

UNIVERSIDADE DE SÃO PAULO

TRABALHO DE FORMATURA

---

# Teoria dos Números e Computação: Uma abordagem utilizando problemas de competições de programação

---

*Autor:*

Antonio R. de Campos Junior

*Supervisor:*

Dr. Carlos Eduardo Ferreira

*Tese apresentada em cumprimento dos requisitos para o curso  
Bacharel em Ciência da Computação*

Instituto de Matemática e Estatística

29 de novembro de 2015

*“To raise new questions, new possibilities, to regard old problems from a new angle, requires creative imagination and marks real advance in science.”*

Albert Einstein

# Resumo

Teoria dos Números é um vasto ramo da matemática que estuda números inteiros. Números primos, fatorização de números inteiros, funções aritméticas, são alguns dos tópicos mais estudados e também importantes para resolução de problemas computacionais.

Hoje em dia a importância da Teoria dos Números na Computação é inquestionável, e desse modo, esse trabalho vem ilustrar como a teoria pode ser aplicada na criação de algoritmos para resolução de problemas computacionais, em especial problemas de competições de programação.

Equações diofantinas, Congruência Modular, Números de Fibonacci, são alguns dos assuntos que serão abordados nesse trabalho. Após a devida demonstração da teoria serão exibidos alguns problemas de competições de programação que aplicam essa teoria, seguido da implementação e análise do algoritmo que resolve o problema abordado.



# Agradecimentos

Gostaria de agradecer ao doutorando *Renzo Gonzalo Gomez Diaz* pelo auxílio na revisão dos textos e na seleção dos problemas. E um agradecimento especial ao Professor Doutor *Carlos Eduardo Ferreira* pelo suporte durante todo o desenvolvimento desse trabalho.



# Sumário

<b>1</b>	<b>Divisibilidade</b>	<b>1</b>
1.1	Introdução	1
1.1.1	Divisores	2
1.2	Números Primos	3
1.3	Máximo Divisor Comum	3
1.3.1	Algoritmo de Euclides	4
1.3.2	Teorema de Bézout	4
1.4	Crivo de Erastóteles	5
1.5	Equações Diofantinas	6
1.5.1	Algoritmo de Euclides Extendido	7
1.6	Problemas Propostos	8
1.6.1	UVA-543	8
1.6.2	CodeChef-GOC203	8
1.6.3	UVA-10407	9
1.6.4	CodeChef-MAANDI	9
1.6.5	UVA-10090	9
1.6.6	UVA-718	11
<b>2</b>	<b>Aritmética Modular</b>	<b>15</b>
2.1	Congruência	15
2.2	Congruência Linear	16
2.3	Teoremas de Fermat e de Wilson	16
2.3.1	Teorema de Fermat	16
2.3.2	Inverso Multiplicativo Modular	17
2.3.3	Teorema de Wilson	17
2.4	Exponenciação	18
2.4.1	Exponenciação Binária	18
2.4.2	Exponenciação Binária Modular	18
2.4.3	Exponenciação de Matriz	18
2.5	Problemas Propostos	20
2.5.1	SPOJ-DCEPC11B	20
2.5.2	CodeChef-IITK2P10	21
2.5.3	CodeChef-CSUMD	21
<b>3</b>	<b>Funções Aritméticas</b>	<b>25</b>
3.1	$\Phi$ de Euler	25
3.1.1	Algoritmo $\Phi$ de Euler	26
3.1.2	Teorema de Euler	26
3.2	Sequência de Fibonacci	27
3.3	Problemas Propostos	28
3.3.1	UVA-11424	28
3.3.2	TJU-3506	29

3.3.3	CodeChef-IITK2P05 . . . . .	30
3.3.4	CodeChef-PUPPYGCD . . . . .	30
3.3.5	CodeChef-MODEFB . . . . .	32
3.3.6	Codeforces-227E . . . . .	33
<b>4</b>	<b>Conclusão</b>	<b>35</b>
<b>A</b>	<b>Curiosidades da ACM-ICPC</b>	<b>37</b>
<b>B</b>	<b>Juízes Online (Online Judges)</b>	<b>39</b>
B.1	Ahmed-Aly . . . . .	39
B.2	UVa . . . . .	39
B.3	URI . . . . .	39
B.4	Topcoder . . . . .	39
B.5	Codeforces . . . . .	40
B.6	CodeChef . . . . .	40
	<b>Bibliografia</b>	<b>41</b>



# Lista de Figuras

A.1 Crescimento do número de participantes por ano. . . . .	37
---	----



# Lista de Tabelas



# Capítulo 1

## Divisibilidade

### 1.1 Introdução

A noção de divisibilidade dos números inteiros é fundamental na **Teoria dos Números**. Nesse seção vamos descrever algumas definições e propriedades que serão utilizados ao longo desse trabalho.

**Definição 1** A notação  $d|n$  ("*d divide n*"), significa que existe um inteiro  $q$ , tal que,  $n = dq$ . Se  $d|n$  dizemos que  $n$  é múltiplo de  $d$ . Caso  $n$  não seja múltiplo de  $d$  (ou seja,  $d$  não divide  $n$ ), escrevemos  $d \nmid n$ .

**Definição 2** A notação  $d \bmod n$  ("*d módulo n*"), significa o resto da divisão de  $d$  por  $n$ .

**Proposição 1**  $d|n, d|m \Rightarrow d|(n + m)$

**Demonstração:** Se  $d|n$  e  $d|m$ , então existe inteiros  $q$  e  $k$ , tal que,  $n = qd$  e  $m = kd$ . Desse modo temos:

$$(n + m) = qd + kd = (q + k)d \Rightarrow d|(n + m) \quad \square$$

**Proposição 2**  $d|(\frac{n}{m}) \Rightarrow dm|n$

**Demonstração:**

$$d|(\frac{n}{m}) \Rightarrow \exists q \in \mathbb{Z} \mid \frac{n}{m} = qd$$

$$d|(\frac{n}{m}) \Rightarrow n = q(dm) \Rightarrow dm|n \quad \square$$

**Corolário 1** Dado um subconjunto dos inteiros  $S = \{S_1, S_2, S_3, \dots, S_n\}$  ordenado crescentemente, e um número inteiro  $d$ , tal que,  $d|(S_i - S_{i-1})$ ,  $2 \leq i \leq n$ , temos que:

$$d|(S_i - S_j), \forall S_i, S_j \in S.$$

**Demonstração:** Tome  $S_i, S_j \in S$  quaisquer, e sem perda de generalidade assumamos que  $S_i \geq S_j$  (ie,  $i \geq j$ , pois  $S$  está ordenado crescentemente).

Como  $i \geq j$ , tome  $r \in \mathbb{N}$  como sendo a diferença entre  $i$  e  $j$ :  $i = j + r$ .

Vamos agora provar por indução que  $d|(S_{j+r} - S_j)$ .

Para  $r = 0$  ou  $r = 1$  a demonstração segue trivialmente.

Assumamos que o corolário funciona para  $(r - 1)$ , ie,  $d|(S_{j+r-1} - S_j)$ .

Temos então que:

$$d|(S_{j+r} - S_{j+r-1}) \Rightarrow d|(S_{j+r} - S_{j+r-1}) + (S_{j+r-1} - S_j) \quad (\triangleright \text{Proposição 1})$$

$$d|(S_{j+r} - S_{j+r-1}) \Rightarrow d|(S_{j+r} - S_j) \quad \square$$

**Corolário 2** O **Corolário 1** funciona mesmo se o conjunto  $S$  não estiver ordenado.

**Demonstração:** Deixaremos a demonstração a cargo do leitor.

**Teorema 1 (Teorema da Divisão)** Para todo número inteiro  $a$  e qualquer número inteiro positivo  $n$ , existe inteiros únicos  $q$  e  $r$ , tal que:

$$a = qn + r, 0 \leq r < n$$

O valor  $q$  ( $q = \lfloor \frac{a}{n} \rfloor$ ) é chamado de **quociente** da divisão, e o valor  $r$  ( $r = a \bmod n$ ) é chamado de **resto** (ou **resíduo**) da divisão.

**Demonstração:** Suponha que  $q$  e  $r$  não sejam únicos, ie, que exista  $q^*$  e  $r^*$  tal que:  
 $a = q^*n + r^*, 0 \leq r^* < n$ .

$$a = qn + r = q^*n + r^* \Rightarrow (r - r^*) = (q^* - q)n \Rightarrow n|(r - r^*) \text{ já que } n|(q^* - q)n.$$

Porém, como  $r \neq r^*$ , e tanto  $r$  quanto  $r^*$  são menores que  $n$ , temos que:

$$(r \bmod n) \neq (r^* \bmod n) \Rightarrow n \nmid (r - r^*).$$

Chegando numa contradição, e assim  $q$  e  $r$  são únicos  $\square$

**Corolário 3**  $d|n, d|m \Rightarrow d|(n \bmod m)$

**Demonstração:**

$$d|n \Rightarrow n = k_1d, k_1 \in \mathbb{Z}$$

$$d|m \Rightarrow m = k_2d, k_2 \in \mathbb{Z}$$

$$n = qm + (n \bmod m) \Rightarrow (n \bmod m) = n - qm \text{ (} \triangleright \text{ Teorema 1)}$$

$$(n \bmod m) = k_1d - qk_2d = (k_1 - qk_2)d \Rightarrow d|(n \bmod m) \square$$

**Corolário 4**  $d|m, d|(n \bmod m) \Rightarrow d|n$

**Demonstração:**

$$d|m \Rightarrow m = k_1d, k_1 \in \mathbb{Z}$$

$$d|(n \bmod m) \Rightarrow (n \bmod m) = k_2d, k_2 \in \mathbb{Z}$$

$$n = qm + (n \bmod m) \Rightarrow n = qk_1d + k_2d \text{ (} \triangleright \text{ Teorema 1)}$$

$$n = (qk_1 + k_2)d \Rightarrow d|n \square$$

### 1.1.1 Divisores

Nessa subseção mostraremos um algoritmo simples para calcular todos os divisores de um determinado número inteiro positivo qualquer.

