Matematyka dyskretna

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. zimowy 2025/26

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

Teoria liczb

Relacja podzielności

- a dzieli b, oznaczenia $a|b$, w.t.w. $\exists x.\, b = a \cdot x$
  – a jest dzielnikiem, b jest wielokrotnością, czasami żądamy $b \neq 0$
  – zawsze $b = a \cdot (b \div a) + b \bmod a$, $a|b$ jest równoważne $b \bmod a = 0$
  – oczywiście $a|0$, $a|a$, $1|a$, jeśli $a|b$ oraz $b|c$ to $a|c$, jeśli $a|b$ oraz $a|c$, to $a|(\beta \cdot b + \gamma \cdot c)$ – kombinacje liniowe
- def.: $p > 1$ jest liczbą pierwszą gdy jedynymi dzielnikami są 1 i p
  – fakt: liczba liczb pierwszych $< m \approx m/(\ln m)$
  np. liczb pierwszych dokładnie 100 cyfrowych jest $\geqslant 10^{97}$
  – fakt: każda liczba naturalna ma jednoznaczny rozkład na czynniki pierwsze

Relacja kongruencji

- def.: $a = b \pmod m \Leftrightarrow m|(a - b)$ czyli $a = b + m \cdot q$ dla pewnego q
  nazwa: a przystaje do b modulo m
- zakładamy, że $m \in \mathbb{N}$, ale pozostałe liczby mogą być ujemne
- tw.: $a = b \pmod m \Leftrightarrow a \bmod m = b \bmod m$
  dw.: $a = m \cdot q_a + r_a$, $b = m \cdot q_b + r_b$, po odjęciu stronami
  $a - b = m \cdot (q_a - q_b) + (r_a - r_b)$
- relacja $a = b \pmod m$ jest równoważnością, tj. spełnia
  - zwrotność: $a = a \pmod m$
  - symetria: jeśli $a = b \pmod m$, to $b = a \pmod m$
  - przechodniość: jeśli $a = b \pmod m$ i $b = c \pmod m$, to $a = c \pmod m$
- jeśli $a_i = b_i \pmod m$, $i = 0, 1$, to $a_0 \pm a_1 = b_0 \pm b_1 \pmod m$ oraz $a_0 \cdot a_1 = b_0 \cdot b_1 \pmod m$
- przykład $2025 = 0 \pmod 3$, bo $10 = 1 \pmod 3$

Klasy abstrakcji kongruencji, pierścienie $\mathbb{Z}_m$

- dla każdej realacji równoważności można rozważać klasy abstrakcji, czyli zbiory elementów równoważnych
- $[x]_m = \{y \in \mathbb{Z} \mid x = y \pmod m\} = \{x + q \cdot m \mid q \in \mathbb{Z}\}$
- fakt: $x = y \pmod m \Leftrightarrow y \in [x]_m \Leftrightarrow [x]_m = [y]_m$
- fakt: różne klasy abstrakcji są rozłączne
- def.: pierścień $\mathbb{Z}_m$
  - elementy: klasy abstrakcji relacji kongruencji modulo m
  - zero: $[0]_m = \{q \cdot m \mid q \in \mathbb{Z}\}$
  - jedynka: $[1]_m = \{1 + q \cdot m \mid q \in \mathbb{Z}\}$
  - dodawanie, odejmowanie, mnożenie: poprzez reprezentantów, np. $[x]_m \cdot [y]_m = [x \cdot y]_m$
    dw.: jeśli $[x]_m = [x']_m$ i $[y]_m = [y']_m$, to $[x \cdot y]_m = [x' \cdot y']_m$
- tw.: $\mathbb{Z}_m$ ma zero, jedynkę, istnieją elementy przeciwne, działania są przemienne, łączne, mnożenie jest rozdzielne względem dodawania

$\mathbb{Z}_5$

- tabliczki dodawania i mnożenia

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

+	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- widać, że każdy element niezerowy posiada element odwrotny
  np. $3 \cdot 2 = 1 \pmod 5$ czyli $3^{-1} = 2 \pmod 5$
  nazwa: $\mathbb{Z}_5$ jest nie tylko pierścieniem ale i ciałem

