Matematyka dyskretna

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. zimowy 2025/26

inf.ug.edu.pl/~amb/MaD

Teoria liczb c.d.

Chińskie twierdzenie o resztach (CRT)

- przykład: $x = 25 \pmod{42}$
  – oznacza $x = 25 + \gamma \cdot 6 \cdot 7$
  – czyli $x = 25 = 1 \mod 6$ oraz $x = 25 = 4 \pmod 7$
- tw.: Jeśli $NWD(k, m) = 1$, to układ równań

$$\begin{cases} x = a \mod k \\ x = b \mod m \end{cases}$$

  ma dokładnie jedno rozwiązanie $\mod k \cdot m$
- dw.: $\exists \alpha, \beta. \alpha \cdot k + \beta \cdot m = 1$ (Euklides),
  czyli $\beta \cdot m = 1 \pmod k$ oraz $\alpha \cdot k = 1 \pmod m$
  $x = a \cdot \beta \cdot m + b \cdot \alpha \cdot k$, spełnia oba równania
  jeśli x_1 też spełnia, to ich różnica spełnia $y = 0 \pmod k$ (czyli $\exists \gamma. y = \gamma \cdot k$) i $y = 0 \pmod m$ (czyli $\exists \delta. y = \delta \cdot m$)
  wówczas
  $y = y \cdot \alpha \cdot k + y \cdot \beta \cdot m = \delta \cdot m \cdot \alpha \cdot k + \gamma \cdot k \cdot \beta \cdot m =$ wielokrotność $k \cdot m$

Chińskie twierdzenie o resztach c.d.

- tw.: $f(x) = \langle x \bmod k, x \bmod m \rangle$ jest izomorfizmem Z_N^* oraz $Z_k^* \times Z_m^*$
  gdzie $N = k \cdot m$, $\alpha \cdot k + \beta \cdot m = 1$
  – odwrotnym jest $g\langle a, b \rangle = a \cdot \beta \cdot m + b \cdot \alpha \cdot k \mod k \cdot m$
- przykład: $42 = 6 \cdot 7, \quad 6 \cdot 6 + (-5) \cdot 7 = 1$
  $f(25) = \langle 25 \bmod 6, 25 \bmod 7 \rangle = \langle 1, 4 \rangle$
  $g\langle 1, 4 \rangle = 1 \cdot (-5) \cdot 7 + 4 \cdot 6 \cdot 6 = 109 = 25 \pmod{42}$
- wniosek: jeśli dany jest układ równań dla zmiennej x

$$\begin{cases} x = a_1 \mod k_1 \\ \dots \\ x = a_\ell \mod k_\ell \end{cases}$$

  i wszystkie k_i są względnie siebie pierwsze, to istnieje jednoznaczne rozwiązanie $\mod k_1 \cdot \ldots \cdot k_\ell$

Twierdzenie Fermata (małe)

- tw.: jeśli p jest liczbą pierwszą i nie dzieli a, to $a^{p-1} = 1 \pmod p$
- dw.: $a^{p-1} = (a \bmod p)^{p-1} \pmod p$, wystarczy więc zbadać przypadek $1 \leqslant a < p$
  - zbiór $\{a \cdot 1 \pmod p, a \cdot 2 \pmod p, \ldots, a \cdot p{-}1 \pmod p\}$ jest równy zbiorowi wszystkich liczb $\{1, 2, \ldots, p{-}1\}$, elementów jest tyle samo, odwracalność $a \pmod p$ gwarantuje, że są różne
  - iloczyn elementów drugiego zbioru jest równy $(p-1)!$, modularnie $(p-1)! \pmod p$
  - iloczyn pierwszy różni się tylko czynnikiem a^{p-1} mod p
  - więc czynnik ten równa się 1

