Matematyka dyskretna - teoria

Jan Rodziewicz-Bielewicz, Wydział Informatyki ZUT

May 10, 2019

7 Teoria liczb

Zadanie domowe:

1. Przypomnieć sobie cechy podzielności przez 2, 3, 4, 5, 6, 8, 9, 10, 11.
2. Zapoznać się z algorytmem Euklidesa (wersja z dzieleniem) oraz rozszerzonym algorytmem Euklidesa.

Definicja 37. Liczbę naturalną p nazywamy **pierwszą**, jeżeli posiada dokładne dwa dzielniki naturalne: 1 oraz p. Zbiór wszystkich liczb pierwszych oznaczany jest symbolem $\mathbb{P}$ ($\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$).

Definicja 38. Liczbę naturalną $n > 1$ nazywamy **złożoną**, jeżeli posiada więcej niż 2 dzielniki naturalne.

Definicja 39. Mówimy, że liczba całkowita m **dzieli** liczbę całkowitą a, jeżeli istnieje taka liczba całkowita n, że $m \cdot n = a$. Jeżeli $m \neq 0$, liczbę tą nazywamy **dzielnikiem** lub **wielokrotnością** a.

Twierdzenie 110. (Podstawowe własności podzielności) Niech $a, m, n \in \mathbb{Z}$ oraz $m \neq 0$. Wówczas:

1. Jeżeli $m|a$ i $a|b$, to $m|b$ (przechodniość)
2. $a|a$
3. Jeżeli $m|b$ i $b \in \mathbb{Z}$, to $m|ab$
4. Jeżeli $a|b$ oraz $b \neq 0$, to $|a| \leq |b|$
5. Jeżeli $a|b$ i $b|a$ to $b = a$ lub $b = -a$.
6. Jeżeli $m|a$ i $m|b$ to $m|a \pm b$
7. Jeżeli $p \in \mathbb{P}$ dzieli iloczyn ab, to $p|a \vee p|b$
8. Jeżeli $p \in \mathbb{P}$ dzieli iloczyn $a_1 \cdot \ldots \cdot a_n$, to p dzieli przynajmniej jedną z liczb $a_1, \ldots a_n$

Twierdzenie 111. (O dzieleniu z resztą) Niech $a, b \in \mathbb{Z}$ oraz $b \neq 0$. Istnieją wówczas liczby całkowite q, r takie że:

$$a = bq + r,\ 0 \leq r < |b|$$

Przy tym b dzieli a wtedy i tylko wtedy gdy $r = 0$.

Definicja 40. **Największym wspólnym dzielnikiem (NWD)** liczb całkowitych a i b nazywamy największą liczbę naturalną d, taką że $d|a$ i $d|b$. Używamy oznaczenia $d = NWD(a, b)$ lub krótko $d = (a, b)$.

Twierdzenie 112. (Podstawowe własności NWD) Niech $a, b \in \mathbb{Z}$, $a \neq 0 \vee b \neq 0$. Wówczas:

1. $NWD(a, b) = a \Leftrightarrow b|a$
2. $NWD(a, a + 1) = 1$
3. $NWD(a, 0) = |a|$ $(a \neq 0)$
4. Jeżeli $m = nq + r$, to $NWD(m, n) = NWD(n, r)$ (algorytm Euklidesa)

5. Jeżeli $NWD(an, bn) = dn$, to $NWD(a, b) = d$
6. Jeżeli $d = NWD(a, b)$ to istnieją α, β takie, że $\alpha a + \beta b = d$ ($NWD(a, b)$ jest kombinacją liniową a i b).

Definicja 41. Liczby całkowite a i b nazywamy **względnie pierwszymi**, jeżeli $NWD(a, b) = 1$.

Twierdzenie 113. (Zasadnicze Twierdzenie Arytmetyki) Każda liczba naturalna $n > 1$ da się przedstawić jednoznacznie (z dokładnością co do kolejności czynników) w postaci:

$$n = p_1 p_2 \dots p_k$$

gdzie $k \geq 1$, a $p_1, \dots, p_k$ są liczbami pierwszymi.
Wniosek Każda liczba naturalna $n > 1$ da się przedstawić jednoznacznie (z dokładnością co do kolejności czynników) w postaci iloczynu $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, gdzie $k \geq 1$, a $p_1, \dots, p_k$ są różnymi liczbami pierwszymi (tzw. rozkład kanoniczy).

