2 + g^2 \leq (2g)^2$ , czyli  $a \leq g\sqrt{3}$ . Osiągnięcie prędkości startowej  $v$  wymaga rozpędzenia samolotu ze stałym przyspieszeniem  $a$  w czasie  $t = v/a \geq v/(g\sqrt{3})$ , a potrzebna do tego długość pasa startowego wynosi  $s = at^2/2 = v^2/(2a) \geq v^2/(2g\sqrt{3})$ . Po podstawieniu danych liczbowych otrzymujemy  $t \geq 4,1$  s,  $s \geq 139,3$  m. Obie wartości to oszacowania z dołu – osiągnięcie przyspieszenia  $a$  wymaga pewnego czasu.



zdefiniowane następująco:

$$\begin{aligned} a_1 = 1, & \quad a_2 = 2, & \quad a_3 = 4, & \quad a_4 = 8, & \quad a_5 = 16, & \quad a_6 = 32, & \quad a_7 = 0, \\ m_1 = 2, & \quad m_2 = 4, & \quad m_3 = 8, & \quad m_4 = 16, & \quad m_5 = 32, & \quad m_6 = 64, & \quad m_7 = 64, \\ p_1 = 3, & \quad p_2 = 5, & \quad p_3 = 17, & \quad p_4 = 257, & \quad p_5 = 65537, & \quad p_6 = 641, & \quad p_7 = 6700417. \end{aligned}$$

Wówczas układ kongruencji

$$n \equiv a_i \pmod{m_i} \quad \text{dla } i \in \{1, 2, 3, 4, 5, 6, 7\} \quad (*)$$

pokrywa cały zbiór liczb naturalnych  $\mathbb{N}$ . Możemy także zauważyć, że

$$2^{m_i} \equiv 1 \pmod{p_i} \quad \text{dla } i \in \{1, 2, 3, 4, 5, 6, 7\}.$$

Dowody obu powyższych spostrzeżeń pozostawię jako nietrudne ćwiczenie.

Ustalmy teraz na chwilę liczbę  $i \in \{1, 2, 3, 4, 5, 6, 7\}$ . Liczba  $p_i$  jest nieparzysta, więc  $\text{NWD}(2^{a_i}, p_i) = 1$ . Stąd wynika, że kongruencja

$$2^{a_i} \cdot x \equiv -1 \pmod{p_i}$$

z niewiadomą  $x$  ma rozwiązanie. Niech liczba  $b_i$  będzie rozwiązaniem tej kongruencji. Wówczas mamy:

$$b_i \cdot 2^{a_i} + 1 \equiv 0 \pmod{p_i}.$$

Teraz skorzystamy z chińskiego twierdzenia o resztach. Istnieje nieskończenie wiele liczb naturalnych  $k$  spełniających układ kongruencji:

$$k \equiv b_i \pmod{p_i} \quad \text{dla } i \in \{1, 2, 3, 4, 5, 6, 7\}.$$

Weźmy jedną z takich liczb  $k$  oraz dowolną liczbę  $n \in \mathbb{N}$ . Wówczas  $k \cdot 2^n + 1 \in A_k$ . Układ kongruencji  $(*)$  pokrywa cały zbiór liczb naturalnych, więc istnieje taka liczba  $i \in \{1, 2, 3, 4, 5, 6, 7\}$ , że

$$n \equiv a_i \pmod{m_i}.$$

Wówczas  $n = c \cdot m_i + a_i$  dla pewnej liczby  $c \in \mathbb{N}$ . Stąd wynika, że

$$\begin{aligned} k \cdot 2^n + 1 &= k \cdot 2^{c \cdot m_i + a_i} + 1 = k \cdot 2^{c \cdot m_i} \cdot 2^{a_i} + 1 = k \cdot (2^{m_i})^c \cdot 2^{a_i} + 1 \equiv \\ &\equiv b_i \cdot 1^c \cdot 2^{a_i} + 1 = b_i \cdot 2^{a_i} + 1 \equiv 0 \pmod{p_i}. \end{aligned}$$

