Number Theory

Aritmética Modular, Diofantina e GCD Estendido

Lucas Turci

GRUPO DE ESTUDOS PARA A MARATONA DE PROGRAMAÇÃO

Number Theory

A teoria dos números é o ramo da matemática pura que estuda propriedades dos números em geral, e em particular dos números inteiros, bem como a larga classe de problemas que surge no seu estudo - Wikipedia PT-BR

Aritmética Modular

- Baseada na operação mod (% na computação).
- Diz-se que $a \equiv b \; (mod \; m)$ se:
  - Na matemática: $m|(a - b)$
  - Na computação: $a\%m = b\%m$

Aritmética Modular

- As operações +, -, x continuam valendo, por isso se diz que é uma outra “aritmética”

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3

$$ka \underset{m}{\equiv} kb \iff k(a-b) \underset{m}{\equiv} 0$$

Aritmética Modular

- A operação de / vira a multiplicação pelo inverso modular
- O inverso modular de x mod m é y tal que $xy \underset{m}{\equiv} 1$
- Assim como 1/x é o inverso de x, pois $x\frac{1}{x} = 1$

OBS: Só existe inverso modular de a módulo m se a for coprimo com m (vamos ver depois)

Aritmética Modular

Utilidade em alguns problemas

- Quantas subsequências de um array tem soma divisível por K?
- Quantos múltiplos de K existem nos primeiros N números de Fibonacci? (e pra N=10^18?)

$$1 \leq N \leq 10^5, 1 \leq K \leq 50$$

Aritmética Modular

Utilidade em alguns problemas

- Contar algo e imprimir o resto da divisão por 10^9 + 7
- Se a resposta for um número racional irredutível $\frac{p}{q}$, imprimir $pq^{-1} mod\ M$
- Se M for primo, achar o inverso modular é mais fácil.

Algoritmo de Euclides

- Como encontrar g = gcd(a, b)?

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

$$g|a, g|b$$

Algoritmo de Euclides

- Como encontrar g = gcd(a, b)?

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

$$g|a, g|b$$

$$ga' = gb'q + r \Rightarrow r = g(a' - b'q) \Rightarrow g|r$$

Algoritmo de Euclides

- Como encontrar g = gcd(a, b)?

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

gcd(a, b) = gcd(b, a%b)

$$g|a, g|b$$

$$ga' = gb'q + r \Rightarrow r = g(a' - b'q) \Rightarrow g|r$$

Equação Diofantina

- A equação diofantina é a equação da forma:
  $ax + by = c$, onde a, x, b, y e c são inteiros

- Nosso objetivo é descobrir valores inteiros de x e y que satisfaçam a equação para valores dados de a, b e c.

Equação Diofantina

- Esse problema nem sempre tem solução!

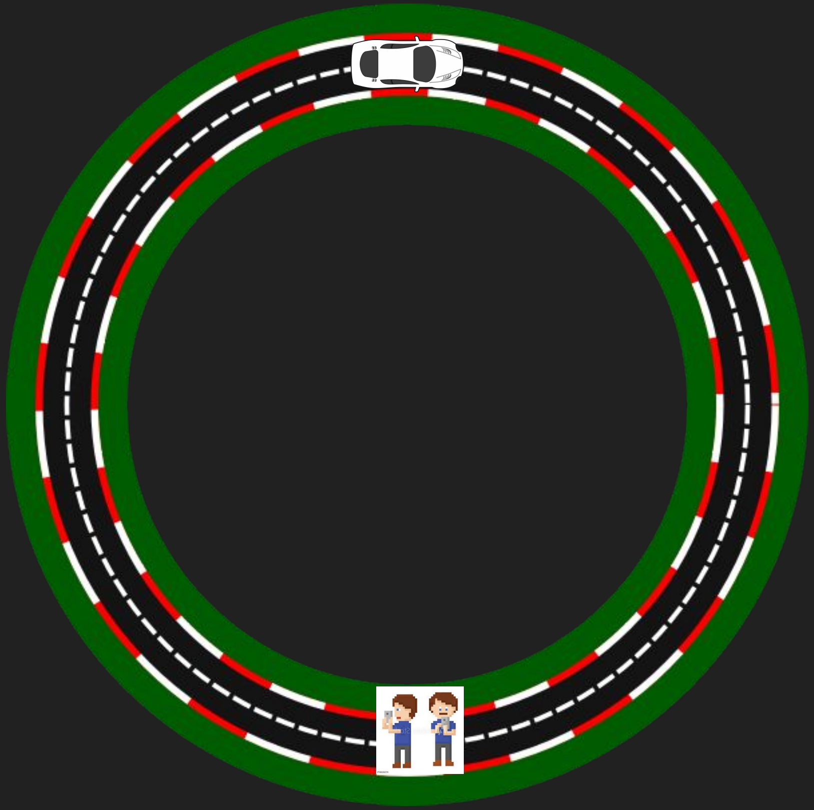
$$ax + by = c$$

Há solução <=> **c** é múltiplo de **gcd(a, b)** (Teorema de Bezout)

Equação Diofantina

- Problema

Um carro viaja numa pista circular de M metros com velocidade inteira constante em m/s. Uma pessoa tira fotos da pista a cada 1s. A pessoa irá conseguir tirar foto do carro?



Equação Diofantina

- Como encontrar uma solução?

$$ax + by = c$$

Usamos o algoritmo de euclides estendido

Equação Diofantina

- Como encontrar uma solução?

$$ax + by = c$$

Usamos o algoritmo de euclides estendido

Vamos na verdade achar os resultados da equação:

$$ax + by = gcd(a, b)$$

Euclides Estendido

- O algoritmo de euclides estendido manipula as tuplas (x, y) que resultam nos valores da equação de euclides, a cada etapa.

$$a = bq + r$$

$$(x_1, y_1) = (1, 0)$$

$$(x_2, y_2) = (0, 1)$$

Euclides Estendido

$$r_1 = r_2 q + r_3 \iff r_3 = r_1 - r_2 q$$

$$r_1 = x_1 a + y_1 b$$

$$r_2 = x_2 a + y_2 b$$

$$r_3 = ?a + ?b$$

Euclides Estendido

$$r_1 = r_2 q + r_3 \iff r_3 = r_1 - r_2 q$$

$$r_1 = x_1 a + y_1 b$$

$$x_3 a + y_3 b = x_1 a + y_1 b - (x_2 a - y_2 b) q$$

$$r_2 = x_2 a + y_2 b$$

$$r_3 = ?a + ?b$$

Euclides Estendido

$$r_1 = r_2 q + r_3 \iff r_3 = r_1 - r_2 q$$

$$r_1 = x_1 a + y_1 b$$

$$r_2 = x_2 a + y_2 b$$

$$x_3 a + y_3 b = x_1 a + y_1 b - (x_2 a - y_2 b) q$$

$$r_3 = ?a + ?b$$

$$x_3 = x_1 - x_2 q$$

$$y_3 = y_1 - y_2 q$$

Euclides Estendido

- Como encontrar todas as soluções?
- A partir de uma solução inicial, $ax_0 + by_0 = c$

$$a(x_0 + k) + b(y_0 + l) = c$$

$$ka = -bl \Rightarrow ka = lcm(a, b)$$

$$k = \frac{b}{g}, l = \frac{a}{g}$$

Problemas

- Achar pontos inteiros em uma reta cuja inclinação é um número racional
- Achar inverso modular
- Se um sapo começa na folha 0 e pula x folhas pra direita e y folhas pra esquerda, quais folhas são alcançáveis por ele?
- https://www.spoj.com/problems/CEQU/
- https://codeforces.com/gym/100812/problem/L