Definicja 42. Niech $n \in \mathbb{N}$. **Funkcja Eulera** $\varphi(n)$ określa, ile jest liczb naturalnych nie większych od n i względnie pierwszych z n:

$$\varphi(n) = |\{a \in \mathbb{N} : a \leq n \wedge NWD(a, n) = 1\}|$$

Przymuje się, że $\varphi(1) = 1$.

Twierdzenie 114. (Własności funkcji Eulera) Niech $p, q \in \mathbb{P}$ Wówczas:

1. $\varphi(p^a) = p^{a-1}(p - 1)$
2. $\varphi(p) = p - 1$
3. $\varphi(p \cdot q) = (p - 1) \cdot (q - 1)$

Dodatkowo, jeżeli $p_1, p_2, \dots, p_k$ są parami względnie pierwsze, to funkcja jest multiplikatywna:

$$\varphi(p_1 \cdot p_2 \cdot \dots \cdot p_k) = \varphi(p_1) \cdot \varphi(p_2) \cdot \dots \cdot \varphi(p_n)$$

Definicja 43. Mówimy, że liczby całkowite a oraz b **przystają** (inaczej: są kongruentne) modulo liczba n, jeżeli $n|a - b$ (jeżeli dają tą samą resztę z dzielenia przez n. Zapisujemy to krótko:

$$a \equiv b \pmod{n} \text{ lub } a \equiv b < n >$$

Twierdzenie 115. (Własności kongruencji) Niech $a, b, c \in \mathbb{Z}$, $k, n \in \mathbb{N}$. Wówczas:

1. $(a \equiv c \pmod{n} \wedge b \equiv c \pmod{n}) \Rightarrow a \equiv c \pmod{n}$
2. $(a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}) \Rightarrow a \pm c \equiv b \pm d \pmod{n}$
3. $(a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}) \Rightarrow ac \equiv bd \pmod{n}$
4. $(a + b \equiv c \pmod{n}) \Leftrightarrow a \equiv c - b \pmod{n}$
5. $a \pm kn \equiv a \pmod{n}$
6. $a \equiv b \pmod{n} \Rightarrow a^n \equiv b^n \pmod{n}$
7. $a \equiv b \pmod{n} \Rightarrow ak \equiv bk \pmod{nk}$
8. $(a \equiv b \pmod{n} \wedge a = a_1 d \wedge b = b_1 d \wedge n = n_1 d) \Rightarrow a_1 \equiv b_1 \pmod{n}$
9. $(a \equiv b \pmod{n_1} \wedge a \equiv b \pmod{n_2} \wedge \dots \wedge a \equiv b \pmod{n_k}) \Rightarrow a \equiv b \pmod{n}$, gdzie $n = n_1 n_2 \dots n_k$

Definicja 44. Rozważmy zbiór reszt z dzielenia przez n i oznaczmy go jako $\mathbb{Z}_n = \{0, \dots, n - 1\}$. Niech $a \in \mathbb{Z}_n$. **Elementem przeciwnym** do a nazywamy $-a \in \mathbb{Z}_n$, taki że $a + (-a) \equiv 0 \pmod{n}$. Definiujemy również **element odwrotny** do a (o ile istnieje), oznaczany jako a^{-1}, taki że $a \cdot a^{-1} \equiv 1 \pmod{n}$.