Liczba  $k \cdot 2^n + 1 \in A_k$  jest podzielna przez liczbę  $p_i$ . Z dowolności  $n$  wynika, że zbiór  $B = \{p_1, p_2, \dots, p_7\}$  pokrywa zbiór  $A_k$ . Istnieje więc nieskończenie wiele liczb  $k$ , dla których zbiór  $B$  pokrywa zbiór  $A_k$ . To kończy dowód twierdzenia.  $\square$

Z dowodu twierdzenia Sierpińskiego możemy także odtworzyć liczby  $k$  – najmniejszą z nich jest  $k = 15\,511\,380\,746\,462\,593\,381$ . Nie jest to jednak najmniejsza liczba Sierpińskiego. W roku 1962 John Selfridge znalazł mniejszą:  $k = 78557$ . Wykazał także, że zbiór  $B = \{3, 5, 7, 13, 19, 37, 73\}$  pokrywa zbiór  $A_{78557}$ . Jednak nie wiemy, czy liczba 78557 jest najmniejszą liczbą Sierpińskiego. Według *Wikipedii* do kwietnia 2021 roku było jeszcze pięć kandydatek na najmniejszą liczbę Sierpińskiego:

$$21181, \quad 22699, \quad 24737, \quad 55459 \quad \text{oraz} \quad 67607,$$

tzn. o wszystkich pozostałych liczbach mniejszych od 78557 wiadomo, że liczbami Sierpińskiego nie są.

Metoda znajdowania zbiorów pokrywających ma zastosowanie w innych zadaniach. Pokażę jedno z nich. Weźmy dowolną liczbę  $k \geq 2$ . Do niej, na końcu, dopisujemy jedynek. Powstaje pytanie, czy dla każdej liczby naturalnej  $k$  wszystkie tak utworzone liczby są złożone. Odpowiedź jest prawie natychmiastowa: to nie jest prawdą. Dla  $k = 2$  mamy liczbę złożoną 21 oraz liczbę pierwszą 211. Dla  $k = 3$  i  $k = 4$  wystarczy jedna jedynka: liczby 31 i 41 są pierwsze. Dla  $k = 5$  mamy dopiero liczbę pierwszą 511111. Jeszcze gorzej jest dla  $k = 32$  i dla  $k = 12$ : do liczby 32 trzeba dopisać na końcu 35 jedynek, by otrzymać liczbę pierwszą, a do liczby 12 trzeba dopisać aż 136 jedynek.

Okazuje się, że dla liczby 37 jest inaczej. Oznaczmy  $s_n = 37111 \dots 111$ , gdzie w zapisie liczby  $s_n$  mamy  $n$  jedynek. Wówczas można pokazać, że zbiór  $B = \{3, 7, 13, 37\}$  pokrywa zbiór

$$A = \{s_n : n \in \mathbb{N}\}.$$

Warto zauważyć, że dla przeprowadzenia dowodu liczby  $p_1, \dots, p_7$  zostały dobrane tak, żeby  $2^{2^i}$  dzieliło się przez  $p_i$  dla  $1 \leq i \leq 6$  oraz żeby  $2^{2^6}$  dzieliło się przez  $p_7$ .



#### Rozwiązanie zadania F 1044.

W zegarku mechanicznym elementem odmierającym upływ czasu jest tzw. balans drgający pod wpływem siły sprężystości sprężyny. Balans drga w powietrzu znajdującym się wewnątrz zegarka i podczas drgań wprawia w ruch także otaczające powietrze. Masa poruszanego powietrza zwiększa „efektywny” moment bezwładności balansu. Na szczycie wysokiej góry ciśnienie atmosferyczne jest mniejsze niż u jej podnóża, a więc i powietrze wewnątrz zegarka jest rzadsze. Tym samym masa powietrza unoszonego podczas drgań zmniejsza się, co prowadzi do zmniejszenia „efektywnego” momentu bezwładności balansu i skrócenia okresu jego drgań. Na szczycie wysokiej góry zegarek profesora Rabiego spieszył się. Podobno podczas wspólnej podróży koleją Rabi wspominał o swojej obserwacji Enrico Fermiemu, który po godzinie przedstawił dokładny ilościowy opis zjawiska.

