

## Liczby pierwsze

**Definicja.** Liczbą pierwszą nazywamy liczbę  $p > 1$  taką, że jedynymi dzielnikami  $p$  są liczby 1 i  $p$ . Liczby  $a > 1$  nie będące liczbami pierwszymi nazywamy liczbami złożonymi.

**Przykłady.** Liczby pierwsze  $p \leq 20$  : 2, 3, 5, 7, 11, 13, 17, 19.

Liczby złożone  $a \leq 20$  : 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20.

**Twierdzenie.** Każda liczba naturalna większa od 1 ma dzielnik pierwszy.

**Dowód.** Niech  $a > 1$ . Liczba  $a$  ma dzielnik  $d > 1$ , np.  $d = a$ . Niech  $p$  będzie najmniejszym dzielnikiem liczby  $a$ , większym od 1. Wtedy można łatwo pokazać, że  $p$  jest liczbą pierwszą, QED.

Zauważmy, że jeśli liczba  $a > 1$  jest złożona, to najmniejszy dzielnik pierwszy  $p$  liczby  $a$  spełnia nierówność  $p \leq \sqrt{a}$ .

Następujące ważne twierdzenie pochodzi prawdopodobnie od Euklidesa:

**Twierdzenie.** Istnieje nieskończenie wiele liczb pierwszych.

**Dowód.** Przypuśćmy, że istnieje tylko skończenie wiele liczb pierwszych:  $p_1, p_2, \dots, p_n$ . Weźmy liczbę

$$m = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1.$$

Liczba  $m$  ma dzielnik pierwszy  $p$ . Ponieważ  $p_i \mid m - 1$ , więc  $p_i \nmid m$  dla  $i = 1, 2, \dots, n$ . Zatem liczba pierwsza  $p$  jest różna od wszystkich liczb  $p_1, p_2, \dots, p_n$ , wbrew założeniu, że są to wszystkie liczby pierwsze. Zatem istnieje nieskończenie wiele liczb pierwszych, QED.

**Uwaga.** Jeśli liczby  $p_1, p_2, p_3, \dots$  są początkowymi liczbami pierwszymi, to liczba

$$m = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$$

nie musi być pierwsza. Na przykład

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509.$$

**Twierdzenie.** Dla każdej liczby  $n$  istnieje  $n$  kolejnych liczb złożonych.

**Dowód.** Liczby

$$\begin{aligned} &(n+1)! + 2, \\ &(n+1)! + 3, \\ &(n+1)! + 4, \\ &\dots \\ &(n+1)! + n, \\ &(n+1)! + (n+1) \end{aligned}$$

są złożone (pierwsza z nich dzieli się przez 2, druga przez 3, trzecia przez 4 itd.), QED

**Przykład.** Liczby

$$6! + 2 = 722, \quad 6! + 3 = 723, \quad 6! + 4 = 724, \quad 6! + 5 = 725, \quad 6! + 6 = 726$$

są złożone. Nie jest to ciąg najmniejszych kolejnych pięciu liczb złożonych. Najmniejszymi są:

$$24, 25, 26, 27, 28.$$

### **Twierdzenie o istnieniu i jednoznaczności rozkładu na czynniki pierwsze**

**Twierdzenie.** Każda liczba  $a > 1$  jest iloczynem liczb pierwszych:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}.$$

Ten rozkład na czynniki pierwsze jest jednoznaczny (z dokładnością do kolejności czynników). ♠.

**Przykład.** Liczbą 144 ma m. in. następujące rozkłady na czynniki pierwsze:

$$144 = 2^4 \cdot 3^2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 3.$$

Rozkłady te różnią się tylko kolejnością czynników.

**Uwaga.** Nie znamy dotychczas żadnego efektywnego algorytmu rozkładania liczb na czynniki pierwsze. Obecnym rekordem jest rozłożenie w 1999 r. na czynniki liczby 155-cyfrowej. Czas pracy ponad 1000 komputerów osobistych i jednego superkomputera wyniósł ponad 4,5 miesiąca. Istnieją natomiast efektywne algorytmy rozpoznawania liczb pierwszych. ♠.

