Elementos de Matemática Discreta

Resumo

Rafael Rodrigues

LEIC
Instituto Superior Técnico
2023/2024

Contents

1 Teste 1

2 Teste 2

Congruências

1. $a + c \equiv_n b + d$
2. $a^k \equiv_n b^k \rightarrow a \equiv_n b$
3. $-$
4. $-$
5. $ac \equiv_n bc \rightarrow a \equiv_{\frac{n}{n \frown c}} b$
6. $x \equiv_{pq} a$, sse $x \equiv_p a$ e $x \equiv_q a$ com $p \frown q = 1$

2.1 Teorema Chinês do Resto

1. Escrever o sistema na forma normal

$$\begin{cases} x \equiv_{c_1} a_1 \\ x \equiv_{c_2} a_2 \\ x \equiv_{c_3} a_3 \end{cases}$$

2. Verificar se os módulos são primos entre si
   (a) caso sejam:
      i. $M = \prod c_i$
   (b) caso não sejam:
      i. Verificar se $a_i - a_j = xt$ para $x = gcd(c_i, c_j)$
      ii. $M = lcm(c_1, ..., c_k)$
      iii. Fatorizar M e utilizar cada um dos fatores como novo c_i
3. Aplicar o algoritmo
   (a) Construir a tabela:

a_i	c_i	n_i	$mod(n_i, c_i)$	$\tilde{n}_i$	$a_i n_i \tilde{n}_i$
		$c_2 \times c_3$			
		$c_1 \times c_3$			
		$c_1 \times c_2$			

   (b) Calcular a solução particular: $x_0 = \sum a_i n_i \tilde{n}_i$
   (c) Calcular a solução geral: $x = x_0 + Mk$, com $k \in \mathbb{Z}$.
   (d) Escolher a solução que se enquadra no problema.

2.2 Algoritmo RSA

1. Criar as chaves, usando dois números primos diferentes p e q:
   - Chave pública (N, e)
   - Chave privada (N, d)

   (a) $N = p \times q$

   (b) Para encontrar e ou d resolver equação diofantina: $1 = (e \times d) + [(p-1)(q-1) \times k]$
2. Encriptar mensagem M usando a chave pública: $M^e \equiv_N R$
3. Desencriptar mensagem R usando a chave privada: $R^d \equiv_N M$

Algoritmo de Saunderson

a_i	q_i	x_i	y_i
100		1	0
49	2	0	1
2	24	1	-2
1	2	-24	49
0			

$$x_{i+1} = x_{i-1} - q_i x_i$$

$$y_{i+1} = y_{i-1} - q_i y_i$$

2.3 Equações Diofantinas

1. Escrever equação diofantina: $(\ )x \pm (\ )y =$

2.4 Pequeno Teorema de Fermat

3 Teste 3

3.1 Funções Geradoras

3.2 Algoritmo FFT

3.3 Grafos

3.3.1 Algoritmo de Kruskal

3.3.2 Algoritmo de Dijkstra

3.3.3 Teorema de Kuratowski