$2^2 \cdot 5 \cdot 7$ urodziny

W roku 1882 w Dniu Liczby π (który wówczas raczej nie był jeszcze obchodzony) urodził się Wacław Franciszek Sierpiński, postać kluczowa dla rozwoju polskiego środowiska matematycznego. Aby uczcić tę okoliczność, postanowiliśmy w niniejszym wydaniu *Delty* nakreślić wybrane zagadnienia bliskie sercu Jubilata. Nie mogło rzecz jasna zabraknąć „królowej królowej nauk", czyli teorii liczb – o pewnych jej aspektach piszą Mikołaj Rotkiewicz i Wojciech Guzicki. Piotr Zakrzewski przybliża zaś fragmenty ogromnego dorobku Wacława Sierpińskiego z zakresu podstaw matematyki, czyli teorii mnogości. Jeśli zaś chodzi o „pracę u podstaw" – już nie matematyki, a edukacji – Mariusz Skałba przedstawia działalność Jubilata związaną z upowszechnianiem nauki. Dodajmy, że miłośnicy trójkąta Sierpińskiego również znajdą coś dla siebie. Życzymy sobie i Czytelnikom, aby pamięć o Wacławie Sierpińskim, matematyku światowego formatu dostrzegającym i pielęgnującym społeczną rolę nauki, stanowiła inspirację dla przyszłych pokoleń adeptów królowej nauk, tak jak dla obecnych.

Liczby pseudopierwsze

*Mikołaj ROTKIEWICZ**

*Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Możliwość szybkiego i poprawnego identyfikowania liczb jako liczb pierwszych jest kluczowa do prowadzenia efektywnych badań w zakresie teorii liczb. Z tego powodu, przed upowszechnieniem się komputerów, publikowano tablice liczb pierwszych. Dla liczb wykraczających poza granice takich tablic czasami do sprawdzenia pierwszości wykorzystywano jeden z najprostszych algorytmów, polegający na zastosowaniu Małego Twierdzenia Fermata. Mówi ono, że jeśli p jest liczbą pierwszą, to dla każdej liczby całkowitej a liczba $a^p - a$ jest podzielna przez p. W języku kongruencji ten fakt można zapisać jako $a^p \equiv a \pmod p$ lub równoważnie, że $a^{p-1} \equiv 1 \pmod p$, jeśli $p \nmid a$.

D. N. Lehmer, List of Prime Numbers from 1 to 10 006 721 (1914) https://locomat.loria.fr/lehmer1914/lehmer1914doc.pdf

MTF zostało sformułowane (bez dowodu) przez francuskiego matematyka Pierre'a de Fermata (1601–1665). Gottfried Wilhelm Leibniz (1646–1716), wielki filozof i matematyk, pozostawił manuskrypt z dowodem MTF. Jednocześnie Leibniz (mylnie) stwierdził, że podzielność $n \mid 2^n - 2$ nie jest spełniona przez żadną liczbę złożoną.

Ciekawy kombinatoryczny dowód MTF Czytelnik znajdzie w Δ^4_{17}. MTF jest bardzo pomocne przy rozwiązywaniu zadań z olimpiad matematycznych.

Za pomocą MTF udowodnimy, że 221 jest liczbą złożoną. Obliczamy $2^{221} \mod 221$: niech $x_k = 2^{2^k} \mod 221$, więc $x_{k+1} = x_k^2 \mod 221$. Dostajemy kolejno:

k		0	1	2	3	4	5	6	7
x_k	mod 221	2	4	16	35	−101	35	−101	35

Mamy $221 = 2^7 + 2^6 + 2^4 + 2^3 + 2^2 + 2^0$, więc

$$2^{221} \equiv 35 \cdot (-101) \cdot (-101) \cdot 35 \cdot 16 \cdot 2 \equiv 32 \not\equiv 2 \pmod{221},$$

zatem 221 jest złożona. Dla dużej liczby n podany algorytm testowania jej pierwszości jest dużo szybszy od standardowego sprawdzenia warunku $p \nmid n$ dla kolejnych liczb pierwszych $p \leqslant \sqrt{n}$.