Można próbować szukać informacji o rozkładzie na czynniki tzw. liczb RSA: są to iloczyny dwóch liczb pierwszych podobnego rzędu wielkości. Rozkład na czynniki po angielsku to *factorization*.

Dowód twierdzenia o istnieniu i jednoznaczności rozkładu pomijamy. Twierdzenie to ma liczne zastosowania.

**Wniosek.** Dzielnikami liczby

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

są liczby postaci

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k},$$

gdzie

$$0 \leq \beta_1 \leq \alpha_1 \quad \wedge \quad 0 \leq \beta_2 \leq \alpha_2 \quad \wedge \quad \dots \quad \wedge \quad 0 \leq \beta_k \leq \alpha_k.$$

**Wniosek.** Liczba dzielników liczby  $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  jest równa

$$d(a) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_k + 1).$$

Często piszemy  $\tau(a)$  zamiast  $d(a)$ .

### Liczby względnie pierwsze

**Definicja.** Liczby  $a$  i  $b$  takie, że  $\text{NWD}(a, b) = 1$  nazywamy liczbami względnie pierwszymi.

**Twierdzenie.** Jeśli

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} \quad \text{oraz} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k},$$

to

$$\text{NWD}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \dots \cdot p_k^{\min(\alpha_k, \beta_k)}.$$

**Przykład.** Niech  $a = 2^4 \cdot 3^5 \cdot 5^3$  oraz  $b = 2^3 \cdot 3^7 \cdot 5^3$ . Wtedy

$$\text{NWD}(a, b) = 2^3 \cdot 3^5 \cdot 5^3.$$

Istnieje metoda wyznaczania największego wspólnego dzielnika dwóch liczb całkowitych nie wymagająca rozkładania tych liczb na czynniki pierwsze. Jest to tzw. algorytm Euklidesa. Działanie tego algorytmu wyjaśnimy na przykładzie.

**Przykład.** Niech  $a = 39$  oraz  $b = 15$ . Wykonujemy ciąg dzielen z resztą:

$$39 = 2 \cdot 15 + 9$$

$$15 = 1 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3$$

Zatem  $\text{NWD}(39, 15) = 3$ ; największym wspólnym dzielnikiem jest ostatnia niezerowa reszta.

### Kongruencje

**Definicja.** Mówimy, że liczba  $a$  przystaje do liczby  $b$  modulo  $m$ , jeśli liczby  $a$  i  $b$  dają te same reszty przy dzieleniu przez  $m$ . Piszemy wtedy

$$a \equiv b \pmod{m}.$$

Równoważnie:

$$a \equiv b \pmod{m} \Leftrightarrow m \mid a - b.$$

Własności kongruencji:

- 1)  $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$ ;
- 2)  $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a - c \equiv b - d \pmod{m}$ ;
- 3)  $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$ ;
- 4)  $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ .

Dowody tych własności pozostawimy Czytelnikowi jako ćwiczenie.

**Zadanie.** Oblicz resztę z dzielenia  $3^{105} + 4^{105}$  przez 11.

**Rozwiązanie.** Zauważmy, że

$$3^5 = 243 \equiv 1 \pmod{11}.$$

Zatem

$$3^{105} = (3^5)^{21} \equiv 1^{21} = 1 \pmod{11}.$$

Podobnie

$$4^5 = 1024 \equiv 1 \pmod{11}.$$

Zatem

$$4^{105} = (4^5)^{21} \equiv 1^{21} = 1 \pmod{11}.$$

Stąd

$$3^{105} + 4^{105} \equiv 1 + 1 = 2 \pmod{11}.$$

Z własności 1) – 4) wynika, że jeśli  $W(x)$  jest wielomianem o współczynnikach całkowitych, to

$$5) \quad a \equiv b \pmod{m} \Rightarrow W(a) \equiv W(b) \pmod{m}.$$

**Cecha podzielności przez 9.** Niech  $n = \overline{c_m c_{m-1} \dots c_1 c_0}$ . Oznaczmy przez  $S(n)$  sumę cyfr liczby  $n$ :

$$S(n) = c_m + c_{m-1} + \dots + c_1 + c_0.$$

Wówczas

$$9 \mid n \Leftrightarrow 9 \mid S(n).$$