

# Teoria liczb

- Zajmuje się własnościami liczb, przede wszystkim całkowitych
- Niepraktyczna? - kryptografia

# Dzielenie liczb całkowitych z resztą

- Niech  $b > 0$ , wtedy dla każdej liczby całkowitej  $a$  istnieją jednoznacznie wyznaczone: iloraz  $q$  i reszta  $r$  spełniające:  $a = bq + r$   $0 \leq r < b$
- Resztę  $r$  z dzielenia  $a$  przez  $b$  zapisujemy też jako:  $a \bmod b$  np.
  - $13 \bmod 6 = 1$   $13 = 2 \cdot 6 + 1$
  - $70 \bmod 8 = 6$   $70 = 8 \cdot 8 + 6$
  - $135 \bmod 11 = 3$
  - $123456789 \bmod 2 = 1$
  - $-3 \bmod 7 = 4$

# Własności

- $b$  dzieli  $a$  (lub  $a$  jest podzielne przez  $b$ ), co zapisujemy  $b|a$ , jeśli istnieje  $q$  takie, że  $b=aq$ .  
W takim wypadku mówimy też, że  $b$  jest dzielnikiem  $a$  lub że  $a$  jest wielokrotnością  $b$ .  
Innymi słowy, jeśli  $b$  dzieli  $a$  to reszta z dzielenia  $a$  przez  $b$  równa jest  $0$  tzn.  $a \bmod b = 0$ .
- Dla dowolnych  $a, b, c$  zachodzi:
  - jeśli  $a|b$  to  $a|bc$ ,
  - jeśli  $a|b$  i  $b|c$  to  $a|c$ ,
  - jeśli  $a|b$ ,  $a|c$  to  $a|(b+c)$ .

# Największy wspólny dzielnik

- Największy wspólny dzielnik liczb  $a$  i  $b$  (zapisywany przez  $\text{NWD}(a,b)$ ), gdzie chociaż jedna z liczb  $a,b$  jest różna od  $0$ , to największa liczba  $d$  taka, że  $d|a$  i  $d|b$ .
- $1 \leq \text{NWD}(a,b) \leq \min(a,b)$ .
- $\text{NWD}(15,25) = 5$
- $\text{NWD}(2,1024) = 2$

# Algorytm Euklidesa

(*Elementy* ok. 300 p.n.e.)

1. Wczytaj liczby  $a, b > 0$ .
2. Oblicz  $r$  jako resztę z dzielenia  $a$  przez  $b$ .
3. Zastąp  $a$  przez  $b$ , zaś  $b$  przez  $r$ .
4. Jeżeli  $b=0$  to zwróć  $a$  w przeciwnym wypadku przejdź do (2).

1.  $a=65$      $b=91$      $65 = 91 \cdot 0 + 65$

2.  $a=91$      $b=65$      $91 = 1 \cdot 65 + 26$

3.  $a=65$      $b=26$      $65 = 2 \cdot 26 + 13$

4.  $a=26$      $b=13$      $26 = 2 \cdot 13 + 0$

5.  $a=13$      $b=0$     Wynik: 13

# Rozszerzenie algorytmu Euklidesa

- Szukamy liczb  $x, y \in \mathbb{Z}$ , takich że:
  - $ax + by = \text{NWD}(a, b)$ .
- Korzystamy z faktu, że:
  - $\text{NWD}(a, b) = r_n = 1 \cdot a_n - b_n q_n \quad (a_0 = a, b_0 = b)$
  - $b_n = r_{n-1} = a_{n-1} - b_{n-1} q_{n-1} \quad (a_n = b_{n-1})$
  - $\text{NWD}(a, b) = b_{n-1} - q_n (a_{n-1} - b_{n-1} q_{n-1}) = (q_n q_{n-1} + 1) b_{n-1} - q_n a_{n-1}$
- Np.
  - $13 = 65 - 2 \cdot 26$
  - $13 = 65 - 2 \cdot (91 - 1 \cdot 65) = 65 - 2 \cdot 91 + 2 \cdot 65 = 3 \cdot 65 - 2 \cdot 91$

# Liczby pierwsze

- Każda liczba  $b > 1$  ma przynajmniej dwa dodatnie dzielniki: 1 oraz  $b$ .
- Liczba pierwsza to liczba naturalna  $p$  posiadająca dokładnie dwa różne dzielniki. W szczególności  $p > 1$ .
- 2,3,5,7,11,13,17,19,23...
- Liczba złożona to liczba naturalna  $a$ , która nie jest pierwsza, a więc ma jakiś dodatni dzielnik różny od 1 i  $a$ .

# Liczby względnie pierwsze

- Liczby względnie pierwsze to takie liczby  $a$  i  $b$ , dla których  $\text{NWD}(a,b)=1$ , co zapisujemy inaczej jako  $a \perp b$ .
- $10 \perp 3$  bo  $\text{NWD}(10,3)=1$
- $12 \nmid \perp 3$  bo  $\text{NWD}(12,3)=3$
- $7 \perp 15$  bo  $\text{NWD}(7,15)=1$

# Lemat Euklidesa

- Jeśli  $n|ab$  i  $n \perp a$ , to  $n|b$ .
- Ponieważ  $\text{NWD}(a,n)=1$ , to istnieją  $x,y$  takie, że  $xa+yn=1$ . Mnożąc obie strony równości przez  $b$  otrzymujemy:  $xab+ynb=b$ .
- Z założenia wiemy, iż  $n$  dzieli lewą stronę powyższej równości. Musi zatem dzielić też prawą.