**Teorema 2** O número de divisores de  $n \in \mathbb{Z}^+$  é da ordem de  $O(\sqrt{n})$ .

**Demonstração:** Tome um divisor  $d$  de  $n$  qualquer, com  $d > \sqrt{n}$ . Dessa forma sabemos que existe um inteiro  $q$ , com  $n = qd$  (observe que  $q$  também é divisor de  $n$ ). Como  $d > \sqrt{n}$  então  $q < \sqrt{n}$ . Assim, para qualquer divisor  $d$  de  $n$  maior que  $\sqrt{n}$ , existe exatamente um divisor  $q$  de  $n$  menor que  $\sqrt{n}$  correspondente ao mesmo. O que implica que só existe no máximo  $\sqrt{n}$  divisores maiores que  $\sqrt{n}$ . Por outro lado, claramente só existem  $\sqrt{n}$  divisores menores que  $\sqrt{n}$ . Concluimos então que o número total de divisores de  $n$  é da ordem de  $O(\sqrt{n})$ .  $\square$

**Pseudocódigo:****Algorithm 1** Encontra todos os divisores de  $N$ 


---

```

1: procedure FINDDIVISORS ( $N$ )
2:    $D \leftarrow \emptyset$  ▷ Conjunto  $D$  contém os divisores de  $N$ 
3:   for ( $d = 1; d^2 \leq N; d++$ ) do
4:     if  $d \nmid N$  then
5:       continue
6:      $D \leftarrow D \cup \{d\}$ 
7:      $q \leftarrow \frac{N}{d}$ 
8:     if  $q \neq d$  then
9:        $D \leftarrow D \cup \{q\}$ 
10:  return  $D$ 

```

---

**Análise:** O laço da linha 3 consome tempo  $O(\sqrt{N})$ , testando se os números menores que  $\sqrt{N}$  são divisores. Na linha 7 são calculados os divisores correspondentes maiores que  $\sqrt{N}$ . E a condição da linha 8 garante que se  $N$  for quadrado perfeito, então é inserido  $\sqrt{N}$  somente uma vez no conjunto  $D$ . Assim a complexidade total do algoritmo é  $O(\sqrt{N})$ .

## 1.2 Números Primos

**Definição 3** Todo número inteiro  $n$  ( $n > 1$ ) que têm apenas dois divisores distintos (1 e  $n$ ) é chamado de número primo. Se  $n$  ( $n > 1$ ) não for primo, dizemos que  $n$  é número composto.

**Teorema 3 (Fatoração Única)** Um número natural qualquer  $n$ , pode ser escrito unicamente como um produto da forma:  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ , onde os  $p_i$  são números primos,  $p_1 < p_2 < \dots < p_k$ , e os números  $a_i$  são inteiros positivos.

**Demonstração:** Deixaremos a demonstração a cargo do leitor. **Dica:** Use o fato de que o conjunto dos primos que divide um número inteiro é único, e o fato de que se qualquer potência  $a_i$  for alterado o valor de  $n$  será alterado.

## 1.3 Máximo Divisor Comum

**Definição 4** O Máximo Divisor Comum de dois inteiros quaisquer  $a$  e  $b$  (com  $a$  ou  $b$  diferente de zero), denotado por  $MDC(a, b)$ , é o maior inteiro que divide ambos  $a$  e  $b$ . Se  $MDC(a, b) = 1$  dizemos que  $a$  e  $b$  são primos entre si.

**Corolário 5** Para números inteiros quaisquer  $a$  e  $b$ ,  $MDC(a, b) = MDC(b, a \bmod b)$

**Demonstração:** Pelo Corolário 3 e 4, temos:

$$d|a, d|b \Leftrightarrow d|b, d|(a \bmod b)$$

Assim, qualquer divisor de  $a$  e  $b$  é também divisor de  $b$  e  $(a \bmod b)$  (e vice versa). Implicando que o Máximo Divisor Comum de  $a$  e  $b$  é igual ao Máximo Divisor Comum de  $b$  e  $(a \bmod b)$ .  $\square$

**Corolário 6**  $MDC(a, b) = d \Rightarrow MDC(\frac{a}{d}, \frac{b}{d}) = 1$

**Demonstração:** Suponha que  $MDC(\frac{a}{d}, \frac{b}{d}) = r > 1$ . Assim temos:

$$r \mid \frac{a}{d} \Rightarrow dr \mid a \text{ (}\triangleright \text{Proposição 2)}$$

$$r \mid \frac{b}{d} \Rightarrow dr \mid b \text{ (}\triangleright \text{Proposição 2)}$$

$$r > 1 \Rightarrow dr > d \Rightarrow dr > MDC(a, b)$$

Chegamos então numa contradição, pois  $dr$  é divisor comum de  $a$  e  $b$ , e  $dr$  é maior que o **Máximo Divisor Comum** de  $a$  e  $b$ .  $\square$

**Corolário 7** Para números inteiros quaisquer  $a$  e  $b$ ,  $MDC(a, b) = MDC(a, a \pm b)$

**Demonstração:** A prova dessa expressão vem do fato de que qualquer divisor de  $a$  e  $b$ , é também divisor de  $(a \pm b)$ .

**Corolário 8** Para números inteiros quaisquer  $a$  e  $b$ , temos:

$$MDC(a, b) = 1 \Rightarrow MDC(a, bk) = MDC(a, k), \text{ com } k \in \mathbb{Z}$$

**Demonstração:** A prova dessa expressão vem do fato de que qualquer divisor  $d$  de  $a$  e  $b$ , é também divisor de  $k$ , pois  $d$  não divide  $b$  ( $MDC(a, b) = 1$ ).

**Corolário 9**  $MDC((p-1)!, p) = 1$ , para  $p$  primo qualquer.

**Demonstração:** Tome um inteiro positivo  $d < p$ . Como  $p$  é primo, sabemos que  $MDC(p, d) = 1$ , ie,  $d$  não tem nenhum fator primo em comum com  $p$ . Assim o produto  $(p-1)!$  de todos os inteiros positivos menores que  $p$  também não terá nenhum fator primo em comum com  $p$ .  $\square$

### 1.3.1 Algoritmo de Euclides

A ideia principal do **Algoritmo de Euclides** é calcular recursivamente o **Máximo Divisor Comum** de dois números baseando-se no **Corolário 5**.

**Pseudocódigo:**

---

**Algorithm 2** Algoritmo de Euclides

---

```

1: procedure  $MDC(a, b)$ 
2:   if  $a = 0$  then
3:     return  $b$ 
4:   return  $MDC(b \bmod a, a)$ 

```

---

**Análise:** O *Algoritmo de Euclides* consome tempo proporcional à  $O(\log b)$ . Para provar a análise do custo do algoritmo é preciso conhecer algumas propriedades da *Sequência de Fibonacci*, e desse modo, a demonstração será feita no **Capítulo 3, Subseção 3.2**.

### 1.3.2 Teorema de Bézout

**Corolário 10** Dado o conjunto de combinações lineares positivas  $S := \{x \in \mathbb{Z}, x > 0 \mid x = ma + nb, m, n \in \mathbb{Z}\}$ , onde os números  $a$  e  $b$  são inteiros, e pelo menos um desses números é diferente de zero. Temos então que  $S \neq \emptyset$ .



**Demonstração:** As combinações possíveis para  $a$  e  $b$  são:

$$a > 0 \Rightarrow |a| = 1.a + 0.b$$

$$a < 0 \Rightarrow |a| = (-1).a + 0.b$$

$$b > 0 \Rightarrow |b| = 0.a + 1.b$$

$$b < 0 \Rightarrow |b| = 0.a + (-1).b$$

Como não temos ambos  $a$  e  $b$  iguais à zero, então  $S$  deve conter pelo menos  $|a|$  ou  $|b|$ , e assim  $S \neq \emptyset$   $\square$

**Corolário 11** Dado o conjunto de combinações lineares positivas  $S := \{x \in \mathbb{Z}, x > 0 \mid x = ma + nb, m, n \in \mathbb{Z}\}$ , onde os números  $a$  e  $b$  são inteiros, e pelo menos um desses números é diferente de zero. Temos então que o menor número  $d \in S$  divide todos elementos de  $S$ .

**Demonstração:** Como  $d \in S$ ,  $\exists m, n \in \mathbb{Z} \mid d = ma + nb$ .

Tome  $x \in S$  qualquer. Pelo **Teorema 1**  $x = qd + r$ ,  $0 \leq r < d$ .

