Wskazówki do zadań z artykułu *Liczby pseudopierwsze*

Mikołaj Rotkiewicz

1. (IMO 2005) Wyznaczyć wszystkie liczby naturalne, które są względnie pierwsze z każdym z wyrazów ciągu $2^n + 3^n + 6^n - 1$, $n \geq 1$.

   Z $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$ i MTF dostajemy $p | 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$ dla $p \neq 2, 3$. Odpowiedź: tylko $n = 1$, gdyż $2 \mid a_1$, $3 \mid a_2$ i $p \mid a_{p-2}$.

2. Znaleźć wszystkie rozwiązania kongruencji $x^2 \equiv 1 \pmod{680}$.

   $680 = 2^3 \cdot 5 \cdot 17 \mid x^2 - 1 \iff 2^3, 5, 17 \mid x^2 - 1$. Zatem $x \equiv \pm 1 \pmod 5$, $x \equiv \pm 1 \pmod{17}$ oraz $x \equiv \pm 1, \pm 3 \pmod 8$. Na mocy twierdzenia chińskiego o resztach, układ kongruencji $x \equiv x_1 \pmod 8$, $x \equiv x_2 \pmod 5$, $x \equiv x_3 \pmod{17}$ jest spełniony przez dokładnie jedną liczbę $0 \leq x < 680$. Pierwsze dwie kongruencje $x \equiv \pm 1 \pmod 5$, $x \equiv \pm 1 \pmod{17}$ dają $x \equiv \pm 1, \pm 16 \pmod{85}$. Odpowiedź: wszystkie $4 \cdot 2 \cdot 2$ rozwiązań można zapisać w postaci $x \equiv a + b \cdot 85$, gdzie $a \in \{\pm 1, \pm 16\}$, $b = 0, \pm 2, 4$.

3. Wykazać, że (a) 91 jest 3-pseudopierwsza, (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.)

   (a) $91 = 7 \cdot 13$, $3^6 \equiv 1 \pmod 7$ (MTF) i również $3^6 \equiv 1 \pmod{13}$, gdyż $\equiv -1 \pmod{13}$. Zatem $3^{6k} \equiv 1 \pmod{7, 13}$, skąd $7 \cdot 13 \mid 3^{90} - 1$, gdyż $6 \nmid 90$.

   (b) $17 \equiv_9 -1$, $17^2 \equiv_5 -1$ oraz $4 \mid 44$.

   (c) Należy wykazać, że $73, 1103 \mid 2^{n-1} - 1$, gdzie $n - 1 = 2 \cdot 73 \cdot 1103 - 1 = 3^2 \cdot 29 \cdot 617$. Mamy $2^6 \equiv -9 \pmod{73}$, skąd $2^9 \equiv -9 \cdot 2^3 \equiv 1 \pmod{73}$. Z kolei, $1102 = 2 \cdot 29 \cdot 119$ i $2^{29} \equiv 1 \pmod{1103}$.

4. Wykazać, że jeśli n jest liczbą pseudopierwszą nieparzystą, to $2^n - 1$ jest liczbą silnie pseudopierwszą. Wywnioskować stąd, że liczb pseudopierwszych (i silnie pseudpierwszych) jest nieskończenie wiele.

   Dowód. $N = 2^n - 1$ jest złożona, bo $2^d - 1 \mid N$ dla każdego $d \mid n$. Mamy $4 \nmid N - 1$, a z $n \mid \frac{N-1}{2}$ wynika, że $N = 2^n - 1 \mid 2^{(N-1)/2} - 1$, więc N jest silnie pseudopierwsza. □

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.

   Dowód. Niech $\mathrm{NWD}(a, n) = 1$, gdzie $n = (6k + 1)(12k + 1)(18k + 1)$. Z MTF, liczba $a^{18k} - 1$ jest podzielne przez każdą z liczb pierwszych $6k + 1$, $12k + 1$ i $18k + 1$. Ponadto $18k \mid n - 1$, skąd $n \mid a^{n-1} - 1$. □

6. Wykazać, że (a) 25 jest silnie 7-pseudopierwsza, (b) $829 \cdot 1657$ jest silnie pseudopierwsza przy podstawach 2 i 3.

   (a) $7^2 \equiv -1 \pmod{25}$, skąd $7^6 \equiv -1 \pmod{25}$.

   (b) $N - 1 = 829 \cdot 1657 - 1 = 2^2 \cdot 3^3 \cdot 7 \cdot 23 \cdot 79$, $828 = 2^2 \cdot 3^2 \cdot 23$ i $1656 = 2 \cdot 828$. Mamy $2^{414} \equiv 1 \pmod{829}$ i $2^{414} \equiv -1 \pmod{1657}$, skąd szybko $2^{(N-1)/2} \equiv -1 \pmod N$. Podobnie można wyliczyć, że $3^{(N-1)/4} \equiv 1 \pmod N$.

7. Niech $p \equiv -1 \pmod 6$ będzie liczbą pierwszą, $a = p(p - 1)$, $b = 3p$. Uzasadnij, że ciąg arytmetyczny $(ak + b)$ nie zawiera ani jednej liczby pseudopierwszej.

Dowód. Niewprost, niech n będzie pseudopiersza, $n = ak + b$. Wtedy $p \mid n \mid 2^n - 2$. Z drugiej strony, $2^{ak+b} = 2^{p(p-1)k+3p} \equiv 2^3 \not\equiv 2 \pmod{p}$, skąd sprzeczność □

8. Uzasadnić, że jeśli S jest nieskończonym podzbiorem liczb naturalnych takim, że dla dowolnych liczb względnie pierwszych a, b w ciągu $(ak + b)_{k\geq 1}$ jest co najmniej jedna liczba ze zbioru S, to w każdym takim ciągu jest nieskończenie wiele liczb z S. Wskazówka: zastosować założenie do ciągów $(a^m k + b)$, gdzie m jest liczbą naturalną.

9. Znaleźć wszystkie liczby Carmichaela n takie, że każdy dzielnik pierwszy liczby n jest jedną z liczb 7, 11, 13, 31, 41, 61.

   Niech $S \subset \{7, 11, 13, 31, 41, 61\}$, $n = \prod_{p\in S} p$, $d = \mathrm{NWW}\{p - 1 : p \in S\}$. (i) Liczba Carmichaela jest iloczynem co najmniej trzech różnych liczb pierwszych. (ii) Z kryterium Korselta, $n \equiv 1 \pmod{d}$, gdzie $d = 60$ lub $120 = 2^3 \cdot 3 \cdot 5$. Dla weryfikacji tej kongruencji warto obliczyć $p \mod 3, 4$ i 5 i podanych liczb pierwszych p. Odpowiedź: $n = 7 \cdot 11 \cdot 13 \cdot 41$, $11 \cdot 13 \cdot 31 \cdot 61$ lub $11 \cdot 31 \cdot 41 \cdot 61$.