P. F. Sarrus (1798-1861), znany z *reguły Sarrusa* stosowanej często do obliczania wyznacznika macierzy 3×3.

János Bolyai (1802–1860), odkrywca i badacz geometrii nieeuklidesowej, osiągnął również znaczące wyniki w teorii liczb. Znalazł wiele liczb złożonych n takich, że $n \mid a^n - a$ dla pewnych ustalonych liczb a. Między innymi uogólnił podany przez Pierre'a Sarrusa przykład (najmniejszej) liczby złożonej n takiej, że $n \mid 2^n - 2$. Jest nią $341 = 11 \cdot 31$, co łatwo pokazać, korzystając z MTF. Mamy $2^{10} \equiv 1 \pmod{11}$, więc $2^{10k} = (2^{10})^k \equiv 1 \pmod{11}$ dla każdej liczby całkowitej k. W szczególności, $11 \mid 2^{340} - 1$. Z drugiej strony $2^5 \equiv 1 \pmod{31}$, więc $31 \mid 2^{340} - 1$ (bo $5 \mid 340$). Zatem $2^{340} - 1$ jest podzielna przez obie liczby pierwsze, 11 i 31, stąd rzeczywiście $11 \cdot 31$ dzieli dwukrotność $2^{340} - 1$, czyli $2^{341} - 2$.

Definicja. Niech a będzie liczbą całkowitą, $a > 1$. Jeśli n jest liczbą złożoną i $n \mid a^n - a$, to n nazywamy liczbą *pseudopierwszą przy podstawie* a, lub krócej – *a-pseudopierwszą*.

Czasami w definicji liczby a-pseudopierwszej przyjmuje się silniejszy warunek, że $n \mid a^{n-1} - 1$. Z warunku $n | 2^{n-1} - 1$ wynika, że n jest nieparzysta. Ciekawą klasę tworzą liczby 2-pseudopierwsze parzyste (patrz zadanie 3), czyli liczby parzyste $n > 2$ takie, że $n | 2^n - 2$. Jest ich nieskończenie wiele (Beeger, 1951).

Zatem 341 jest liczbą 2-pseudopierwszą. Takie liczby zwykło się nazywać krótko liczbami pseudopierwszymi. Podamy teraz odrobinę bardziej wyszukany przykład. Pierre de Fermat był przekonany, że wszystkie wyrazy ciągu $F_n = 2^{2^n} + 1$ są liczbami pierwszymi. Euler (1707–1784) zauważył, że tak nie

F_n nazywa się n-tą liczbą Fermata. Jedynymi znanymi liczbami pierwszymi Fermata są F_1, F_2, F_3 i F_4.

jest, gdyż $641 \mid F_5 = 2^{32} + 1$. Niemniej $F_n \mid 2^{F_n} - 2$, więc F_5 jest pseudopierwsza, co zauważył już János Bolyai. Rzeczywiście, z $2^{2^n} \equiv -1 \pmod{F_n}$ wynika, że $2^{2^{n+1}} = \left(2^{2^n}\right)^2 \equiv (-1)^2 \equiv 1 \pmod{F_n}$. Ponadto mamy $2^{n+1} \mid 2^{2^n}$, gdyż $n+1 \leqslant 2^n$, więc

$$F_n \mid 2^{2^{n+1}} - 1 \mid 2^{2^{2^n}} - 1 = 2^{F_n - 1} - 1 \mid 2^{F_n} - 2.$$