Tw. Fermata, przykłady

- przykład: $2^{10} = 1 \pmod{11}$
  stąd $2^{123456789} = 2^9 = 6 \pmod{11}$
- $a^{560} = a^0 = 1 \pmod 3$ ponieważ $560 = 0 \pmod 2$
  $a^{560} = a^0 = 1 \pmod{11}$ ponieważ $560 = 0 \pmod{10}$
  $a^{560} = a^0 = 1 \pmod{17}$ ponieważ $560 = 0 \pmod{16}$
  więc $a^{560} = 1 \pmod{561}$ (chińskie tw. o resztach, $561 = 3 \cdot 11 \cdot 17$)
- prawie zawsze $2^{n-1} = 1 \pmod n$ implikuje, że n jest liczbą pierwszą
  – 561 jest wyjątkiem, dowolne a spełnia $a^{n-1} = 1 \pmod n$
  – test pierwszości: szybkie potęgowanie w celu sprawdzenia czy $a^{n-1} = 1 \pmod n$, dla różnych wartości a zaczynając od $a = 2$
  – jeśli nie ma równości, to liczba nie jest pierwsza

Funkcja Eulera φ

- $\varphi(n) =$ liczba liczb $a \in \{1, .., n-1\}$ takich że $NWD(a, n) = 1$
- tw. Euklidesa: istnieją współczynniki k, ℓ takie, że $k \cdot a + \ell \cdot n = NWD(a, n)$
- czyli $\varphi(n)$ jest rzędem grupy multiplikatywnej $\mathbb{Z}_n^*$
  – jeśli $n = p$, to $\varphi(p) = p - 1$ (tw. Fermata)
  – jeśli $n = p^k$, to $\varphi(p^k) = p^k - p^{k-1} = (1 - \frac{1}{p}) \cdot n$
  (nie są względnie pierwsze wielokrotności p: $\{p, 2 \cdot p, \ldots, p^k - p\}$)
  – ogólnie $\varphi(n) = n \cdot$ iloczyn $(1 - \frac{1}{p})$ po wszystkich dzielnikach pierwszych n (chińskie tw. o resztach)
  – ważny przypadek $\varphi(p \cdot q) = (p-1) \cdot (q-1)$
  – np. $\varphi(26) = \varphi(2 \cdot 13) = 12$

Twierdzenie Eulera

- tw.: Jeśli $NWD(a, n) = 1$, to $a^{\varphi(n)} = 1 \pmod n$
- małe tw. Fermata jest przypadkiem szczególnym
- wniosek: jeśli $NWD(a, n) = 1$, $x = y \pmod{\varphi(n)}$, to $a^x = a^y \pmod n$
  – tzn. działania mod n można zastąpić działaniami mod $\varphi(n)$ w wykładniku
  – przykład: $2^{43210} = 2^{10} = 10 \pmod{26}$, bo $\varphi(26) = 12$, $43210 = 3600 \cdot 12 + 10$ oraz $2^{10} = 1024 = 39 * 26 + 10$
  – albo: $3^{456789} = 3^9 = 1 \pmod{26}$, bo $\varphi(26) = 12$, $456789 = 38065 \cdot 12 + 9$ oraz $3^9 = 19683 = 757 * 26 + 1$

Kryptografia klucza publicznego: RSA

- Duże liczby pierwsze p oraz q (co najmniej 500 bitowe)
  – $N = p \cdot q$, $\varphi(N) = (p-1) \cdot (q-1)$
  – wybieramy $e \in \mathbb{Z}_N^*$, w zasadzie losowe $< N$ wystarczy, szansa, że jest wielokrotnością p lub q jest zaniedbywalnie mała
  – dla e znajdujemy d takie, że $e \cdot d = 1 \pmod{\varphi(N)}$
  w tym celu wykonujemy algorytm Euklidesa dla e oraz $\varphi(N)$
  – klucz publiczny (N, e), klucz prywatny (N, d)
  – $E((N, e), m) = m^e \pmod{N}$, $D((N, d), c) = c^d \pmod{N}$, $m \in \mathbb{Z}_N^*$, (szansa, że m nie będzie spełniać warunku jest zaniedbywalnie mała)
- Uzasadnienie:
  $D((N, d), E((N, e), m)) = D((N, d), m^e \pmod{N}) =$
  $(m^e)^d \pmod{N} = m^{(e \cdot d) \pmod{\varphi(N)}} \pmod{N} = m^1 \pmod{N} = m$