MC358 - Fundamentos matemáticos da computação

Prof. Dr. Hilder Vitor Lima Pereira

Instituto de computação

UNICAMP

29 de novembro de 2023

Conceitos básicos de contagem

Binômio de Newton

$$(x+y)^n = \sum_{k=0}^{n} x^k \cdot y^{n-k} \cdot \binom{n}{k}$$

Exemplo: quantidade de desordenações

Considere o conjunto $X = \{1, 2, ..., n\}$.

Dizemos que uma tupla $(x_1, ..., x_n) \in X^n$ é uma *desordenação* se ela satisfaz duas propriedades:

1. $i \neq j \Rightarrow x_i \neq x_j$
2. $x_i \neq i$ para $1 \leq i \leq n$.

Exemplo: quantidade de desordenações

Considere o conjunto $X = \{1, 2, ..., n\}$.

Dizemos que uma tupla $(x_1, ..., x_n) \in X^n$ é uma *desordenação* se ela satisfaz duas propriedades:

1. $i \neq j \Rightarrow x_i \neq x_j$
2. $x_i \neq i$ para $1 \leq i \leq n$.

Por exemplo, para $n = 4$, as tuplas $(2, 1, 4, 3)$ e $(3, 1, 4, 2)$ são desordenações.

Já a tupla $(2, 4, 3, 1)$ não é, pois 3 aparece na terceira posição.

Considere o conjunto $X = \{1, 2, ..., n\}$.

Dizemos que uma tupla $(x_1, ..., x_n) \in X^n$ é uma *desordenação* se ela satisfaz duas propriedades:

1. $i \neq j \Rightarrow x_i \neq x_j$
2. $x_i \neq i$ para $1 \leq i \leq n$.

Por exemplo, para $n = 4$, as tuplas $(2, 1, 4, 3)$ e $(3, 1, 4, 2)$ são desordenações.

Já a tupla $(2, 4, 3, 1)$ não é, pois 3 aparece na terceira posição.

Considere $n = 3$. Quantas desordenações existem?

Exemplo: números com quantidade par de zeros

Seja s_n a quantidade de sequências com n dígitos decimais, ou seja, elementos de $\{0, 1, ..., 9\}^n$, que têm uma quantidade par de zeros.

Vamos encontrar uma expressão para s_n.

Teorema chinês do resto

Você tem um vetor $v \in \mathbb{Z}^n$ com dados de entrada.

Você quer calcular uma função $f : \mathbb{Z} \to \mathbb{Z}$ para cada entrada v_i.

Quantas operações você precisa fazer?

Você tem um vetor $\mathrm{v} \in \mathbb{Z}^n$ com dados de entrada.

Você quer calcular uma função $f : \mathbb{Z} \to \mathbb{Z}$ para cada entrada v_i.

Quantas operações você precisa fazer?

Por exemplo, para $\mathrm{v} = (1, 4, 3, 5)$ e $f(z) = 3z^3 + 10$, temos

$$(f(1), f(4), f(3), f(5)) = (13, 202, 91, 385)$$

Você tem um vetor $v \in \mathbb{Z}^n$ com dados de entrada.

Você quer calcular uma função $f : \mathbb{Z} \to \mathbb{Z}$ para cada entrada v_i.

Quantas operações você precisa fazer?

Por exemplo, para $v = (1, 4, 3, 5)$ e $f(z) = 3z^3 + 10$, temos

$$(f(1), f(4), f(3), f(5)) = (13, 202, 91, 385)$$

Considere $p = (2053, 2063, 2069, 2081)$ e $x = 10206570230120...$

Calcule f uma única vez: $y = f(x)$...

Isomorfismos

São bijeções que preservam as propriedades das estruturas algébricas.

- Grafos
- $(i, \times) \simeq (\mathbb{Z}_4, +)$
- $(\mathbb{Z}_N, +, \times) \simeq (\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_m}, +, \times)$

É praticamente o contrário do exemplo em que calculamos várias vezes a função em paralelo (módulo cada primo) calculando-a uma única vez...

Imagine que você quer trabalhar com inteiros de 600 bits. Ou seja, você quer operar em $\mathbb{Z}_N$ para $N \geq 2^{600}$.

Então, você pode

- Escolher primos p_1, ..., p_{10} de 60 bits cada
- Definir $N = \prod_{i=1}^{10} p_i$
- E trabalhar com cada $\mathbb{Z}_{p_i}$ em paralelo.

Teorema

Seja $N = n_1 \cdot n_2 \cdot ... \cdot n_m$, onde os fatores n_i's são coprimos entre si. Então, para quaisquer inteiros $a_1, a_2, ..., a_m$, o seguinte sistema tem uma única solução $x \in \mathbb{Z}_N$

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_m \pmod{n_m} \end{cases}$$

Exemplo

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases}$$

Exemplo

Encontre x tal que

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 0 \pmod{3} \\ x \equiv 2 \pmod{7} \end{cases}$$

Exemplo

Encontre x tal que

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 0 \pmod 3 \\ x \equiv 2 \pmod 7 \end{cases}$$

Encontre y tal que

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 0 \pmod 7 \end{cases}$$

Perguntas, observações, comentários?