Tematyka liczb pseudopierwszych zainteresowała jednych z najpłodniejszych i najwybitniejszych matematyków XX wieku, Paula Erdösa i Wacława Sierpińskiego. Erdös od razu uzyskał znaczące wyniki dotyczące asymptotycznego rozmieszczenia takich liczb. Sierpiński swój wielki entuzjazm i miłość do matematyki, w szczególności teorii liczb, przekazywał swoim uczniom. Jednym z nich był Andrzej Rotkiewicz (mój Tata) – autor kilkudziesięciu prac i monografii z obszaru liczb pseudopierwszych (i ich uogólnień). Sierpiński lubił dzielić się otwartymi, często drobnymi, zagadnieniami, które go interesowały, zmniejszając tym samym dystans między mistrzem a uczniem. Jednym z takich wspólnie rozwiązanych problemów było to, czy dla liczby złożonej n liczba $(2^n - 2)/n$ może być pierwsza. – Nie może.

Liczb pseudopierwszych jest nieskończenie wiele. Krótki i elegancki dowód podał Sierpiński. Dowód ten zamieszczamy w formie zadania na końcu artykułu.

Istnieją liczby złożone n, dla których $n \mid a^n - a$, dla każdej liczby całkowitej a, czyli liczby a-pseudopierwsze przy dowolnej podstawie a. Nazywamy je liczbami Carmichaela. Robert D. Carmichael (1879-1967) słusznie przypuszczał, że takich liczb jest nieskończenie wiele. Hipoteza ta została jednak rozstrzygnięta dopiero w 1994 roku.

Liczby Carmichaela można znajdować, posługując się prostym kryterium Korselta:

Dowód można znaleźć w K. H. Rosen, *Elementary number theory and its applications.*

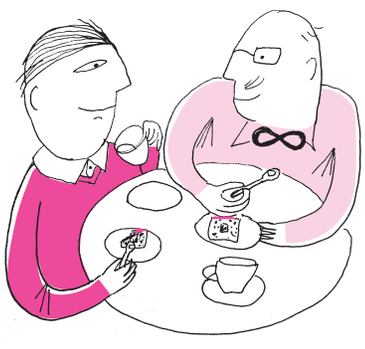
Twierdzenie. *Niech n będzie liczbą złożoną. Następujące warunki są równoważne:*

(i) $n \mid a^{n-1} - 1$ *dla każdej liczby całkowitej a, względnie pierwszej z n.*
(ii) *n jest iloczynem różnych liczb pierwszych i dla każdej takiej liczby p zachodzi $p - 1 \mid n - 1$.*
(iii) $n \mid a^n - a$ *dla każdej liczby całkowitej a.*

Zatem $561 = 3 \cdot 11 \cdot 17$ jest liczbą Carmichaela, gdyż $2, 10, 16 \mid 560$. Jest ona najmniejszą taką liczbą.

Pójdźmy teraz w innym kierunku: ustalamy podstawę a i zajmiemy się konsekwencjami podzielności $n \mid a^{n-1} - 1$, gdzie $2 \nmid n$ i $\mathrm{NWD}(a, n) = 1$. Przedstawmy $n - 1$ w postaci $n - 1 = d \cdot 2^s$, gdzie d jest liczbą nieparzystą, więc $s \geqslant 1$. Niech $x_j = a^{2^j d}$ dla $0 \leqslant j \leqslant s$. Mamy $x_s \equiv 1 \pmod{n}$ i $x_{j+1} \equiv x_j^2 \pmod{n}$. Jeśli n jest liczbą pierwszą, $n \neq 2$, to kongruencja $x^2 \equiv 1 \pmod{n}$ ma dokładnie dwa rozwiązania (1 oraz -1), więc

(i) $x_0 \equiv 1 \pmod{n}$ (wtedy $x_0, x_1, \ldots, x_s \mod n$ jest ciągiem samych jedynek) lub
(ii) istnieje k takie, że $s > k \geqslant 0$ i $x_k \equiv -1 \pmod{n}$ (wtedy $x_{k+1} \equiv x_{k+2} \equiv \ldots \equiv x_s \equiv 1 \pmod{n}$).