Algorytm rozwiązywania kongruencji w postaci $ax \equiv b \pmod{n}$

1. Obliczyć $d = NWD(a, n)$
2. Jeżeli:
   (a) $d = 1$ to równanie ma dokładnie jedno rozwiązanie. Można je wyznaczyć mnożąc kongruencję przez a^{-1}.
   (b) $d > 1 \wedge \sim d|b$ to równanie nie ma rozwiązań.
   (c) $d > 1 \wedge d|b$ to równanie ma dokładnie d rozwiązań rozwiązań, które wyznacza się z użyciem wzoru:
   $$x_{k+1} \equiv (n_1 k + \alpha) \pmod{n}$$
   gdzie $k = 0, 1, \ldots, d-1$, a α jest rozwiązaniem równania $a_1 x \equiv b_1 \pmod{n_1}$, gdzie $n = \frac{n}{d}$, $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$

Twierdzenie 116. (Chińskie Twierdzenie o resztach) Jeżeli liczby całkowite $n_1, \ldots, n_k$ są parami względnie pierwsze, to układ równań:
$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \ldots \\ x \equiv a_k \pmod{n_k} \end{cases}$$
ma jednoznaczne rozwiązanie w zbiorze $\mathbb{Z}_n$, gdzie $n = n_1 \cdot \ldots \cdot n_k$.
Do wyznaczenia rozwiązania służy algorytm Gaussa:
$$x \equiv \sum_{i=1}^{k} a_i \cdot N_i \cdot M_i \pmod{n}$$
gdzie $N_i = \frac{n}{n_i}$, $M_i = N_i^{-1} \pmod{n_i}$

Twierdzenie 117. (Eulera) Niech $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz a i n są względnie pierwsze (NWD(a,n) = 1). Wówczas:
$$a^{\varphi(n)} \equiv 1 \pmod{n}$$
Wniosek Jeżeli $NWD(a, n) = 1$ i $r \equiv s \pmod{\varphi(n)}$ to:
$$a^r \equiv a^s \pmod{n}$$

Twierdzenie 118. (Małe Twierdzenie Fermata) Niech $a \in \mathbb{Z}$, $p \in \mathbb{P}$ oraz a i p są względnie pierwsze (NWD(a,p) = 1). Wówczas:
$$a^{p-1} \equiv 1 \pmod{p}$$
Wniosek 1. $a^p \equiv a \pmod{p}$
Wniosek 2. $n \equiv m \pmod{p-1} \Rightarrow a^n \equiv a^m \pmod{p}$

Definicja 44. Rozpatrzmy kongruencję $x^2 \equiv a \mod p$, gdzie $a \not\equiv 0 \pmod{p}$ oraz $p \in \mathbb{P} \setminus \{2\}$. Jeśli równanie to posiada rozwiązanie, a nazywamy **resztą kwadratową** modulo p. W przeciwnym razie a nazywamy **nieresztą kwadratową**. Zbiór reszt kwadratowych modulo p oznaczamy Q_p, a niereszt $\overline{Q_p}$

Definicja 45. **Symbolem Legendre'a** nazywamy wyrażenie:
$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ gdy } p|a \\ 1, \text{ gdy } a \in Q_p \\ -1, \text{ gdy } a \in \overline{Q_p} \end{cases}$$
Jeśli $\left(\frac{a}{p}\right) = 1$, to równanie $x^2 \equiv a \mod p$ ma rozwiązanie.

Definicja 46. Niech n będzie liczbą nieparzystą o rozkładzie kanonicznym $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. **Symbol Jacobiego** definiujemy następująco:
$$\left(\frac{x}{n}\right) = \prod_{i=1}^{k} \left(\frac{x}{p_i}\right)^{\alpha_i}$$

Twierdzenie 119. (Własności symbolu Legendre'a) Niech $p, q \in \mathbb{P}$. Wówczas:

1. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
2. $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
3. $\left(\frac{1}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
5. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
6. $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$
7. $\left(\frac{p}{q}\right)^2 = 1$
8. $p \neq q \Rightarrow \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ lub $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$ (prawo wzajemności)

References

[1] Larisa Dobryakova, *Matematyka dyskretna*. Lulu, 2012.

[2] Grzegorz Szkibiel, Czesław Wowk, *Zadania z arytmetyki szkolnej i teorii liczb*. Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, 2001.

[3] Władysław Narkiewicz *Teoria liczb*. Wydawnictwo Naukowe PWN, 2003.

[4] Kenneth A. Ross, Charles R. B. Wright, *Matematyka dyskretna*. Wydawnictwo Naukowe PWN, 1999.