Oto dowód. Zauważmy najpierw, że

$$s_n = 37 \cdot 10^n + \frac{1}{9} \cdot (10^n - 1) = \frac{333 \cdot 10^n + 10^n - 1}{9} = \frac{334 \cdot 10^n - 1}{9}.$$

Następnie zauważmy, że liczba  $n$  jest jednej z czterech postaci:

$$n = 3m, \quad n = 6m + 1, \quad n = 6m + 4 \quad \text{lub} \quad n = 3m + 2,$$

gdzie  $m$  jest liczbą naturalną. Mamy zatem cztery przypadki.

**Przypadek 1.** Niech  $n = 3m$ , gdzie  $m$  jest liczbą naturalną. Wówczas:

$$\begin{aligned} 334 &= 9 \cdot 37 + 1 \equiv 1 \pmod{37}, \\ 1000 &= 27 \cdot 37 + 1 \equiv 1 \pmod{37}. \end{aligned}$$

Stąd wynika, że

$$\begin{aligned} 334 \cdot 10^n - 1 &= 334 \cdot 10^{3m} - 1 = 334 \cdot 1000^m - 1 \equiv \\ &\equiv 1 \cdot 1^m - 1 = 0 \pmod{37}. \end{aligned}$$

**Przypadek 2.** Niech  $n = 6m + 1$ , gdzie  $m$  jest liczbą naturalną. Wówczas:

$$\begin{aligned} 3340 &= 477 \cdot 7 + 1 \equiv 1 \pmod{7}, \\ 10^6 &= 142857 \cdot 7 + 1 \equiv 1 \pmod{7}. \end{aligned}$$

Stąd wynika, że

$$\begin{aligned} 334 \cdot 10^n - 1 &= 334 \cdot 10^{6m+1} - 1 = 3340 \cdot (10^6)^m - 1 \equiv \\ &\equiv 1 \cdot 1^m - 1 = 0 \pmod{7}. \end{aligned}$$

**Przypadek 3.** Niech  $n = 6m + 4$ , gdzie  $m$  jest liczbą naturalną. Wówczas:

$$\begin{aligned} 3340000 &= 256923 \cdot 13 + 1 \equiv 1 \pmod{13}, \\ 10^6 &= 76923 \cdot 13 + 1 \equiv 1 \pmod{13}. \end{aligned}$$

Stąd wynika, że

$$\begin{aligned} 334 \cdot 10^n - 1 &= 334 \cdot 10^{6m+4} - 1 = 3340000 \cdot (10^6)^m - 1 \equiv \\ &\equiv 1 \cdot 1^m - 1 = 0 \pmod{13}. \end{aligned}$$

**Przypadek 4.** Niech  $n = 3m + 2$ , gdzie  $m$  jest liczbą naturalną. Wówczas:

$$\begin{aligned} 33400 &= 1237 \cdot 27 + 1 \equiv 1 \pmod{27}, \\ 1000 &= 37 \cdot 27 + 1 \equiv 1 \pmod{27}. \end{aligned}$$

Stąd wynika, że

$$\begin{aligned} 334 \cdot 10^n - 1 &= 334 \cdot 10^{3m+2} - 1 = 33400 \cdot 1000^m - 1 \equiv \\ &\equiv 1 \cdot 1^m - 1 = 0 \pmod{27}. \end{aligned}$$

Skoro liczba  $334 \cdot 10^n - 1$  jest podzielna przez 27, więc liczba

$$s_n = \frac{334 \cdot 10^n - 1}{9}$$

jest podzielna przez 3.

