Lista 7: Teoria dos números & recorrências

Igor Lacerda

11 de maio de 2023

Questões Discursivas

1. d é divisor de n se n/d deixa resto 0. Alternativamente, podemos dizer que d divide n, usando a notação $d \mid n$. Podemos ainda dizer que n é múltiplo de d, que significa que existe um $c \mid d \cdot c = n$. Aqui, claro, só estamos trabalhando com inteiros.

2. Seja q o quociente e r o resto, então vale que:

$$a = b \cdot q + r$$

3. **div** e **mod** são operações relacionadas à divisão de a por b. **div** é o quociente de a por b e **mod** é o resto da divisão de a por b.

4. a e b são congruentes módulo m se, e somente se, $a - b$ deixa resto 0 por m. Alternativamente podemos dizer que $a - b$ é múltiplo de m. Ou, equivalentemente, a e b são congruentes módulo m se, e somente se, a e b deixam o mesmo resto quando divididos por m.

5. Sejam $a, b, c, d, m \in \mathbb{Z}; m > 0$. Se $a \equiv b \pmod{m} \land c \equiv d \pmod{m}$, então:

$$a + c \equiv b + d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

6. Um número primo é um número natural não nulo e diferente de 1 com a propriedade de ser divisível somente por 1 e por ele mesmo.

7. O Teorema Fundamental da Aritmética prova que qualquer inteiro positivo diferente de 1 pode ser escrito como um único (salvo de ordenações) produto de primos.

8. Seja $\pi(x)$ a função que conta todos os números primos até x:

$$\pi(x) =\mid \{1 < p \leq x : \text{p é primo}\}$$

Então o Teorema do Número Primo estabelece que:

$$\lim_{x \to \infty} \pi(x) = \left\lfloor \frac{x}{\log x} \right\rfloor$$

9. O máximo divisor comum (MDC) de dois números (inteiros) a e b é um número (inteiro) c tal que $c \mid a \wedge c \mid b \wedge \forall d > c, d \nmid a \vee \nmid b$, ou seja, é o maior número que divide simultaneamente a e b.

10. Dois números são primos entre si se seu MDC é 1.

11. Converter de uma base b_1 para uma base b_2 consiste em aplicar divisões sucessivas (parecidas com o *Algoritmo de Euclides*), em que fixamos o divisor como a nova base e trocamos os divisores pelos quocientes antecessores, terminando quando o quociente for nulo. O resultado final são os restos concatenados na ordem inversa em que foram obtidos. Vamos fazer um exemplo: converter $(53)_{10}$ para base 2:

$$\begin{aligned} 53 &= 2 \cdot 26 + 1 \\ 26 &= 2 \cdot 13 + 0 \\ 13 &= 2 \cdot 6 + 1 \\ 6 &= 2 \cdot 3 + 0 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

Ou seja, $(53)_{10} = (110101)_2$. Similarmente, poderíamos fazer:

$$\begin{aligned} 53 &= 16 \cdot 3 + 5 \\ 3 &= 16 \cdot 0 + 3 \end{aligned}$$

Assim, $(53)_{10} = (35)_{16}$

12. Existe um jeito mais simples de converter para base 10: dado um número inteiro positivo c qualquer em uma base arbitrária b, podemos convertê-lo para base 10 usando a definição de base[1]:

$$(c)_b = a_k b^k + a_{k+1} b^{k-1} + \ldots a_1 b + a_0$$

Façamos uns exemplos: que número em base 10 é $(1110001)_2$?

$$1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 = 1 + 16 + 32 + 64 = 113$$

Para a base hexadecimal é a mesma coisa, por exemplo, $(CF)_{16}$ é:

$$15 \cdot 16^0 + 12 \cdot 16^1 = 15 + 192 = 207$$

13. Usamos o **Algoritmo de Euclides** para encontrar o MDC de forma mais eficiente do que métodos tradicionais. Aplicamos divisões sucessivas até encontrar um resto nulo: neste ponto o MDC é o resto anterior. Nas divisões trocamos o dividendo pelo divisor antecedente e o divisor pelo resto antecedente. Por exemplo, qual o MDC de 1344 e 328?

$$\begin{aligned} 1344 &= 328 \cdot 4 + 32 \\ 328 &= 32 \cdot 10 + 8 \\ 32 &= 8 \cdot 4 + 0 \end{aligned}$$

Ou seja, o MDC entre esses números é 8.

[1] Aqui, k é não negativo, e os $a_0, \ldots a_n$ estão entre (inclusivamente) 0 e b

14. Se m_k é um inteiro positivo e $\gcd(m_i, m_j) = 1 \forall i \neq j$, então o sistema de congruências lineares:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots \\ x &\equiv a_{n-1} \pmod{m_{n-1}} \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Tem uma única solução: $x = X \pmod{m}$, em que $m = m_1 \cdot m_2 \cdot \ldots \cdot m_{n_1} \cdot m_n$. O valor de X pode ser encontrado utilizando-se o **Teorema Chinês dos Restos**:

$$X = a_1 \cdot M_1 \cdot x_1 + a_2 \cdot M_2 \cdot x_2 + \ldots + a_n \cdot M_n \cdot x_n$$

Em que M_a é o produto de todos os m_k com exceção de m_a e x_a é o número que torna $M_a \cdot x_a \equiv 1 \pmod{m_a}$.

15. Uma **relação de recorrência** é uma equação em que cada termo de uma sequência é definido em função dos termos anteriores (ex: sequência de Fibonacci).

16. $F(1) = 1, F(2) = 1, F(n) = F(n-1)+F(n-2)$ para $n > 2$, produzindo: 1,1,2,3,5,8...

17. **Torre de Hanói** é um quebra-cabeça que consiste em uma base contendo três pinos, em um dos quais são dispostos alguns discos uns sobre os outros, em ordem crescente de diâmetro, de cima para baixo. O problema consiste em passar todos os discos de um pino para outro qualquer, usando um dos pinos como auxiliar, de maneira que um disco maior nunca fique em cima de outro menor em nenhuma situação.

Exercícios

Sejam a e b inteiros.

1. $\forall a, a \cdot 1 = a \Rightarrow \exists c \mid a = c \cdot 1$

$$\therefore 1 \mid a \forall a$$

2. $\forall b, 0 \cdot b = 0 \Rightarrow \exists c \mid 0 = c \cdot b$

$$\therefore b \mid 0 \forall b$$

3. $0 \mid a \Rightarrow \exists c \mid a = c \cdot 0 \Rightarrow a = 0 \wedge a = 0 \Rightarrow \exists c \mid a = c \cdot 0 \Rightarrow 0 \mid a$ □

$\models \exists n \mid P = p_1 p_2 \ldots p_n + 1$ não é primo. **[3.5.34]**
Usando uma calculadora, podemos fatorar $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$, cujos fatores primos são 59 e 509.