Suponha que  $d \nmid x$ , ie,  $x \neq qd$  e  $0 < r$ . Como  $x \in S$ ,  $\exists m^*, n^* \in \mathbb{Z} \mid x = m^*a + n^*b$ , e assim:

$$x = m^*a + n^*b, x = qd + r \Rightarrow r = m^*a + n^*b - qd = m^*a + n^*b - q(ma + nb)$$

$$\Rightarrow r = (m^* - qm)a + (n^* - qn)b \Rightarrow r \in S, \text{ pois } r > 0$$

Chegando numa contrdição, pois  $r \in S$ ,  $d \in S$ ,  $r < d$  e  $d$  é o menor elemento em  $S$ .

Desse modo, temos que  $d$  divide todos os elementos de  $S$ .  $\square$

**Teorema 4 (Teorema de Bézout)**  $\forall a, b \in \mathbb{Z}$  (com pelo menos um dos dois números diferente de zero),  $\exists x, y \in \mathbb{Z} \mid ax + by = \text{mdc}(a, b)$ .

**Demonstração:** Tome o conjunto das combinações lineares de  $a$  e  $b$ :

$$S := \{x \in \mathbb{Z}, x > 0 \mid x = ma + nb, m, n \in \mathbb{Z}\}.$$

Pelo **Corolário 10** sabemos que  $S \neq \emptyset$ . Como  $S$  contém somente números positivos e não é vazio,  $S$  está limitado inferiormente por zero e assim,  $S$  tem um elemento mínimo que chamaremos de  $d$ .

Como  $d \in S$ , então existe  $u, v \in \mathbb{Z}$ , tal que,  $d = ua + vb$ . Pelo **Corolário 11**, sabemos que  $d$  divide todos elementos em  $S$ , em particular:

$$d \text{ divide } |a| \text{ e } |b| \Rightarrow d \mid \text{MDC}(a, b) \Rightarrow 0 < d \leq \text{MDC}(a, b)$$

Por outro lado,  $\text{MDC}(a, b)$  também divide  $a$  e  $b$ :

$$\text{MDC}(a, b) \mid a \text{ e } \text{MDC}(a, b) \mid b \Rightarrow \text{MDC}(a, b) \mid (ua + vb)$$

$$\Rightarrow \text{MDC}(a, b) \mid d \Rightarrow \text{MDC}(a, b) \leq d$$

$$\text{MDC}(a, b) \leq d \text{ e } d \leq \text{MDC}(a, b) \Rightarrow \text{MDC}(a, b) = d \Rightarrow \text{MDC}(a, b) \in S \quad \square$$

## 1.4 Crivo de Erastóteles

O *Crivo de Erastóteles* é um algoritmo criado pelo matemático **Erastótenes** (a.C. 285-194 a.C.) para o cálculo de números primos até um certo valor limite  $N$ . O algoritmo mantém uma tabela com  $N$  elementos, e para cada primo, começando pelo número 2, marca na tabela os números compostos múltiplos desses primos. Desse modo, ao final do algoritmo, os elementos não marcados são números primos.

**Pseudocódigo:****Algorithm 3** Crivo de Erastótenes para o cálculo de números primos

---

```

1: procedure CRIVOERASTÓTENES (N)
2:    $isPrime[] \leftarrow \text{new Array}[N]$   $\triangleright isPrime[]$  é um vetor booleano
3:
4:   for ( $p = 2; p \leq N; p++$ ) do
5:      $isPrime[p] \leftarrow \text{true}$ 
6:
7:   for ( $p = 2; p^2 \leq N; p++$ ) do
8:     if  $isPrime[p] = \text{false}$  then
9:       continue
10:    for ( $n = p^2; n \leq N; n = n + p$ ) do
11:       $isPrime[n] \leftarrow \text{false}$ 
12:
13:   return  $isPrime[]$ 

```

---

**Análise:** O laço da linha 4 itera sobre todos os valores de 2 até  $N$  e assim consome tempo  $O(N)$ . Já o laço mais interno na linha 9 itera sobre de  $p^2$  até  $N$  múltiplos de  $p$ , e assim consome tempo  $O(N/p)$ .

Desse modo a complexidade conjunta dos laços das linhas 6 e 9, será  $O(\sum_{p \text{ primo} \mid p \leq \sqrt{N}} \frac{1}{p})$  (observe que o laço da linha 6 itera sobre os primos menores que  $\sqrt{N}$ ).

Como foi sugerido por *Leonhard Euler* no século XVIII, temos que  $\sum_{p \text{ primo} \mid p \leq \sqrt{N}} \frac{1}{p} = O(N \log \log N)$ . E assim a complexidade final do algoritmo é  $O(N \log \log N)$ .

## 1.5 Equações Diofantinas

*Equações Diofantinas* são equações polinomiais com variáveis inteiras. Alguns exemplos são mostrados a seguir, sendo  $x, y, z$  incógnitas, e  $a, b, n$  constantes inteiras:

$$ax + by = n \quad (\triangleright \text{Equação Diofantina Linear})$$

$$ax + by = \text{MDC}(a, b) \quad (\triangleright \text{Identidade de Bézout})$$

$$x^n + y^n = z^n \quad (\triangleright \text{Equação base do Último Teorema de Fermat})$$

$$x^2 - ny^2 = \pm 1 \quad (\triangleright \text{Equação de Pell})$$

Nesse trabalho abordaremos somente *Equações Diofantinas Lineares*, da forma:

$$\sum_{i=1}^k a_i x_i = c$$

onde  $c$  e  $a_i$  são constantes, e  $x_i$  variáveis inteiras.

**Teorema 5** Dados inteiros  $a, b, c$ , temos que:

$$\text{MDC}(a, b) \mid c \Leftrightarrow \text{a Equação Diofantina } ax + by = c, \text{ tem solução inteira.}$$

**Demonstração:** Provaremos primeiro a ida da implicação.

Pelo **Teorema 4** sabemos que existe  $x^*$  e  $y^*$ , tal que,  $ax^* + by^* = \text{MDC}(a, b)$ . Logo:

$$\text{MDC}(a, b) \mid c \Rightarrow \exists! q \in \mathbb{Z} \mid c = \text{MDC}(a, b)q \Rightarrow a(x^*q) + b(y^*q) = \text{MDC}(a, b)q = c \quad \square$$

Provaremos agora a volta da implicação.

Sabemos que existe inteiros  $u$  e  $v$ , tal que,  $a = \text{MDC}(a, b)u$  e  $b = \text{MDC}(a, b)v$ . Logo:

$$ax + by = c, \text{ tem solução inteira} \Rightarrow \text{MDC}(a, b)ux + \text{MDC}(a, b)vy = c$$

$$\Rightarrow \text{MDC}(a, b)(ux + vy) = c \Rightarrow \text{MDC}(a, b) \mid c. \quad \square$$

### 1.5.1 Algoritmo de Euclides Extendido

*Algoritmo de Euclides Extendido* é uma extensão do *Algoritmo de Euclides* que calcula não só o  $MDC(a, b)$ , para dados  $a$  e  $b$ , mas também encontra uma solução para a *Identidade de Bézout*  $ax + by = MDC(a, b)$ .

**Pseudocódigo:**

---

**Algorithm 4** Algoritmo de Euclides Extendido

---

```

1: procedure ExtendedMDC( $a, b$ )
2:   if  $a = 0$  then
3:     return  $[b, 0, 1]$ 
4:
5:    $[d, x, y] \leftarrow \text{ExtendedMDC}(b \bmod a, a)$ 
6:    $x^* \leftarrow y - \lfloor \frac{b}{a} \rfloor x$ 
7:    $y^* \leftarrow x$ 
8:   return  $[d, x^*, y^*]$ 

```

---

**Análise:** Em vez de retornar um inteiro,  $\text{ExtendedMDC}(a, b)$  retorna uma tupla  $[d, x, y]$ , onde  $d = MDC(a, b)$  e  $x, y$  são a solução da equação  $ax + by = d = MDC(a, b)$ . Sabemos que  $[d, x, y]$  na linha 5 satisfaz a equação,  $(b \bmod a)x + ay = d$ , assim:

$$(b \bmod a)x + ay = d \Rightarrow (b - \lfloor \frac{b}{a} \rfloor a)x + ay = d$$

$$\Rightarrow a(y - \lfloor \frac{b}{a} \rfloor x) + b(x) = ax^* + by^* = d = MDC(a, b)$$

Observe que o *Algoritmo de Euclides Extendido* é baseado no *Algoritmo de Euclides*, tendo a mesma complexidade  $O(\log(a + b))$ .

**Corolário 12** Tome  $[d, x_0, y_0]$  como sendo a tupla retornada pelo  $\text{ExtendedMDC}(a, b)$ , com  $a, b, c$  inteiros e  $MDC(a, b) | c$ . Então temos que todas as soluções da equação  $ax + by = c$  são da forma:  $x = (x_0 \frac{c}{d} + \frac{bq}{d})$ ,  $y = (y_0 \frac{c}{d} - \frac{aq}{d})$ , em que  $q \in \mathbb{Z}$ .

**Demonstração:** Pelo *Algoritmo de Euclides Extendido* sabemos que  $ax_0 + by_0 = d$ . Sabemos também que  $d | c$  por definição, ie, existe  $k \in \mathbb{Z}$  tal que  $c = kd$ . Assim temos que  $x = x_0k$  e  $y = y_0k$  é solução, já que  $a(x_0k) + b(y_0k) = kd = c$ .

