

Liczby pierwsze i złożone; arytmetyka „modulo”

Stefan Sokołowski

Elbląg, 5 V 2025

Wskazówka ogólna:

Żeby udowodnić, że liczba $n > 1$ jest *złożona*, należy znaleźć dwie liczby $p > 1$ i $q > 1$ takie, że $n = p \cdot q$. Proszę nie zapominać o tym pierwszym warunku: oba czynniki **muszą być większe niż 1**.

Żeby udowodnić, że liczba $n > 1$ jest *pierwsza*, należy sprawdzić, że nie jest podzielna przez żadną liczbę (równoważnie: przez żadną liczbę pierwszą) p taką, że $2 \leq p \leq \sqrt{n}$. Tak, wystarczy sprawdzić do pierwiastka kwadratowego, prosty dowód tego faktu proszę wykonać samemu.

Zadanie 1:

Udowodnić, że $n^4 + 4$ jest liczbą złożoną dla dowolnego $n \geq 2$.

Rozwiązanie:

Liczba $n^4 + 4$ daje się rozłożyć na czynniki w następujący sposób:

$$\begin{aligned} n^4 + 4 &= (n^2)^2 + 2^2 \\ &= (n^2 + 2)^2 - 4n^2 \\ &= (n^2 + 2)^2 - (2n)^2 \\ &= (n^2 + 2 - 2n)(n^2 + 2 + 2n) \end{aligned}$$

Trzeba tylko sprawdzić, że żaden z tych czynników nie jest równy 1. Ale z założenia $n \geq 2$ wynika, że

$$n^2 + 2 - 2n = n(n - 2) + 2 \geq 2(2 - 2) + 2 = 2$$

Drugi z tych czynników jest jeszcze większy.

Zadanie 2 (domowe specjalne):

Udowodnić, że

- (a) jeśli F_k jest k -tą liczbą Fermata, t.zn. $F_k = 2^{2^k} + 1$ dla $k \in \mathbb{N}$, to

$$F_0 \cdot F_1 \cdot \dots \cdot F_{n-1} = F_n - 2$$

dla wszystkich $n \in \mathbb{N}$;

- (b) każde dwie **różne** liczby Fermata są względnie pierwsze (czyli nie mają żadnego wspólnego dzielnika większego niż 1);
- (c) istnieje nieskończenie wiele liczb pierwszych.

Punkt (c) powyżej daje się udowodnić na różne sposoby — ale w tym zadaniu proszę to zrobić w oparciu o wcześniej udowodnione własności liczb Fermata.

Uwaga:

Pierwszej osobie, która przyśle mi (na s.sokolowski@ans-elblag.pl) poprawne rozwiązanie tego zadania, przysługują punkty do zaliczenia laboratorium/ćwiczeń. Liczba tych punktów zależy od oryginalności i elegancji rozwiązania. W mailu proszę koniecznie podać swoje **nazwisko, numer zajęć i numer zadania**.

Zadanie 3:

Które z poniższych liczb są pierwsze?

- (a) 2047
- (b) $2^{201} + 1$ (*Wskazówka:* sprawdzić podzielność przez 3)
- (c) $2^{201} - 1$ (*Wskazówka:* sprawdzić podzielność przez 7)
-

Zadanie 4:

Rozłożyć na iloczyn liczb pierwszych liczby:

- (a) 6647
- (b) 9970
-

Zadanie 5:

Wyznaczyć najmniejszą wspólną wielokrotność liczb:

- (a) 980 i 2100
- (b) 1575 i 231
-

Oznaczenia:

$\begin{array}{c} \text{reszta z dzielenia } n \text{ przez } k \\ \text{jest równa} \\ \text{reszcie z dzielenia } m \text{ przez } k \end{array}$	$\Longleftrightarrow$	$\begin{cases} n \bmod k = m \bmod k \\ n \equiv_k m \\ [n]_k = [m]_k \end{cases}$
---	-----------------------	--

Zadanie 6:

Policzyć **bez użycia kalkulatora** (i nie zaplątać się w wielkich liczbach) resztę z dzielenia:

- (a) $1213^3 + 4818^5$ przez 9
- (b) $2123456789 \cdot 801234567$ przez 3
- (c) 2018^{50} przez 6
- (d) $2123456789 \cdot 801234567 + 987654321$ przez 11

Rozwiązanie:

Dla rozwiązania zadania 6(a) można wyliczyć $1213^3 + 4818^5$ a następnie podzielić przez 9, ale wtedy nie unikniemy wielkich liczb. Więc lepiej jest od razu liczyć reszty. Reszta z dzielenia liczby przez 9 jest równa reszcie z dzielenia jej sumy cyfr przez 9:

$$\begin{aligned} [1213]_9 &= [1 + 2 + 1 + 3]_9 = [7]_9 \\ [1213^3]_9 &= [7 \cdot 7 \cdot 7]_9 = [49 \cdot 7]_9 = [4 \cdot 7]_9 = [28]_9 = [1]_9 \\ [4818]_9 &= [4 + 8 + 1 + 8]_9 = [21]_9 = [2 + 1]_9 = [3]_9 \\ [4818^5]_9 &= [3^5]_9 = [27 \cdot 9]_9 = [0]_9 \\ [1213^3 + 4818^5]_9 &= [1 + 0]_9 = [1]_9 \end{aligned}$$

Dlatego resztą z dzielenia liczby $1213^3 + 4818^5$ przez 9 jest 1.

Pozostałe punkty tego zadania można rozwiązać analogicznie.

Zadanie 7:

Wyznaczyć zbiory:

- (a) $[1019932]_{997} \cap \{0, 1, 2, \dots, 996\}$
- (b) $[-1019932]_{997} \cap \{0, 1, 2, \dots, 996\}$

Zadanie 8:

Wyznaczyć dwie ostatnie cyfry liczb:

- (a) $2^{2019} + 3^{2020}$
- (b) $2^{43\,112\,609} - 1$