Jeśli zaś n jest złożona, to rozwiązań modulo n podzielności $n \mid x^2 - 1$ mamy co najmniej 4, poza przypadkami $n = 4$, p^{k+1}, $2p^k$, gdzie $p \neq 2$ jest liczbą pierwszą, a k – naturalną (patrz zadanie 2). Liczby złożone n, które spełniają alternatywę (i)–(ii) nazywamy *silnie a-pseudopierwszymi.* Czy dana liczba może być silnie a-pseudopierwsza przy każdej podstawie a? Okazuje się, że nie – nie istnieją „silne" liczby Carmichaela. Co więcej, dla każdej liczby złożonej n co najmniej 3/4 możliwych wartości a to dobrzy świadkowie złożoności tej liczby, tzn. n nie jest silnie a-pseudopierwsze. Test pierwszości Millera–Rabina polega na losowaniu k różnych podstaw a i zweryfikowaniu, czy n spełnia powyższy warunek. Prawdopodobieństwo, że liczba złożona n zda powyższy test, jest mniejsze niż $1/4^k$.

Jak dużo jest liczb pseudopierwszych? Problemy dotyczące asymptotycznego rozmieszczenia liczb pierwszych nie są proste. Twierdzenie o liczbach pierwszych, kamień milowy w teorii liczb osiągnięty jeszcze w XIX wieku, mówi, że $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$, gdzie $\pi(x)$ jest liczbą liczb pierwszych nie większych niż x. Dla liczb pseudopierwszych ani też dla liczb Carmichaela nie doczekaliśmy się tak dokładnego wyniku. Niemniej wiadomo, że:

- $\pi_2(x)/\pi(x)$ dąży do zera przy $x \to \infty$, gdzie $\pi_2(x)$ funkcją zliczającą liczby pseudopierwsze nie większe niż x. (P. Erdös, 1950).
- W każdym ciągu arytmetycznym $(an+b)_{n\geqslant 1}$, gdzie $\mathrm{NWD}(a,b) = 1$, $a \geqslant 1$, jest nieskończenie wiele liczb pseudopierwszych (A. Rotkiewicz, 1963). Warunek $\mathrm{NWD}(a,b) = 1$ nie jest tutaj warunkiem koniecznym. Na przykład w ciągu $(4n+2)$ jest też nieskończenie wiele liczb pseudopierwszych. Coś trzeba jednak założyć, bo w niektórych ciągach arytmetycznych nie ma liczb pseudopierwszych (Zadanie 7).

Słynne twierdzenie Dirichleta mówi to samo, ale o liczbach pierwszych.

- $\sum_{n=1}^{\infty} \frac{1}{q_n} < +\infty$ (K. Szymiczek, 1967), gdzie q_n oznacza n-tą liczbę pseudopierwszą.

Szereg odwrotności liczb pierwszych jest rozbieżny, więc liczb pseudopierwszych jest istotnie mniej.

- $\sum_{n=1}^{\infty} \frac{1}{\log q_n} = +\infty$ (A. Mąkowski, 1974).

To jest także pierwszy dowód, że liczb Carmichaela jest nieskończenie wiele.

- Jeśli przez $C(x)$ oznaczymy liczbę liczb Carmichaela nie większych niż x, to $C(x) > x^{2/7}$ dla dostatecznie dużych x (W. R. Alford, A. Granville, C. Pomerance, 1994).

Hipoteza Erdösa mówi, że dla każdego $\epsilon > 0$ zachodzi $\lim_{x\to\infty} C(x)/x^{1-\epsilon} = +\infty$. Z drugiej strony dostępne obliczenia funkcji $C(x)$ i $\pi_2(x)$ (patrz tabela poniżej) nie potwierdzają tego. Raczej można przypuszczać, że $\pi_2(x) < \sqrt{\pi(x)}$ (D. Shanks). Obie hipotezy, Erdösa i hipoteza $\pi_2(x) < \sqrt{\pi(x)}$, stoją we wzajemnej sprzeczności, gdyż $\sqrt{\pi(x)} < \sqrt{x}$ i $\pi_2(x) > C(x)$. Do dziś jednak nie obalono żadnej z nich. Cóż, granica ciągu nie zależy od wartości jego początkowych wyrazów. Liczby w nieskończoności różnią się znacznie od tych, które widzimy tutaj w tabeli: średnia liczba dzielników pierwszych liczb nie większych od x rośnie jak $\log\log x$, i chociaż rośnie bardzo powoli, rośnie bez ograniczeń.