Agora tome a solução  $x^*, y^*$  qualquer ( $ax^* + by^* = c$ ). Subtraindo as últimas duas equações temos:

$$a(x_0k - x^*) + b(y_0k - y^*) = 0 \Rightarrow a(x_0k - x^*) = b(y^* - y_0k) \Rightarrow a | [b(y^* - y_0k)]$$

$$\Rightarrow \frac{a}{MDC(a, b)} | (y^* - y_0k) \Rightarrow \exists! q \in \mathbb{Z}, \text{ tal que } \frac{a}{MDC(a, b)} q = (y^* - y_0k)$$

$$\Rightarrow y^* = y_0k + \frac{a}{MDC(a, b)} q \Rightarrow y^* = y_0 \frac{c}{d} - \frac{aq}{d}$$

$$\text{Analogamente, temos: } x^* = x_0 \frac{c}{d} + \frac{bq}{d}$$

Assim todas as soluções de  $ax + by = c$  são da forma:  $x = x_0 \frac{c}{d} + \frac{bq}{d}$ ,  $y = y_0 \frac{c}{d} - \frac{aq}{d}$   $\square$

## 1.6 Problemas Propostos

### 1.6.1 UVA-543

#### 543 - Goldbach's Conjecture

**Resumo:** É dado um número inteiro  $n$  ( $6 \leq n < 10^6$ ). O problema consiste em verificar se  $n$  pode ser escrito como a soma de dois números primos ímpares. E em caso positivo dizer quais são esses primos.

**Solução:** Para resolver esse problema basta rodar o **Algoritmo 3** para  $N = n$ , e fazer uma varredura linear no vetor  $isPrime[]$ . Se existir um índice  $a$  ( $6 \leq a \leq n$ ) tal que  $isPrime[a]$  é *true* e  $isPrime[n-a]$  também é *true*, então o problema acima tem solução.

**Pseudocódigo:**

---

#### Algorithm 5 Sum of odd primes

---

```

1: procedure SumOfPrimes( $n$ )
2:    $isPrime[] \leftarrow CrivoErastotenes(n)$ 
3:
4:   for  $i := 6$  to  $n$  do
5:     if  $isPrime[i]$  e  $isPrime[n-i]$  then
6:       return  $[i, n-i]$ 
7:
8:   return "No Solution"
```

---

**Análise:** O *Crivo de Erastótenes* consome tempo proporcional a  $O(n \log \log n)$ , e o laço na linha 4 consome tempo  $O(n)$ . Assim a complexidade do algoritmo  $SumOfPrimes(n)$  é  $O(n \log \log n)$ .

### 1.6.2 CodeChef-GOC203

#### GOC203 - Fight for Attendance

**Resumo:** São dados inteiros  $a, b, c$  ( $1 \leq a, b, c \leq 10^6$ ) e a equação  $ax + by = c$ . O problema consiste em determinar quando tal equação tem solução inteira.

**Solução:** Solução é decorrente do **Teorema 5**, bastando checar se  $MDC(a, b) | c$ .

**Pseudocódigo:**

---

#### Algorithm 6 Fight for Attendance

---

```

1: procedure EquationSolution( $a, b, c$ )
2:   if  $MDC(a, b) | c$  then
3:     return true
4:   return false
```

---

**Análise:** O algoritmo tem a mesma complexidade do *Algoritmo de Euclides*,  $O(\log(a + b))$ .

### 1.6.3 UVA-10407

#### 10407 - Simple Division

**Resumo:** Tome  $P(S) := \{x \in \mathbb{Z} \mid \forall a, b \in S, a \equiv b \pmod{x}\}$  em que  $S \subset \mathbb{Z}$ .

O problema consiste em encontrar o valor máximo de  $P(S)$  dado um conjunto  $S$ .

**Solução:** Seja  $S = \{S_1, S_2, S_3, \dots, S_n\}$ , com  $n = |S|$ , o conjunto dado pelo problema (assumiremos que os valores de  $S$  estão ordenados crescentemente).

Tome um número qualquer  $d \in P(S)$ . Por definição temos que  $\forall S_i, S_j \in S, S_i \equiv S_j \pmod{d} \Rightarrow (S_i - S_j) \equiv 0 \pmod{d} \Rightarrow d \mid (S_i - S_j)$ .

Pelo **Corolário 1** sabemos que:

$$d \mid (S_i - S_{i-1}), \forall i \in \mathbb{N}, 2 \leq i \leq n \Rightarrow d \mid (S_i - S_j), \forall S_i, S_j \in S \Rightarrow d \in P(S).$$

E desse modo, para calcular o valor máximo de  $P(S)$  só precisamos calcular o Máximo Divisor Comum das diferenças  $(S_i - S_{i-1})$  com  $i$  variando de 2 à  $n$ .  $\square$

**Pseudocódigo:**

---

#### Algorithm 7 Simple Division

---

```

1: procedure GETMAXIMUMVALUE (S)
2:    $S \leftarrow \text{sort}(S)$  ▷ sort(X) retorna o conjunto X ordenado.
3:    $\text{maxValue} \leftarrow 0$ 
4:   for  $i := 2$  to  $|S|$  do
5:      $\text{maxValue} \leftarrow \text{MDC}(\text{maxValue}, S_i - S_{i-1})$ 
6:   return  $\text{maxValue}$ 

```

---

**Análise:** Pelo **Corolário 2** sabemos que não é preciso o conjunto  $S$  ser ordenado. Assim a complexidade do algoritmo final será  $O(|S| \log(\max(S_i - S_{i-1})))$ .

### 1.6.4 CodeChef-MAANDI

#### MAANDI - Maxim and Dividers

**Resumo:** Calcular quantos divisores de um número inteiro  $n$  ( $1 \leq n \leq 10^9$ ), contém os dígitos 4 e 7 na forma decimal. Por exemplo, para  $n = 94$  os únicos divisores que contém tais dígitos são: 47, 94.

**Solução:** Para esse problema, basta calcular todos os divisores de  $n$ , com o **Algoritmo 1**, e depois verificar quais deles contém os dígitos 4 ou 7.

**Pseudocódigo:**

**Análise:** O laço da linha 5 roda em tempo  $O(\sqrt{n})$ , já que o número de elementos em  $D$  é da ordem de  $O(\sqrt{N})$ . O número de dígitos de cada divisor  $d$  é da ordem de  $O(\log_{10} d)$ , ou melhor  $O(\log n)$ . Assim o laço da linha 8 consome tempo proporcional à  $O(\log n)$  e a complexidade total do algoritmo é  $O(\sqrt{n} \log n)$ .

### 1.6.5 UVA-10090

#### 10090 - Marbles

**Resumo:** É dado um inteiro  $n$  ( $1 < n \leq 2 \cdot 10^9$ ) que corresponde ao número de bolinhas disponíveis que serão colocadas em caixas. São dados também dois tipos de

**Algorithm 8** Maxim and Dividers

---

```

1: procedure FINDOVERLUCKIDIVISORS (N)
2:    $D \leftarrow \text{FindDivisors}(n)$ 
3:    $count \leftarrow 0$ 
4:
5:   for each  $d \in D$  do
6:      $hasDigits \leftarrow false$ 
7:
8:     while  $d > 0$  do
9:        $resto \leftarrow d \bmod 10$ 
10:      if  $resto = 4 \vee resto = 7$  then
11:         $hasDigits \leftarrow true$ 
12:         $d \leftarrow \frac{d}{10}$ 
13:
14:      if  $hasDigits$  then
15:         $count \leftarrow count + 1$ 
16:
17:   return  $count$ 

```

---

▷ **Algoritmo 1**

caixas: A caixa do tipo 1 que pode armazenar  $n_1$  bolinhas e custa  $c_1$ ; E a caixa do tipo 2 que pode armazenar  $n_2$  bolinhas e custa  $c_2$ .

O problema consiste em encontrar o custo mínimo para comprar caixas de forma que todas as caixas compradas estejam totalmente preenchidas e todas as  $n$  bolinhas estejam dentro de alguma caixa.

**Solução:** Imagine que compramos  $x$  caixas do tipo 1 e  $y$  caixas do tipo 2. Desse modo, o problema se resume em encontrar os valores  $x$  e  $y$ , tal que:

$$n_1x + n_2y = n, \text{ com } x, y \geq 0, \text{ e que } c_1x + c_2y \text{ seja mínimo.}$$

Como no enunciado do problema é garantido que existe uma solução, então pelo **Teorema 5** sabemos que  $MDC(n_1, n_2) | n$ .