$\mathbb{Z}_6$

- tabliczki dodawania i mnożenia

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

+	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- $\mathbb{Z}_6$ nie jest ciałem, nie każdy element niezerowy posiada element odwrotny
  np. $3 \cdot 2 = 0 \pmod 6$, nie może istnieć element odwrotny 3^{-1} bo wówczas byłoby $3^{-1} \cdot 3 \cdot 2 = 1 \cdot 2 = 2 = 3^{-1} \cdot 0 = 0 \pmod 6$
  – albo istnieją nietrywialne dzielniki zera albo każdy element niezerowy ma odwrotny

Największy wspólny dzielnik (NWD)

- $NWD(a, b) = c$ jeśli $c|a$, $c|b$ oraz c jest największe j.w.
  – w zasadzie będziemy stosować to pojęcie do liczb dodatnich
  – wspólnym dzielnikiem jest zawsze 1
  – jeśli $a \neq 0$, $c|a$ to $c \leqslant |a|$
  – wniosek: jeśli jedna z liczb a, b jest niezerowa, to $NWD(a, b)$ istnieje
- def: a i b są względnie pierwsze, jeśli $NWD(a, b) = 1$
- fakt: jeśli $NWD(a, b) = 1$ to w ich rozkładach na czynniki pierwsze występują zupełnie inne liczby
  – np. $NWD(45, 56) = NWD(3^2 \cdot 5, 2^3 \cdot 7) = 1$
  – w szczególności, jeśli p jest liczbą pierwszą, to $NWD(p, b) \neq 1$ tylko jeśli $p|b$

Algorytm Euklidesa

- Niech $a = \beta \cdot b + r$, wówczas dzielniki (a, b) oraz (b, r) są te same
  – w szczególności $NWD(a, b) = NWD(b, r)$
  – zaczynając od $a \geqslant b \geqslant 0$ otrzymujemy algorytm Euklidesa, koniec jest dla $NWD(a, 0) = a$
- np. w języku python

```
def nwd(a,b):
while b:
a,b=b,a%b
return a
```

uwaga: przez $a\%b$ oznaczamy resztę a mod b, a/b oznacza resztę całkowitoliczbową

- – argumenty zmniejszają się, własność stopu jest gwarantowana
  – jeśli $a < b$, to pierwsze wywołanie da wynik $NWD(a, b) = NWD(b, a)$

Algorytm Euklidesa, złożoność, przykład

- fakt: liczba kroków jest rzędu $\log a$
  – dw.: po dwóch krokach wielkość zadania jest $<$ połowy, $a\%b < a/2$ (najgorszy przypadek to „złoty podział”: $a = b + r$ ma te same proporcje co $b = r + s$)
- złożoność algorytmu: liczba kroków · złożoność dzieleń czyli $(\log a)^3$ (dokładniejsza analiza pokazuje $(\log a)^2$, bo liczby są szybko coraz mniejsze)

nwd(987654321,6543210)

987654321	6543210
6543210	6172821
6172821	370389
370389	246597
246597	123792
123792	122805
122805	987
987	417
417	153
153	111
111	742
42	27
27	15
15	12
12	3
3	0

Algorytm Euklidesa, rozszerzony

- tw.: jeśli $NWD(a, b) = c$, to $\exists \alpha, \beta.\ \alpha \cdot a + \beta \cdot b = c$
- dw.: każda reszta w algorytmie jest kombinacją liniową argumentów, $NWD(a, b)$ jest ostatnią niezerową resztą.
- wniosek z dowodu: współczynniki można obliczyć efektywnie podczas obliczania NWD (rozszerzony algorytm Euklidesa)

```
#!/usr/bin/env python
#Tadeusz Andrzej Kadlubowski
a,b=map(int,file("dane.txt").readlines()[:2])
p,q,r,s = 1,0,0,1
while b: a,b,p,q,r,s = b,a%b,r,s,p−a/b∗r,q−a/b∗s
file("nwd.txt","w").write("%d\n%d\n%d\n%d\n"%(a,p,q))
```

- dw.: jeśli A i B są pierwotnymi wartościami a i b to w każdym przebiegu pętli zachodzi $p \cdot A + q \cdot B = a$ oraz $r \cdot A + s \cdot B = b$.