Wykazaliśmy zatem, że we wszystkich przypadkach liczba  $s_n$  jest podzielna przez co najmniej jedną liczbę ze zbioru  $B = \{3, 7, 13, 37\}$ , a więc zbiór  $B$  rzeczywiście pokrywa zbiór  $A$ . Stąd wynika, że jeśli liczba jedynek jest różna od zera, to otrzymana liczba jest złożona. Powstaje pytanie, czy istnieje liczba  $k$  o tej własności, że analogiczne liczby  $s_n$  są złożone dla każdej liczby  $n$ , także równej 0. Okazuje się, że liczba  $k = 38$  ma tę własność.

Można udowodnić (w sposób podobny do powyższego), że:

- jeśli  $n = 3m + 1$  (gdzie  $m$  jest liczbą naturalną), to liczba

$$s_n = 38 \cdot 10^n + \frac{1}{9} \cdot (10^n - 1)$$

jest podzielna przez 3,

- jeśli  $n = 3m + 2$  (gdzie  $m$  jest liczbą naturalną), to liczba

$$s_n = 38 \cdot 10^n + \frac{1}{9} \cdot (10^n - 1)$$

jest podzielna przez 37.

Oba dowody pozostawiamy jako ćwiczenie. Jeśli natomiast  $n = 3m$  (gdzie  $m$  jest liczbą naturalną), to liczba  $s_n$  rozkłada się na czynniki w następujący sposób:

$$\begin{aligned} s_n &= 38 \cdot 10^n + \frac{1}{9} \cdot (10^n - 1) = \frac{343 \cdot (10^m)^3 - 1}{9} = \\ &= \frac{(7 \cdot 10^m)^3 - 1}{9} = \\ &= \frac{7 \cdot 10^m - 1}{3} \cdot \frac{(7 \cdot 10^m)^2 + (7 \cdot 10^m) + 1}{3}. \end{aligned}$$

Sprawdzenie, że oba czynniki

$$\frac{7 \cdot 10^m - 1}{3} \quad \text{oraz} \quad \frac{(7 \cdot 10^m)^2 + (7 \cdot 10^m) + 1}{3}$$

są liczbami całkowitymi, większymi od 1, także pozostawiamy jako ćwiczenie.

Na koniec powróćmy jeszcze do liczb Sierpińskiego. W 1993 roku A. S. Izotov udowodnił następujące twierdzenie:

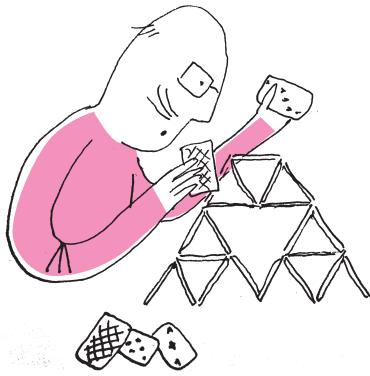
**Twierdzenie.** *Jeśli liczba naturalna  $t$  spełnia układ kongruencji*

$$\begin{cases} t \equiv 1 \pmod{2 \cdot 3 \cdot 17 \cdot 257 \cdot 65537 \cdot 6700417}, \\ t \equiv 0 \pmod{5}, \\ t \equiv 256 \pmod{641} \end{cases}$$

oraz  $k = t^4$ , to  $k$  jest liczbą Sierpińskiego.

**Szkic dowodu.** Można łatwo pokazać, że dla dowolnej liczby naturalnej  $m \geq 0$  zachodzą następujące kongruencje:

$$\begin{aligned} k \cdot 2^{2m+1} + 1 &\equiv 0 \pmod{3}, \\ k \cdot 2^{8m+4} + 1 &\equiv 0 \pmod{17}, \\ k \cdot 2^{16m+8} + 1 &\equiv 0 \pmod{257}, \\ k \cdot 2^{32m+16} + 1 &\equiv 0 \pmod{65537}, \\ k \cdot 2^{64m+32} + 1 &\equiv 0 \pmod{6700417}, \\ k \cdot 2^{64m} + 1 &\equiv 0 \pmod{641}. \end{aligned}$$