Pelo **Corolário 12** sabemos que toda solução  $x$  e  $y$  são da forma:

$$x = (x_0 \frac{n}{d} + \frac{n_2q}{d}) \text{ e } y = (y_0 \frac{n}{d} - \frac{n_1q}{d}), \text{ onde } d = MDC(n_1, n_2) \text{ e } q \text{ é um inteiro qualquer.}$$

Desse modo temos:

$$x \geq 0 \Rightarrow (x_0 \frac{n}{d} + \frac{n_2q}{d}) \geq 0 \Rightarrow q \geq \lceil -\frac{x_0n}{n_2} \rceil$$

$$y \geq 0 \Rightarrow (y_0 \frac{n}{d} - \frac{n_1q}{d}) \geq 0 \Rightarrow q \leq \lfloor \frac{y_0n}{n_1} \rfloor$$

$$\lceil -\frac{x_0n}{n_2} \rceil \leq q \leq \lfloor \frac{y_0n}{n_1} \rfloor$$

Queremos encontrar o valor  $\min\{c_1x + c_2y\}$ , onde  $\min\{f\}$  é o valor mínimo que a expressão  $f$  assume. Portanto:

$$\min\{c_1x + c_2y\} = \min\{c_1(x_0 \frac{n}{d} + \frac{n_2q}{d})\}$$

$$\min\{c_1x + c_2y\} = \min\left\{q\left(\frac{n_2c_1 - n_1c_2}{d}\right) + n\left(\frac{c_1x_0 + c_2y_0}{d}\right)\right\}$$

$$\min\{c_1x + c_2y\} = \min\left\{q\left(\frac{n_2c_1 - n_1c_2}{d}\right)\right\} + n\left(\frac{c_1x_0 + c_2y_0}{d}\right), \text{ já que } n\left(\frac{c_1x_0 + c_2y_0}{d}\right) \text{ é constante.}$$

Se  $\left(\frac{n_2c_1 - n_1c_2}{d}\right)$  for positivo, então  $q\left(\frac{n_2c_1 - n_1c_2}{d}\right)$  assume valor mínimo quando  $q$  é mínimo, ie,  $q = \lceil -\frac{x_0n}{n_2} \rceil$ .

Por outro lado, se  $\left(\frac{n_2c_1 - n_1c_2}{d}\right)$  for negativo, então  $q\left(\frac{n_2c_1 - n_1c_2}{d}\right)$  assume valor mínimo quando  $q$  é máximo, ie,  $q = \lfloor \frac{y_0n}{n_1} \rfloor$ .

### Pseudocódigo:

---

#### Algorithm 9 Marbles

---

```

1: procedure FindMinimumPrice( $n, c_1, n_1, c_2, n_2$ )
2:    $[d, x_0, y_0] \leftarrow \text{ExtendedMDC}(n_1, n_2)$ 
3:
4:   if  $\left(\frac{n_2c_1 - n_1c_2}{d}\right) \geq 0$  then
5:     return  $\lceil -\frac{x_0n}{n_2} \rceil \left(\frac{n_2c_1 - n_1c_2}{d}\right)$ 
6:
7:   else
8:     return  $\lfloor \frac{y_0n}{n_1} \rfloor \left(\frac{n_2c_1 - n_1c_2}{d}\right)$ 

```

---

**Análise:** O único trecho do algoritmo que não roda em tempo constante é a chamada  $\text{ExtendedMDC}(n_1, n_2)$  na linha 2, logo a complexidade total do algoritmo é  $O(\log(n_1 + n_2))$ .

## 1.6.6 UVA-718

### 718 - Skyscraper Floors

**Resumo:** É dado um prédio com  $F$  andares (numerados de 0 até  $F - 1$ ) e  $E$  elevadores. Cada elevador  $i$  tem um posição inicial  $Y_i$  ( $Y_i \geq 0$ ) e uma constante  $X_i$  ( $X_i > 0$ ), de tal forma que os únicos andares que esse elevador consegue chegar são da forma,  $Y_i + X_it$ , com  $t$  inteiro. Cada elevador  $i$  não consegue atingir andares menores que  $Y_i$  e maiores ou iguais à  $F$ , ie,  $Y_i \leq Y_i + X_it \leq F - 1$ , ou melhor,  $0 \leq t \leq \frac{F-1-Y_i}{X_i}$ . Dado os valores  $F$ ,  $E$ , e as constantes  $Y_i$ ,  $X_i$  para cada elevador, o problema consiste em verificar se é possível ir do andar  $A$  até o andar  $B$  ( $0 \leq A, B < F$ ) usando os  $E$  elevadores.

**Solução:** Primeiro imagine que temos um grafo bidirecionado com  $E$  vértices, onde cada vértice representa um elevador e cada aresta  $(u, v)$  nos diz que os elevadores  $u$  e  $v$  conseguem chegar em algum andar em comum. Sabemos quais elevadores atingem o andar  $A$ , basta verificar se  $Y_i + X_it = A$  tem solução  $t$  inteira. Analogamente sabemos quais elevadores atingem o andar  $B$ . Então só precisaríamos fazer uma busca (**BFS** ou **DFS**) nesse grafo e verificar se há um caminho de um elevador que atinge o andar  $A$  até algum elevador que atinge o andar  $B$ .

Porém, para esse problema, não entraremos em detalhe nos algoritmos envolvendo grafos. Nos focaremos na parte matemática do problema, que envolve descobrir quando

dois elevadores conseguem chegar em algum andar em comum, nos possibilitando assim, construir o grafo e resolver o problema.

Dois elevadores  $u$  e  $v$  tem um andar em comum, se existe inteiros  $t_u$  ( $0 \leq t_u \leq \frac{F-1-Y_u}{X_u}$ ) e  $t_v$  ( $0 \leq t_v \leq \frac{F-1-Y_v}{X_v}$ ), tal que  $Y_u + X_u t_u = Y_v + X_v t_v$ , o que nos dá a *Equação Diofantina Linear*  $X_u t_u + (-X_v) t_v = (Y_v - Y_u)$ .

Vamos mostrar agora um método para calcular  $t_u$  e  $t_v$ , tal que  $at_u + bt_v = c$ , com  $a = X_u$ ,  $b = -X_v$  e  $c = (Y_v - Y_u)$ . Pelo **Teorema 5**, sabemos que essa equação tem solução, se e somente se,  $MDC(a, b) | c$ . Observe também que se  $Y_u = Y_v$  os elevadores estarão conexos pelo andar  $Y_u$ . Checaremos essas restrições no começo do algoritmo, e daqui para frente assumiremos que  $MDC(a, b) | c$  e  $Y_u \neq Y_v$ .

Tome  $d$ ,  $t_1$ ,  $t_2$  como sendo os valores retornados por  $ExtendedMDC(a, b)$ , temos então pelo **Corolário 12** que todas as soluções da equação  $at_u + bt_v = c$ , são da forma  $t_u = (t_1 \frac{c}{d} + \frac{bq}{d})$  e  $t_v = (t_2 \frac{c}{d} - \frac{aq}{d})$ , com  $q \in \mathbb{Z}$ . Logo:

$$t_u = (t_1 \frac{c}{d} + \frac{bq}{d}) \Rightarrow \frac{-t_1 c}{b} \leq q \leq \left[ \left( \frac{F-1-Y_u}{X_u} \right) d - t_1 c \right] \frac{1}{b}, \text{ já que } 0 \leq t_u \leq \frac{F-1-Y_u}{X_u}$$

Analogamente temos:

$$t_v = (t_2 \frac{c}{d} - \frac{aq}{d}) \Rightarrow \frac{t_2 c}{a} \geq q \geq \left[ t_2 c - \left( \frac{F-1-Y_v}{X_v} \right) d \right] \frac{1}{a}, \text{ já que } 0 \leq t_v \leq \frac{F-1-Y_v}{X_v}$$

Das duas inequações acima, temos:

$$\max \left( \frac{-t_1 c}{b}, \left[ t_2 c - \left( \frac{F-1-Y_v}{X_v} \right) d \right] \frac{1}{a} \right) \leq q \leq \min \left( \frac{t_2 c}{a}, \left[ \left( \frac{F-1-Y_u}{X_u} \right) d - t_1 c \right] \frac{1}{b} \right)$$

Portanto, se a inequação acima tiver solução inteira  $q$ , os elevadores  $u$  e  $v$  serão conectados pelo andar  $Y_u + X_u t_u = Y_u + X_u \left[ \left( t_1 + \frac{bq}{d} \right) \frac{c}{d} \right]$ .

### Pseudocódigo:

**Análise:** O único trecho do algoritmo que não roda em tempo constante é a chamada  $ExtendedMDC(a, b)$  na linha 5, logo a complexidade total do algoritmo é  $O(\log(a+b)) = O(\log(X_u + X_v))$ .



---

**Algorithm 10** Verifica se os elevadores  $u$  e  $v$  estão conexos.

---

```

1: procedure ElevatorsConected( $X_u, Y_u, X_v, Y_v, F$ )
2:    $a \leftarrow X_u$ 
3:    $b \leftarrow -X_v$ 
4:    $c \leftarrow Y_v - Y_u$ 
5:    $[d, t_1, t_2] \leftarrow \text{ExtendedMDC}(a, b)$ 
6:
7:   if  $Y_u = Y_v$  then
8:     return true
9:
10:  if  $d \nmid c$  then
11:    return false
12:
13:                                     ▷ A partir desse ponto temos:  $c \neq 0$  e  $d|c$ 
14:   $left \leftarrow \max\left(\frac{-t_1c}{b}, \left[t_2c - \left(\frac{F-1-Y_v}{X_v}\right)d\right]\frac{1}{a}\right)$ 
15:   $right \leftarrow \min\left(\frac{t_2c}{a}, \left[\left(\frac{F-1-Y_u}{X_u}\right)d - t_1c\right]\frac{1}{b}\right)$ 
16:
17:  if  $\lceil left \rceil \leq \lfloor right \rfloor$  then
18:    return true
19:
20:  return false

```

---



## Capítulo 2

# Aritmética Modular

### 2.1 Congruência

**Definição 5** Para  $a$  e  $b$  inteiros, dizemos que  $a$  é congruente à  $b$  módulo  $m$  ( $a \equiv b \pmod{m}$ ),  $m > 0$ ) se  $a$  e  $b$  produzem o mesmo resto na divisão por  $m$  (ie,  $m \mid (a - b)$ ). Caso contrário ( $m \nmid (a - b)$ ), dizemos que  $a$  não é congruente à  $b$  módulo  $m$  ( $a \not\equiv b \pmod{m}$ ).

