Algoritmy z teorie čísel

Filip Hlásek

Abstrakt. Příspěvek shrnuje základní matematické metody především z teorie čísel, které je možné využít k návrhu velice efektivních algoritmů. K vyřešení samotných úloh musíme často přidat i špetku důvtipu.

Úmluva. Všechna čísla v celém příspěvku jsou celá.

Důležité poznatky z teorie čísel

Tvrzení. (Bézoutova rovnost) *Pro každá dvě přirozená a, b existují celá α, β taková, že $gcd(a,b) = \alpha \cdot a + \beta \cdot b$, kde $gcd(a,b)$ značí největšího společného dělitele čísel a, b.*

Poznámka. Později tvrzení dokážeme tím, že vyhovující α a β přímo nalezneme.

Tvrzení. (Malá Fermatova věta) *Pro každé prvočíslo p a každé celé číslo a takové, že $gcd(p,a) = 1$, dává a^{p-1} po dělení p zbytek roven jedné (neboli $a^{p-1} \equiv 1 \pmod{p}$).*

Tvrzení. (Čínská věta o zbytcích) *Mějme $m_1, m_2, \ldots, m_r$ po dvou nesoudělná přirozená čísla a $0 \leq a_1 < m_1, 0 \leq a_2 < m_2, \ldots, 0 \leq a_r < m_r$ libovolná. Potom existuje právě jedno $0 \leq x < m_1 \cdot m_2 \cdots m_r$ takové, že dává zbytek a_i po dělení m_i pro všechna $i = 1, 2, \ldots, r$.*

Tvrzení. (Multiplikativní inverz) *Buď p prvočíslo a $0 < a < p$. Pak existuje právě jedno $0 < b < p$ takové, že ab dává po dělení p zbytek jedna (neboli $ab \equiv 1 \pmod{p}$).*

Samotné algoritmy

Algoritmus je postup, jak něco vyřešit. Obvykle je popsán posloupností kroků, které jsou jednoznačné a vedou ke správnému výsledku. Několik takových algoritmů si zkusíme navrhnout na tradičních úlohách, které se nám později budou hodit.

Příklad. (Eratosthenovo síto) Pro dané N nalezněte všechna prvočísla, která jsou menší nebo rovna N.

Klíčová slova. teorie čísel, kombinatorika, algoritmy

Příklad. (Rozšířený Eukleidův algoritmus) K zadaným přirozeným a, b nalezněte α a β taková, že splňují Bézoutovu rovnost $gcd(a, b) = a \cdot \alpha + b \cdot \beta$.

Příklad. (Rychlé mocnění) Mějme přirozená b, N a M. Navrhněte algoritmus, který spočítá zbytek b^N po dělení číslem M. Zajímá nás především efektivita algoritmu vzhledem k N.

Definice. (Kombinační číslo) Pro $0 \leq K \leq N$ budeme symbolem $\binom{N}{K}$ (čteme „*kombinační číslo N nad K*“, nebo jen „*N nad K*“) značit počet možností jak lze z N prvkové množiny vybrat K prvkovou podmnožinu.

Cvičení. (Násobení a sčítání modulo) Pokud nás zajímá zbytek součtu po dělení nějakým přirozeným číslem, stačí nejprve vymodulit jednotlivé sčítance, poté zbytky sečíst a na závěr opět „*vymodulit*“. Analogicky to platí také pro násobení. Dokažte.

Příklad. (Kombinační číslo modulo prvočíslo) Pro zadaná $0 \leq K \leq N \leq M$ (M je prvočíslo) spočítejte zbytek po dělení $\binom{N}{K}$ číslem M. Vylepšete algoritmus tak, aby si nejprve něco předpočítal a poté odpovídal na kombinační čísla efektivně.

Příklad. (Fibonacciho čísla) Spočtěte zbytek N-tého členu Fibonacciho posloupnosti[1] po dělení zadaným přirozeným číslem M.

Ostré úlohy

Příklad 1. Jsou dány rozměry mřížky $1 \leq M, N \leq 100\ 000$. Dále je zadáno $1 \leq K \leq 100$ mřížových bodů, na kterých leží kámen. Navrhněte algoritmus, který spočítá počet cest po mřížce z levého horního do pravého dolního rohu, které jdou pouze doprava nebo dolů, a které neprocházejí přes políčka s kameny. Vypište pouze zbytek po dělení číslem $10^9 + 9$. (MO 59-P-III-4)

Příklad 2. Nalezněte počet neprázdných podmnožin množiny

$$\{1^1, 2^2, 3^3, \ldots, 250250^{250250}\}$$

takových, že součet jejich prvků je dělitelný číslem 250. Zajímá nás pouze posledních 16 cifer odpovědi. (Projecti Euler [1] – úloha 250)

Příklad 3. Je dána mřížka $M \times N$, které chybí pravý horní roh o rozměrech $m \times n$. Kolik existuje různých cest z levého horního do pravého dolního rohu, které jdou po mřížce vždy jen doprava nebo dolů? Vypište zbytek po dělení výsledku číslem 10^9+7. (Codechef [2] - December Challenge 2012 – problem CNTWAYS)

Příklad 4. Monča má dřevěnou šachovnici o rozměrech $R \times C$ a N kovových krychlí takových, že délky jejich hran jsou stejné jako délka strany jednoho čtverečku

[1] Fibonacciho posloupnost je definována následujícím předpisem: $F_0 = 0$, $F_1 = 1$ a $F_{i+2} = F_{i+1} + F_i$ pro nezáporné celé i.

šachovnice. Můžete předpokládat, že $1 \leq R, C \leq 10$ a $1 \leq N \leq 100\ 000$. Chce z nich na šachovnici postavit takové věže, aby bylo dohromady vidět co nejvíce stěn (smí je stavět jen do imaginární krychlové mřížky určené šachovnicí). Navrhněte algoritmus, který spočítá počet rozložení maximalizujících počet viditelných stěn a vypište zbytek výsledku po dělení prvočíslem $10^9 + 9$.

(Rýchlostné programovanie [3] – úloha seecubes2)

Příklad 5. V nově vybudované obytné čtvrti stojí v řadě N obydlí. Chceme uspořádat večírek a seznámit tak zejména co nejvíce lidí, kteří doposud neměli příležitost k setkání. Kolika různými způsoby můžeme pozvat lidi z jednotlivých domů tak, aby nebyli pozváni obyvatelé tří po sobě jdoucích domů? Jinými slovy, „Kolik podmnožin domů nobsahuje tři po sobě jdoucí domy(včetně prázdné podmnožiny)?“ Pro $1 \leq N \leq 10^{15}$ vypište výsledek modulo $10^9 + 7$.

(Codechef [2] – September Challenge 2012 – problem CROWD)

Příklad 6. Je zadáno $1 \leq M \leq 10^{18}$ a $1 \leq N \leq 8$. Kolika způsoby je možné vyskládat mřížku $M \times N$ dominovými kostkami[2]? Vypište výsledek modulo $10^9 + 9$.

(variace MO 60-P-I-1)

Odkazy

[1] http://projecteuler.net/
[2] http://www.codechef.com/
[3] http://people.ksp.sk/~acm
[4] http://www.cse.iitd.ernet.in/~sak/courses/ant/notes/ant.pdf
[5] http://www.math.leidenuniv.nl/~psh/ANTproc/02buhler.pdf
[6] http://mj.ucw.cz/papers/numth.pdf

[2] Dominové kostky jsou tvaru 2×1 a v tomto případě na sebe nemusí navazovat tak, jak je tomu v původní hře.