Arytmetyka modularna, własności

- tw.: jeśli $a \cdot b = a \cdot c \pmod n$ oraz $NWD(a, n) = 1$, to $b = c \pmod n$ (tzn. skracanie ma sens)
- dw. $\exists \alpha, \beta.\ \alpha \cdot a + \beta \cdot n = 1$ czyli $\alpha \cdot a \cdot (b - c) + \beta \cdot n \cdot (b - c) = b - c$, ponieważ $n | \beta \cdot n \cdot (b - c)$ i $n | \alpha \cdot a \cdot (b - c)$ (założenie) więc $n | b - c$
- np. $5 \cdot x = 7 = 40 = 5 \cdot 8 \pmod{11}$ i $NWD(5, 11) = 1$ więc $x = 8 \pmod{11}$
  – ale $4 \cdot 4 = 4 \cdot 1 \pmod{12}$, a jednak $4 \neq 1 \pmod{12}$

Odwrotności liczb w arytmetyce modularnej

- $5 \cdot x = 7 \pmod{11}$ można rozwiązać znajdując odwrotność 5:
  – $9 \cdot 5 = 1 \pmod{11}$ więc $x = 9 \cdot 7 = 8 \pmod{11}$
- jeśli $NWD(a, n) = 1$, to $\exists \alpha, \beta. \alpha \cdot a + \beta \cdot n = 1$, czyli $\alpha \cdot a = 1 \pmod{n}$
  – $11111 \cdot x = 4 \pmod{12345}$, rozwiązanie $x = 2471 \cdot 4 = 9884$
  – ponieważ $2471 \cdot 11111 = 1 \pmod{12345}$ zostało obliczone w rozszerzonym algorytmie Euklidesa
- jeśli $\exists \alpha. \alpha \cdot a = 1 \pmod{n}$, to $\exists \beta. \alpha \cdot a + \beta \cdot n = 1$ czyli $NWD(a, n) = 1$
- problem: rozwiązać równanie $a \cdot x = b \pmod{n}$
  – jeśli istnieje rozwiązanie, to $NWD(a, n) | b$
  – jeśli $NWD(a, b) = c$, $c | b$, to można rozwiązać równoważny problem $(a/c) \cdot x = b/c \pmod{n/c}$
  – np. $12 \cdot x = 21 \pmod{39}$ daje $4 \cdot x = 7 \pmod{13}$, $x = 5$ w oryginalnym problemie są jeszcze rozwiązania 18 i 31

Złożoność działań w arytmetyce modularnej

- zasada: najpierw redukcja modulo, potem działanie
  – $a \cdot b \pmod{N} = ((a \pmod{N}) \cdot (b \pmod{N})) \pmod{N}$
  – złożoność: $\log a + \log b + \log N$ (obliczenie reszt mod N) $+ (\log N)^2$ (obliczenia dla reszt)
- przykład
  – $1098657619865421045 \cdot 87397655445287387345 \pmod{100}$
  $= 45 \cdot 45 = 2025 = 25 \pmod{100}$

Szybkie potęgowanie

Obliczyć

$$
\begin{aligned}
2^{100} &\pmod{123} \\
= 4^{50} \cdot 1 &\pmod{123} \\
16^{25} \cdot 1 &\pmod{123} \\
16^{24} \cdot 16 &\pmod{123} \\
(16^2)^{12} \cdot 16 &\pmod{123} \\
10^{12} \cdot 16 &\pmod{123} \\
(10^2)^6 \cdot 16 &\pmod{123} \\
(100^2)^3 \cdot 16 &\pmod{123} \\
37^3 \cdot 16 &\pmod{123} \\
37^2 \cdot 16 \cdot 37 &\pmod{123} \\
37^2 \cdot 100 &\pmod{123} \\
16^1 \cdot 100 &\pmod{123} \\
16^0 \cdot 100 \cdot 16 &\pmod{123} \\
1 &\pmod{123}
\end{aligned}
$$

```
r=1;
while(n) /* inv: r*b^n mod m */{
    if (n%2) {n--; r=(b*r)%m;}
    else {n=n/2; b=(b*b)%m;}
}
```

```
def potm(b,n,m):
    if n==0: return 1
    if n%2==1: return (b*potm(b,n-1,m))%m
    else: return potm((b*b)%m,n/2,m)%m
```

– liczba kroków $\approx$ długość wykładnika
– przy każdej okazji dokonuje się redukcji modulo
– nigdy nie operuje się na liczbach większych niż kwadrat modułu