**Definição 6** Dizemos que o conjunto de inteiros  $S = \{s_1, s_2, \dots, s_k\}$  é um sistema completo de resíduos módulo  $n$  se:  $\forall a \in \mathbb{Z}, \exists! s_i \in S \mid a \equiv s_i \pmod{n}$

**Proposição 3** Dados inteiros  $a, b, c, d$  com  $\text{MDC}(c, d) = 1$ , temos que:  
 $ac \equiv bc \pmod{d} \Rightarrow a \equiv b \pmod{d}$ .

**Demonstração:**

$$ac \equiv bc \pmod{d} \Rightarrow d \mid (ac - bc) \Rightarrow d \mid c(a - b) \Rightarrow d \mid (a - b), \text{ já que } \text{MDC}(c, d) = 1 \\ \Rightarrow a \equiv b \pmod{d}. \quad \square$$

**Proposição 4** O conjunto  $R = \{0, 1, 2, 3, \dots, n - 1\}$ , é um sistema completo de resíduos módulo  $n$ .

**Demonstração:** Pelo **Teorema 1** sabemos que para qualquer inteiro  $a$ , existe  $q, r$  tal que,  $a = qn + r, 0 \leq r < n$ . Assim,  $a \equiv r \pmod{n}$ , com  $r \in R$ .  $\square$

**Teorema 6** Se o conjunto  $S = \{s_0, s_1, s_2, \dots, s_{k-1}\}$  é um sistema completo de resíduos módulo  $n$ , então  $k = n$ .

**Demonstração:** Tome o conjunto  $R = \{0, 1, 2, 3, \dots, n - 1\}$ . Pela **Proposição 4** sabemos que  $R$  é um sistema completo de resíduos módulo  $n$ .

Podemos concluir então, que cada elemento  $s_i$  de  $S$  é congruente a exatamente um dos elementos  $r_i$  em  $R$ , o que nos garante  $|S| \leq |R|$ , ou simplesmente  $k \leq n$ . Por outro lado, o conjunto  $S$  é por definição um sistema completo de resíduos módulo  $n$ , e desse modo cada elemento  $r_i$  de  $R$  é congruente a exatamente um dos elementos  $s_i$  em  $S$ , o que nos garante  $|R| \leq |S|$ . Disso temos que,  $|R| = |S|$ , ou melhor,  $k = n$ .  $\square$

## 2.2 Congruência Linear

**Definição 7** Congruências da forma  $ax \equiv b \pmod{m}$ , onde  $a$ ,  $b$  e  $m$  são inteiros e  $x$  é uma incógnita, são chamadas de Congruências Lineares.

**Proposição 5**  $ax \equiv b \pmod{m}$  tem solução  $\Rightarrow MDC(a, m) | b$

**Demonstração:** Suponha que  $\exists x \in \mathbb{Z}$ , tal que  $ax \equiv b \pmod{m}$ , assim temos:

$$\begin{aligned} ax \equiv b \pmod{m} &\Rightarrow m | (b - ax) \Rightarrow \exists !r \in \mathbb{Z} \text{ tal que } (b - ax) = mr \\ &\Rightarrow b = mr + ax \Rightarrow MDC(a, m) | b, \text{ pois } MDC(a, m) \text{ divide tanto } a \text{ como } m. \quad \square \end{aligned}$$

**Proposição 6**  $ax \equiv b \pmod{m}$  tem solução  $\Leftarrow MDC(a, m) | b$

**Demonstração:**

$$\begin{aligned} MDC(a, m) | b &\Rightarrow (ax + my) | b \text{ (} \triangleright \text{ Teorema 4)} \\ &\Rightarrow \exists !r \in \mathbb{Z} \text{ tal que, } b = (ax + my)r \Rightarrow b = (xr)a + (yr)m \\ &\Rightarrow b \equiv xra + yrm \pmod{m} \Rightarrow b \equiv xra \pmod{m} \\ &\text{E assim, a Congruência Linear } az \equiv b \pmod{m}, \text{ tem solução } z = xr. \quad \square \end{aligned}$$

**Corolário 13**  $ax \equiv b \pmod{m}$  tem solução  $\Leftrightarrow MDC(a, m) | b$

**Demonstração:** Segue trivialmente das **Proposições 5 e 6**.

**Teorema 7** O conjunto  $S = \{s_0, s_1, s_2, \dots, s_{n-1}\}$  com  $s_i = im + p$ ,  $m, n, p \in \mathbb{Z}$ , e  $MDC(m, n) = 1$  é um sistema completo de resíduos módulo  $n$ .

**Demonstração:** Primeiro provaremos que  $\forall a \in \mathbb{Z}, \exists !s_i \in S \mid a \equiv s_i \pmod{n}$ .

Tome um inteiro  $a$  qualquer e a Congruência Linear:  $(a - p) \equiv xm \pmod{n}$ . Pelo

**Corolário 13** sabemos que essa Congruência Linear tem solução, já que  $MDC(m, n) = 1$ . Assim:

$$\begin{aligned} (a - p) \equiv xm \pmod{n} &\Rightarrow a \equiv xm + p \pmod{n} \Rightarrow a \equiv im + p \pmod{n}, i = x \bmod n \\ &\Rightarrow a \equiv s_i \pmod{n} \end{aligned}$$

Agora provaremos que  $s_i \not\equiv s_j \pmod{n}$  para  $i \neq j$ .

Tome  $s_i$  e  $s_j$  em  $S$  com  $i \neq j$ ,  $0 < |i - j| < n$ . Claramente  $(i - j) \not\equiv 0 \pmod{n}$ , já que  $i$  e  $j$  são distintos e  $0 \leq i, j < n$ . Portanto  $(i - j)m \not\equiv 0 \pmod{n}$ , já que  $MDC(m, n) = 1$ , e assim:

$$\begin{aligned} (i - j)m \not\equiv 0 \pmod{n} &\Rightarrow im \not\equiv jm \pmod{n} \Rightarrow im + p \not\equiv jm + p \pmod{n} \\ &\Rightarrow s_i \not\equiv s_j \pmod{n}. \end{aligned}$$

Disso segue que  $S$  é um sistema completo de resíduos módulo  $n$ .  $\square$

## 2.3 Teoremas de Fermat e de Wilson

### 2.3.1 Teorema de Fermat

**Teorema 8 (Pequeno Teorema de Fermat)** Dado um número primo qualquer  $p$ , temos que:  $a^{p-1} \equiv 1 \pmod{p}, \forall a \in \mathbb{Z} \mid MDC(a, p) = 1$

**Demonstração:** Tome os conjuntos  $S = \{s_0, s_1, s_2, \dots, s_{p-1}\}$ , com  $s_i = ai$ , e  $T = \{0, 1, 2, \dots, p-1\}$ . Claramente o conjunto  $T$  é um Sistema completo de resíduos módulo  $p$ . Pelo **Teorema 7** sabemos que  $S$  também é um Sistema completo de resíduos módulo  $p$ , e assim,  $\forall s_i \in S, \exists !t_j \in T, 0 \leq t_j \leq (p-1)$ , tal que  $s_i \equiv t_j \pmod{p}$ . Dessa informação podemos derivar a seguinte congruência modular:

$s_1.s_2.s_3...s_{p-1} \equiv t_1.t_2.t_3...t_{p-1} \pmod{p}$  ( $\triangleright$  Observe que o correspondente a  $s_0$  é  $t_0$ )  
 $\Rightarrow a.2a.3a....(p-1)a \equiv 1.2.3....(p-1) \pmod{p} \Rightarrow a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$   
 E aplicando os **Corolários 9** e **Proposição 3**, temos:  
 $a^{p-1} \equiv 1 \pmod{p}$ .  $\square$

**Teorema 9** Dados os inteiros  $a$  e  $b$  quaisquer e um número primo  $p$ , com  $\text{MDC}(a, p) = 1$ , temos que:

$$a^b \equiv a^{b \bmod (p-1)} \pmod{p}$$

**Demonstração:** Pelo **Teorema 1** podemos escrever  $b = q(p-1) + r$ , onde  $r = b \bmod (p-1)$ . Assim temos:

$$a^b = a^{q(p-1)+r} = a^{q(p-1)}a^r = (a^{p-1})^qa^r \Rightarrow a^b \equiv (a^{p-1})^qa^r \pmod{p}$$

Pelo **Teorema 8** temos  $a^{p-1} \equiv 1 \pmod{p}$ . Logo:

$$a^b \equiv (1)^qa^r \equiv a^r \equiv a^{b \bmod (p-1)} \pmod{p}. \square$$

### 2.3.2 Inverso Multiplicativo Modular

**Definição 8** Um inteiro  $x$  é chamado de Inverso Multiplicativo de  $a$  módulo  $m$ , se  $ax \equiv 1 \pmod{m}$ , para  $a$  e  $m$  inteiros.