# Rozkład na liczby pierwsze

- Każdą liczbę  $n > 1$  można przedstawić jako iloczyn liczb pierwszych.
- $84 = 2 \cdot 2 \cdot 3 \cdot 7$
- Fundamentalne Twierdzenie Arytmetyki: każda liczba naturalna  $n > 1$  ma jednoznaczny (z dokładnością do kolejności liczb w iloczynie) rozkład na iloczyn liczb pierwszych.
- $61 \cdot 67 = 4087$
- Dla  $a, b, c \in \mathbb{N}$  jeśli  $a|c$ ,  $b|c$  i  $a \perp b$ , to  $ab|c$ .

# Rozkład na liczby pierwsze

- Mając dany rozkład liczb  $a$  i  $b$  możemy błyskawicznie policzyć  $NWD(a,b)$ .
- Jeśli  $a,b>0$ ,  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  i  $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ ,  
gdzie  $\alpha_i, \beta_i \geq 0$ , to

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

# Najmniejsza wspólna wielokrotność

- Najmniejsza wspólna wielokrotność dwu liczb  $a, b > 0$  (oznaczana przez  $NWW(a, b)$ ) to najmniejsza liczba dodatnia  $w$  taka, że  $a|w$  i  $b|w$ .
- Jeśli  $a, b > 0$ ,  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  i  $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ , gdzie  $\alpha_i, \beta_i \geq 0$ , to

$$NWW(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}$$

- $NWD(a,b) * NWW(a,b) = a * b$
- $NWW(a,b) = a * b / NWD(a,b)$

- Liczb pierwszych jest nieskończenie wiele.
- Dowód: rozważmy liczbę  $n = p_1 p_2 \dots p_k + 1$

# Twierdzenie Dirichleta (1837)

- Dla dowolnych dwu dodatnich i względnie pierwszych liczb  $a, d$  istnieje nieskończenie wiele liczb postaci  $nd+a$  dla  $n>0$ .
- np. dla  $4n+1$ : 1, **5**, 9, **13**, **17**, 21, 25, **29**, 33, **37**, **41**...
- np. dla  $4n+3$ : **3**, **7**, **11**, 15, **19**, **23**, 27, **31**, 35, 39, **43**...

# Twierdzenie Czebyszewa (1850)

- Dla dowolnego  $n > 1$  istnieje liczba pierwsza  $p$  taka, że  $n < p < 2n$ .
- Paul Erdos udowodnił powyższe twierdzenie, a ponadto: dla dowolnej liczby naturalnej  $n > 6$ , między liczbami  $n$  a  $2n$  znajdują się co najmniej dwie liczby pierwsze – co najmniej jedna postaci  $4k + 1$  oraz co najmniej jedna postaci  $4k + 3$ .

# Twierdzenie o liczbach pierwszych

- Sformułowane przez Adrien-Marie Legendre w 1796.
- Udowodnione niezależnie przez Hadamarda i de la Vallée Poussina w 1896.
- $\pi(n) \sim n/\ln(n)$  gdzie  $\pi(n)$  to wielkość zbioru liczb pierwszych nie większych od  $n$
- np. dla  $n=10000$        $\pi(n) \approx 10000/9,21$
- np. dla  $n=10^9$        $\pi(n) \approx 10^9/20,73$

# Sito Eratostenesa

- Wczytaj  $n$ . Wypisz listę wszystkich liczb naturalnych od 2 do  $n$ . Na początku wszystkie liczby są nieskreślone.
- Dopóki istnieje nieskreślona jeszcze liczba na naszej liście nie większa od  $\sqrt{n}$  powtarzaj:
  - Weź pierwszą nieskreśloną liczbę  $p$  z listy i dodaj do zbioru znalezionych liczb pierwszych. Później skreśl liczbę  $p$  z listy i skreśl wszystkie wielokrotności liczby  $p$ , które są jeszcze na liście.
- Wszystkie pozostałe, nieskreślone liczby z listy dodaj do zbioru znalezionych liczb pierwszych.

# Zadania domowe

1. Oblicz:

$$20 \bmod 2 = 0$$

$$20 \bmod 3 = 2$$

$$20 \bmod 7 = 6$$

2. Oblicz NWD, NWW oraz  $x, y$ :

Które liczby są względnie pierwsze?

$$\text{NWD}(84, 133) = 7 = 8 \cdot 84 - 5 \cdot 133$$

$$\text{NWD}(221, 169) = 13 = -3 \cdot 221 + 4 \cdot 169$$

$$\text{NWD}(97, 41) = 1 = 11 \cdot 97 - 26 \cdot 41$$

3. Znajdź liczby pierwsze w przedziale  $\langle 2, 100 \rangle$  za pomocą sita Eratostenesa.