Natomiast dla liczb  $n$  postaci  $n = 4m + 2$  liczba  $k \cdot 2^n + 1$  rozkłada się na czynniki. Skorzystamy mianowicie z tożsamości Sophie Germain:

$$\begin{aligned} a^4 + 4b^4 &= a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - (2ab)^2 = \\ &= (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2). \end{aligned}$$

Mamy więc:

$$\begin{aligned} k \cdot 2^n + 1 &= 1 + t^4 \cdot 2^{4m+2} = 1 + 4t^4 \cdot (2^m)^4 = 1^4 + 4(t \cdot 2^m)^4 = \\ &= (1 + 2t \cdot 2^m + 2t^2 \cdot 2^{2m})(1 - 2t \cdot 2^m + 2t^2 \cdot 2^{2m}) = \\ &= (1 + t \cdot 2^{m+1} + t^2 \cdot 2^{2m+1})(1 - t \cdot 2^{m+1} + t^2 \cdot 2^{2m+1}) \end{aligned}$$

oraz obie liczby występujące w rozkładzie po prawej stronie są większe od 1. To kończy szkic dowodu.

Zauważmy także, że dla każdej liczby  $n$  mamy kongruencję

$$k \cdot 2^n + 1 \equiv 1 \pmod{5},$$

z której wynika, że zbiór  $\{3, 5, 17, 257, 641, 65537, 6700417\}$  nie pokrywa zbioru liczb postaci  $k \cdot 2^n + 1$ . Nie mogliśmy zatem powołać się na rozumowanie przedstawione wcześniej w dowodzie twierdzenia Sierpińskiego.



## Zadania

Przygotował Dominik BUREK

**M 1702.** Na kartce w kratkę zaznaczono  $4n$  pól. Udowodnij, że istnieje  $n$  zaznaczonych pól, które są parami rozłączne (tzn. nie mają punktów wspólnych).  
Rozwiązanie na str. 15

**M 1703.** Punkt  $T$  leży wewnątrz trójkąta  $ABC$ , w którym  $\sphericalangle BAC = 60^\circ$ . Ponadto spełniona jest równość

$$\sphericalangle ATB = \sphericalangle CTA = 120^\circ.$$

Punkty  $X$  i  $Y$  są środkami odcinków  $AB$  i  $AC$ , odpowiednio. Udowodnij, że punkty  $A, Y, T$  i  $X$  leżą na jednym okręgu.

Rozwiązanie na str. 4

**M 1704.** Dane są dwie różne liczby całkowite dodatnie  $k$  oraz  $m$ . Udowodnij, że

$$\left(k - \frac{1}{k}\right) \left(m - \frac{1}{m}\right) \leq km - 2.$$

Rozwiązanie na str. 13

Przygotował Andrzej MAJHOFER

**F 1043.** Człowiek poddany działaniu przyspieszenia nieprzekraczającego dwukrotnej wartości przyspieszenia ziemskiego nie doznaje przykrych wrażeń. Prędkość startowa dużych samolotów pasażerskich (np. Jumbo Jeta) wynosi  $v \approx 250$  km/godz. Jaki jest minimalny czas „rozpędzania” samolotu przed startem, podczas którego pasażerowie nie odczuwają dyskomfortu? Jaka jest minimalna długość poziomego pasa startowego potrzebna do osiągnięcia prędkości startowej? Przyspieszenie ziemskie  $g \approx 10$  m/s<sup>2</sup>.

Rozwiązanie na str. 6

**F 1044.** Profesor Izydor Rabi był bardzo dumny z precyzji, z jaką odmierzał czas jego mechaniczny zegarek. Podczas pobytu w laboratorium badającym promieniowanie kosmiczne, położonym na szczycie wysokiej góry, zaobserwował jednak, że jego zegarek przestał wskazywać poprawny czas. Czy na szczycie góry zegarek spieszył się, czy późnił?

Rozwiązanie na str. 7