**Teorema 10** Se  $p$  é primo e  $a$  é primo entre si com  $p$ , então:  $a^{p-2} \equiv a^{-1} \pmod{p}$ , ou seja,  $a^{p-2}$  é inverso multiplicativo de  $a$  módulo  $p$ .

**Demonstração:** Pelo **Teorema 8** sabemos que  $a^{p-1} \equiv 1 \pmod{p}$ . Sabemos também que existe um inverso multiplicativo  $a^{-1}$  de  $a$  módulo  $p$ , já que  $a$  e  $p$  são primos entre si. Desse modo, temos que:

$$a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^{p-1}a^{-1} \equiv 1.a^{-1} \pmod{p} \Rightarrow a^{p-2} \equiv a^{-1} \pmod{p}. \square$$

### 2.3.3 Teorema de Wilson

**Proposição 7** Se  $p$  é um número primo, e  $a$  um inteiro tal que  $1 \leq a \leq p-2$ , então:

$$a^2 \equiv 1 \pmod{p} \Leftrightarrow a = \pm 1$$

**Demonstração:** Claramente se  $a = \pm 1$  então  $a^2 \equiv 1 \pmod{p}$ . Provaremos então somente a ida da implicação.

Sabemos que  $a^2 \equiv 1 \pmod{p}$ , desse modo temos que:

$$\begin{aligned} a^2 &\equiv 1 \pmod{p} \Rightarrow (a^2 - 1) \equiv 0 \pmod{p} \Rightarrow (a-1)(a+1) \equiv 0 \pmod{p} \\ &\Rightarrow (a-1) \equiv 0 \pmod{p} \text{ ou } (a+1) \equiv 0 \pmod{p} \\ &\Rightarrow a \equiv 1 \pmod{p} \text{ ou } a \equiv -1 \pmod{p} \Rightarrow a = 1 \text{ ou } a = -1. \square \end{aligned}$$

**Teorema 11 (Teorema de Wilson)** Se  $p$  é um número primo, então  $(p-1)! \equiv -1 \pmod{p}$

**Demonstração:** Para  $p = 2$  o resultado é trivial, então assumiremos que  $p \geq 3$ .

Pela **Proposição 7** sabemos que  $a^2 \equiv 1 \pmod{p} \Leftrightarrow a = \pm 1$  para  $1 \leq a \leq p-2$ , e assim o inverso multiplicativo de um número  $b$  em  $2 \leq b \leq p-2$  é diferente de  $b$ . Podemos então agrupar os  $\frac{p-3}{2}$  pares de inversos multiplicativos no intervalo  $[2, p-2]$  de modo que teremos:  $2.3....(p-2) \equiv 1 \pmod{p}$ .

Desse modo, temos que:

$$(p-1)! \equiv 2.3.4...(p-2)(p-1) \equiv (p-1) \equiv -1 \pmod{p}. \square$$

## 2.4 Exponenciação

### 2.4.1 Exponenciação Binária

*Exponenciação Binária* é um algoritmo muito usado em *Ciência da Computação* principalmente no campo da *Criptografia*.

O algoritmo recebe inteiros  $a$  e  $b$ , e calcula  $a^b$ , usando divisão e conquista sobre a seguinte equação:

$$a^b = \begin{cases} 1 & \text{se } b = 0 \\ (a^{\lfloor \frac{b}{2} \rfloor})^2 & \text{se } b \text{ for par} \\ a(a^{\lfloor \frac{b}{2} \rfloor})^2 & \text{se } b \text{ for impar} \end{cases}$$

**Pseudocódigo:**

---

**Algorithm 11** Exponenciação Binária

---

```

1: procedure EXPBIN( $a, b$ )
2:   if  $b = 0$  then
3:     return 1
4:
5:    $pot \leftarrow \text{EXPBIN}(a, \lfloor \frac{b}{2} \rfloor)$ 
6:    $pot \leftarrow pot^2$ 
7:
8:   if  $b \equiv 0 \pmod{2}$  then
9:     return  $pot$ 
10:  else
11:    return  $a(pot)$ 
```

---

**Análise:** O tempo  $T(a, b)$  que o algoritmo consome é dado por:  $T(a, b) = T(a, b/2) + O(1)$ , em que  $T(a, 0) = O(1)$ .

Expandindo essa recursão é fácil perceber que a complexidade do algoritmo é  $O(\log b)$ .

### 2.4.2 Exponenciação Binária Modular

*Exponenciação Binária Modular* é uma variação do algoritmo *Exponenciação Binária* que calcula  $a^b \bmod m$ , para dados inteiros  $a, b$ , e  $m$ . Em geral *Exponenciação Binária Modular* é mais usado que *Exponenciação Binária*, pelo fato da expressão  $a^b$  crescer rapidamente e causar *overflow*.

**Pseudocódigo:**

**Análise:** O tempo  $T(a, b, m)$  que o algoritmo consome é dado por:  $T(a, b, m) = T(a, b/2, m) + O(1)$ , em que  $T(a, 0, m) = O(1)$ .

Assim esse algoritmo tem a mesma complexidade  $O(\log b)$  da *Exponenciação Binária*.

### 2.4.3 Exponenciação de Matriz

*Exponenciação de Matrix* é uma outra variação do algoritmo *Exponenciação Binária* que calcula  $A^b \bmod m$ , para dados inteiros  $b$  e  $m$  e a matrix quadrada  $A_{n,n}$ .

**Definição 9** A expressão " $A \bmod m$ ", em que  $A$  é uma matrix e  $m$  um inteiro qualquer, representa uma matrix  $B$  com as mesmas dimensões que  $A$ , tal que:  $B_{ij} = A_{ij} \bmod m, \forall B_{ij} \in B$ .

---

**Algorithm 12** Exponenciação Modular

---

```

1: procedure EXPMOD( $a, b, m$ )
2:   if  $b = 0$  then
3:     return 1
4:
5:    $pot \leftarrow EXPMOD(a, \lfloor \frac{b}{2} \rfloor, m)$ 
6:    $pot \leftarrow pot^2 \bmod m$ 
7:
8:   if  $b \equiv 0 \pmod{2}$  then
9:     return  $pot$ 
10:  else
11:    return  $a(pot) \bmod m$ 

```

---



---

**Algorithm 13** Exponenciação de Matrix

---

```

1: procedure EXPMAT( $A, b, m$ )
2:   if  $b = 0$  then
3:     return  $I$  ▷  $I$  representa a matrix identidade de dimensão  $n$ 
4:
5:    $P \leftarrow EXPMAT(A, \lfloor \frac{b}{2} \rfloor, m)$ 
6:    $P \leftarrow P^2 \bmod m$ 
7:
8:   if  $b \equiv 0 \pmod{2}$  then
9:     return  $P$ 
10:  else
11:    return  $A(P) \bmod m$ 

```

---

**Pseudocódigo:**

**Análise:** A recursão desse algoritmo é similar a recursão da *Exponenciação Binária*, exceto pela operação de produto, que nesse caso são produtos de matrizes. O tempo gasto para multiplicar duas matrizes quadradas de dimensão  $n$  é  $O(n^3)$ . Assim, a complexidade total do algoritmo é  $O(n^3 \log b)$ .

## 2.5 Problemas Propostos

### 2.5.1 SPOJ-DCEPC11B

#### DCEPC11B - Boring Factorials

**Resumo:** São dados inteiros  $N$  ( $1 \leq N \leq 2 \cdot 10^9$ ) e o número primo  $P$  ( $1 < P \leq 2 \cdot 10^9$ ), de tal forma que a diferença entre  $N$  e  $P$  é pequena. O problema consiste em calcular  $N! \bmod P$ .

**Solução:** Pelo **Teorema de Wilson** sabemos que  $(P-1)! \equiv -1 \pmod{P}$ .

Temos que o problema pode ser dividido em dois casos:

**Caso 1:**  $N \geq P$

Nesse caso, teremos que:

$$N! \equiv (P-1)! \prod_{i=P}^N i \equiv (-1) \prod_{i=P}^N i \pmod{P}.$$

**Caso 2:**  $N < P$

Nesse caso, teremos que:

$$N! \equiv (P-1)! \prod_{i=N+1}^{P-1} i^{-1} \equiv (-1) \prod_{i=N+1}^{P-1} i^{-1} \pmod{P}.$$

Para resolver o **caso 1** só precisamos aplicar o **Teorema de Wilson** e construir o produto  $\prod_{i=P}^N i$  iterativamente. Para o **caso 2**, podemos usar o **Pequeno Teorema de Fermat** para calcular o inverso multiplicativo dos números no produto  $\prod_{i=N+1}^{P-1} i^{-1}$ .

**Pseudocódigo:**


---

**Algorithm 14** Boring Factorials
 

---

```

1: procedure BORINGFACT (N, P)
2:   solution  $\leftarrow$  -1
3:
4:   if  $N \geq P$  then
5:     for ( $i = P; i \leq N; i++$ ) do
6:       solution  $\leftarrow$  (solution ·  $i$ ) mod  $P$ 
7:   else
8:     for ( $i = N + 1; i \leq P - 1; i++$ ) do
9:       inverse  $\leftarrow$  MODEXP( $i, P - 2, P$ )
10:      solution  $\leftarrow$  (solution · inverse) mod  $P$ 
11:
12:   return solution
  
```

---

▷ Teorema 10

**Análise:** A complexidade do laço da linha 5 é dado por  $O(N - P)$ . Já o laço da linha 8 consome tempo proporcional a  $O((P - N) \log P)$ , já que a complexidade do algoritmo *MODEXP*() na linha 9 é  $O(\log P)$ .