$k = \log_{10} x$	3	5	7	9	11	13	15	17
$C(x)$	1	16	105	646	3605	19279	105212	585355
$\pi_2(x)$	3	78	750	5597	38975	264239	1801533	12604009
$\pi(x)$	168	9592	$6{,}65\cdot 10^5$	$5{,}08\cdot 10^7$	$4{,}11\cdot 10^9$	$3{,}46\cdot 10^{11}$	$2{,}98\cdot 10^{13}$	$2{,}62\cdot 10^{15}$
$\pi_2(x)/\sqrt{\pi(x)}$	0,23	0,8	0,92	0,78	0,61	0,45	0,33	0,25
$\log_x \pi_2(x)$	0,159	0,378	0,411	0,416	0,417	0,417	0,417	0,418
$\log_x C(x)$	0	0,241	0,289	0,312	0,323	0,330	0,335	0,339

Na koniec proponuję kilka zadań, których rozwiązanie z pewnością pozwoli lepiej oswoić się z tematyką poruszoną w tym artykule. Wskazówki można odnaleźć jako załącznik do elektronicznej wersji artykułu na stronie internetowej *Delty*.

1. Wyznaczyć wszystkie liczby naturalne, które są względnie pierwsze z każdym z wyrazów ciągu $2^n + 3^n + 6^n - 1$, $n \geqslant 1$.
2. Znaleźć wszystkie rozwiązania kongruencji $x^2 \equiv 1 \pmod{680}$.
3. Wykazać, że (a) 91 jest 3-pseudopierwszą, (b) 45 jest liczbą pseudopierwszą przy podstawach 17 i 19, (c) $2 \cdot 73 \cdot 1103$ jest liczbą pseudopierwszą (jest to najmniejsza liczba pseudopierwsza parzysta).
4. Wykazać, że jeśli n jest liczbą pseudopierwszą nieparzystą, to $2^n - 1$ jest liczbą silnie pseudopierwszą. Wywnioskować stąd, że liczb pseudopierwszych (i silnie pseudopierwszych) jest nieskończenie wiele. (Sierpiński, 1947)
5. Udowodnić, że jeśli liczby $6k+1$, $12k+1$ i $18k+1$ są pierwsze, to ich iloczyn jest liczbą Carmichaela. Wywnioskować stąd, że $307 \cdot 613 \cdot 919$ jest liczbą Carmichaela. (Chernik, 1939)
6. Wykazać, że (a) 25 jest silnie 7-pseudopierwszą, (b) $829 \cdot 1657$ jest silnie pseudopierwszą przy podstawach 2 i 3.
7. Niech $p \equiv -1 \pmod 6$ będzie liczbą pierwszą, $a = p(p-1)$, $b = 3p$. Uzasadnij, że ciąg arytmetyczny $(an+b)_{n\geqslant 1}$ nie zawiera ani jednej liczby pseudopierwszej.
8. Uzasadnić, że jeśli S jest nieskończonym podzbiorem liczb naturalnych takim, że dla dowolnych liczb względnie pierwszych a, b w ciągu $(an+b)_{n\geqslant 1}$ jest co najmniej jedna liczba ze zbioru S, to w każdym takim ciągu jest nieskończenie wiele liczb z S.
9. Znaleźć wszystkie liczby Carmichaela n takie, że każdy dzielnik pierwszy n jest jedną z liczb 7, 11, 13, 31, 41, 61.