Teoria liczb IV – liczby pierwsze

Definicja. Liczba $p \in \mathbb{N} \setminus \{1\}$ jest *pierwsza* wtw. gdy dla każdej liczby całkowitej a zachodzi implikacja $a \mid p \Rightarrow a = p$ lub $a = 1$. (Równoważnie, liczby pierwsze to te liczby naturalne, które mają dokładnie dwa różne dzielniki naturalne). Czasami zbiór liczb pierwszych jest oznaczany symbolem $\mathbb{P}$.

Liczbę $n \in \mathbb{N}$, $n > 1$, która nie jest liczbą pierwszą, nazywamy *liczbą złożoną*.

Stw. 1. Liczba $n \in \mathbb{N}$, $n > 1$ jest złożona wtedy i tylko wtedy, gdy istnieje liczba pierwsza p taka, że $p \leqslant \sqrt{n}$ i $p \mid n$.

Tw. 2. Istnieje nieskończenie wiele liczb pierwszych.

Stw. 3. Liczby pierwsze mają następujące własności:

(i) Jeżeli $p, q \in \mathbb{P}$ i $p \neq q$, to $\mathrm{NWD}(p, q) = 1$.

(ii) Jeżeli $p \in \mathbb{P}$, $a \in \mathbb{N}$ i $p \nmid a$, to $\mathrm{NWD}(p, a) = 1$.

(iii) Jeżeli $p \in \mathbb{P}$, $a_1, a_2, \ldots, a_k \in \mathbb{N}$ oraz $p \mid a_1 a_2 \ldots a_k$, to $p \mid a_i$ dla pewnego $i \in \{1, 2, \ldots, k\}$.

(iv) Jeżeli $p, q_1, q_2, \ldots, q_k \in \mathbb{P}$ i $p \mid q_1 q_2 \ldots q_k$, to $p = q_i$ dla pewnego $i \in \{1, 2, \ldots, k\}$.

Tw. 4. (Podstawowe twierdzenie arytmetyki) Każdą liczbę naturalną $n > 1$ można przedstawić w postaci iloczynu liczb pierwszych, tzn.

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k,$$

gdzie $p_1, p_2, \ldots, p_k \in \mathbb{P}$. Ponadto, przedstawienie takie jest jednoznaczne z dokładnością do kolejności czynników.

Wniosek 5. (Postać kanoniczna liczby naturalnej) Każdą liczbę naturalną $n > 1$ można przedstawić jednoznacznie w postaci

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k},$$

gdzie $p_1, p_2, \ldots, p_k \in \mathbb{P}$, $p_1 < p_2 < \ldots < p_k$, oraz $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$.

Stw. 6. Liczby $a, b \in \mathbb{N}$ zapisano w postaci kanonicznej

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \qquad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k},$$

gdzie $p_i \in \mathbb{P}$, $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$ dla $i = 1, 2, \ldots, k$ oraz $p_1 < p_2 < \ldots < p_k$. Wówczas

(i) $a \mid b$ wtedy i tylko wtedy, gdy $\alpha_i \leqslant \beta_i$ dla $i = 1, 2, \ldots, k$,

(ii) $\mathrm{NWD}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k, \beta_k)}$,

(iii) $\mathrm{NWW}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \ldots \cdot p_k^{\max(\alpha_k, \beta_k)}$.

---

1. Sprawdź, czy liczby (a) 347, (b) 481 są pierwsze.

2. Wyznacz wszystkie liczby pierwsze p takie, że liczby $4p^2 + 1$ i $6p^2 + 1$ też są pierwsze.

3. Znajdź wszystkie liczby pierwsze p takie, że liczby $p + 2$ i $p + 4$ też są pierwsze.

4. Wyznacz wszystkie pary liczb pierwszych p, q takie, że liczby $7p + q$ i $pq + 11$ też są pierwsze.

5. Liczba $p > 3$ jest pierwsza. Wykaż, że $p^2 \equiv 1 \pmod{24}$.

6. Liczby p i $p^2 + 2$ są pierwsze. Wykaż, że liczba $p^3 + 2$ też jest pierwsza.

7. Udowodnij, że dla każdej liczby naturalnej n istnieje n kolejnych liczb naturalnych złożonych.

8. Niech $n \in \mathbb{N}$ i $n > 1$. Udowodnij, że każda liczba postaci (a) $4 \cdot 2^{2^n} + 1$, (b) $5 \cdot 3^{3^n} - 2$ jest złożona.

9. Niech $n \in \mathbb{N}$ i załóżmy, że liczba $2^n + 1$ jest pierwsza. Udowodnij, że n jest potęgą dwójki.

10. Liczby Fermata. Dla $n = 0, 1, 2, \ldots$ niech $F_n = 2^{2^n} + 1$. Udowodnij wzór $F_{n+1} = F_0 F_1 \ldots F_n + 2$ i wywnioskuj stąd, że liczb pierwszych jest nieskończenie wiele.

11. Niech $n \in \mathbb{N}$ i $n > 4$. Udowodnij, że n jest liczbą złożoną wtedy i tylko wtedy, gdy $n \mid (n-1)!$.

12. Udowodnij, że liczb pierwszych postaci $4k + 3$, gdzie $k \in \mathbb{N}$, jest nieskończenie wiele.

13. Udowodnij, że każda liczba naturalna jest różnicą dwóch liczb naturalnych mających tyle samo dzielników pierwszych.

14. Liczba p jest pierwsza. Udowodnij, że liczby $2^p + 3^p$ nie można przedstawić w postaci a^m, gdzie $a, m \in \mathbb{N}$ i $m > 1$.

15. Liczba $p > 2$ jest pierwsza, $a \in \mathbb{N}$ i $p \mid a + 1$. Udowodnij, że $p^{n+1} \mid a^{p^n} + 1$ dla każdej liczby całkowitej nieujemnej n.

16. Udowodnij, że liczba $p \in \mathbb{N}$, $p \geqslant 2$, jest pierwsza wtedy i tylko wtedy, gdy $p \mid \binom{p}{k}$ dla $k = 1, 2, \ldots, p - 1$.

17. Znajdź liczby $a, b, c \in \mathbb{N}$ takie, że $\mathrm{NWW}(a, b, c) \cdot \mathrm{NWD}(a, b, c) \neq abc$.

18. Niech $a, b, c \in \mathbb{N}$. Udowodnij tożsamość

$$\mathrm{NWW}(a, b, c) \cdot \mathrm{NWD}(ab, bc, ca) = abc.$$

19. Załóżmy, że $a, b \in \mathbb{N}$ i dla każdego $k \in \mathbb{N}$ $a^{2k-1} \mid b^{2k}$ oraz $b^{2k} \mid a^{2k+1}$. Udowodnij, że $a = b$.

20. Liczby p, q, r są pierwsze, $n \in \mathbb{N}$, oraz $p^n + q^n = r^2$. Udowodnij, że $n = 1$.