Assim, a complexidade total do algoritmo é  $O(|N - P| \log P)$ .

## 2.5.2 CodeChef-IITK2P10

### IITK2P10 - Chef and Pattern

**Resumo:** Tome a seguinte função  $f_K : \mathbb{N}^* \mapsto \mathbb{N}$ :

$$f_K(x) = \begin{cases} 1 & \text{se } x = 1 \\ K & \text{se } x = 2 \\ \prod_{i=1}^{x-1} f_K(i) & \text{se } x \geq 3 \end{cases}$$

São dados dois números inteiros  $N, K$  ( $1 \leq N \leq 10^9, 1 \leq K \leq 10^5$ ). O problema consiste em calcular a expressão:  $f_K(N) \bmod p$ , em que  $p = (10^9 + 7)$ .

**Solução:** Escrevendo os valores dos primeiros termos que a função assume, temos:  $f_K(1) = 1, f_K(2) = K, f_K(3) = K, f_K(4) = K^2, f_K(5) = K^4, f_K(6) = K^8, f_K(7) = K^{16}$ .

Provaremos, por indução, que  $f_K(N) = K^{2^{N-3}}, N \geq 3$ .

Para os primeiros termos essa expressão é trivialmente verificada.

Assuma que a expressão funciona para algum número natural qualquer  $(R-1) \geq 3$  ( $f_K(R-1) = K^{2^{R-4}}$ ).

Nessas condições temos que:

$$f_K(R) = \prod_{i=1}^{R-1} f_K(i) = 1 \cdot K \cdot \prod_{i=3}^{R-1} f_K(i) = K \prod_{i=3}^{R-1} K^{2^{i-3}} = K \prod_{j=0}^{R-4} K^{2^j}$$

$$f_K(R) = K K^{\sum_{j=0}^{R-4} 2^j} = K K^{2^{R-3}-1} = K^{2^{R-3}} \quad \square$$

Para calcular o valor de  $f_K(N) \bmod p$ , podemos aplicar o **Teorema 9**, já que  $p$  é um número primo e  $\text{MDC}(p, K) = 1$ :

$$f_K(N) \bmod p = K^{2^{N-3}} \bmod p = K^{2^{N-3} \bmod (p-1)} \bmod p$$

Reduzindo o problema, dessa maneira, em calcular:  $K^{2^{N-3} \bmod (10^9 + 7)}$ .

**Pseudocódigo:**

---

#### Algorithm 15 Chef and Pattern

---

```

1: procedure F (N, K)
2:    $p \leftarrow (10^9 + 7)$ 
3:    $exp \leftarrow \text{EXPMOD}(2, N - 3, p - 1)$ 
4:    $solution \leftarrow \text{EXPMOD}(K, exp, p)$ 
5:   return solution
```

▷ **Algoritmo 12**  
▷  $solution = K^{2^{N-3} \bmod (p-1)} \bmod p$

---

**Análise:** Como vimos anteriormente, as linhas 3 e 4 do algoritmo consomem tempo proporcional à  $O(n \log n)$ , e assim a complexidade total é  $O(n \log n)$ .

## 2.5.3 CodeChef-CSUMD

### SUMD - My Fair Coins

**Resumo:** Existe um número infinito de moedas de dois tipos: as de 1 centavo, e de 2 centavos. Todas as moedas tem dois lados (*cara* e *coroa*) que representam o valor da moeda.

É dado um inteiro  $N$  ( $1 \leq N \leq 10^9$ ). O problema consiste em calcular o número de arranjos lineares dessas moedas, de modo que a soma das moedas é igual à  $N$ . A única restrição é que a primeira moeda de cada arranjo seja *cara*.

Como esse número pode ser muito grande, a resposta tem que ser dada módulo  $m$  ( $m = 10^7 + 9$ ).

**Solução:** Tome  $f_1(N)$  como sendo o número de arranjos lineares com a primeira moeda sendo *cara*. Analogamente, tome  $f_2(N)$  como sendo o número de arranjos lineares com a primeira moeda sendo *coroa*. Por último, tome  $f(N) = f_1(N) + f_2(N)$ , como sendo o número total de arranjos cujo a soma das moedas é  $N$ .

Nessas condições temos as seguintes **Proposições**:

**Proposição 1:**  $f_1(N) = f_2(N)$

**Prova:** Para cada arranjo em  $f_1$ , se trocarmos a primeira moeda de *cara* para *coroa*, teremos um arranjo correspondente em  $f_2$ . E assim, há uma bijeção de  $f_1$  para  $f_2$ .

**Proposição 2:**  $f_1(N) = f_1(N-1) + f_2(N-1) + f_1(N-2) + f_2(N-2)$

**Prova:** Tome um arranjo  $A$  qualquer em  $f_1$ . A primeira moeda de  $A$  pode ser tanto uma moeda *cara* de 1 centavo, como uma moeda *cara* de 2 centavos. O número de arranjos que começam com a moeda de 1 centavo é  $f(N-1)$  e o número de arranjos que começam com a moeda de 2 centavos é  $f(N-2)$ . Assim temos:

$$f_1(N) = f(N-1) + f(N-2) = f_1(N-1) + f_2(N-1) + f_1(N-2) + f_2(N-2).$$

**Proposição 3:**  $f_1(N) = 2(f_1(N-1) + f_1(N-2))$

**Prova:** Decorrente das **Proposições 1 e 2**.

Claramente  $f_1(1) = 1$ , e  $f_1(2) = 3$ . Mostraremos um modo elegante de calcular  $f_1(N)$  usando *Exponenciação de Matrizes*. Tome a matriz  $A$  com as seguintes entradas:

$$A_{2,2} = \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}$$

Teremos então que:

$$\begin{aligned} [f_1(N) \quad f_1(N-1)] &= [f_1(N-1) \quad f_1(N-2)] \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix} \\ [f_1(N) \quad f_1(N-1)] &= \left( [f_1(N-2) \quad f_1(N-3)] \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix} \right) \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix} \\ [f_1(N) \quad f_1(N-1)] &= [f_1(N-2) \quad f_1(N-3)] \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}^2 \end{aligned}$$

Expandindo essa recursão até a base, teremos:

$$\begin{aligned} [f_1(N) \quad f_1(N-1)] &= [f_1(2) \quad f_1(1)] \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}^{N-2} \\ [f_1(N) \quad f_1(N-1)] &= [3 \quad 1] \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}^{N-2} \end{aligned}$$

**Pseudocódigo:****Algorithm 16** My Fair Coins

---

```

1: procedure  $f_1(N, m)$ 
2:   if  $N = 1$  then
3:     return 1
4:
5:   if  $N = 2$  then
6:     return 3
7:
8:    $A \leftarrow \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}$ 
9:
10:   $B \leftarrow \text{EXPMAT}(A, N - 2, m)$  ▷ Algoritmo 13
11:
12:  return  $3B_{0,0} + 1B_{1,0}$ 

```

---

**Análise:** Esse algoritmo tem a mesma complexidade do **Algoritmo 13**, ou seja,  $O(n^3 \log N)$  (onde  $n$  é a dimensão da matriz). Como nesse problema a matriz é sempre quadrada de dimensão  $n = 2$ , temos que a complexidade final do algoritmo será  $O(\log N)$ .



## Capítulo 3

# Funções Aritméticas

### 3.1 $\Phi$ de Euler

**Definição 10** A Função Totiente de Euler, denotada por  $\Phi(n)$ , é a função aritmética que conta o número de inteiros positivos menores ou iguais a  $n$  que são primos entre si com  $n$ .

$$\Phi(n) := |\{x \in \mathbb{N}^* \mid \text{MDC}(x, n) = 1\}|$$

**Teorema 12**  $\Phi(n)$  é função multiplicativa, ie,  $\Phi(mn) = \Phi(m)\Phi(n)$  para  $\text{MDC}(m, n) = 1$ .

**Demonstração:** A demonstração a seguir foi baseada no livro: OLIVEIRA SANTOS, José Plínio de. *Introdução à Teoria dos Números*. IMPA, 1998. 72 p.

Primeiro vamos dispor os números de 1 à  $nm$  da seguinte maneira:

$$\begin{array}{cccccc} 1 & (m+1) & (2m+1) & \dots & (n-1)m+1 \\ 2 & (m+2) & (2m+2) & \dots & (n-1)m+2 \\ 3 & (m+3) & (2m+3) & \dots & (n-1)m+3 \\ \vdots & & & & \\ m & 2m & 3m & \dots & nm \end{array}$$

Tome a linha  $q$ , com os elementos  $q, m+q, 2m+q, \dots, (n-1)m+q$ . Se o  $\text{MDC}(m, q) = d > 1$ , então nenhum termo dessa linha será primo com  $mn$ , já que:

$$\text{MDC}(m, q) \neq 1 \Rightarrow \text{MDC}(xm + q, q) \neq 1 \Rightarrow \text{MDC}(mn, q) \neq 1.$$

Logo, as únicas linhas da tabela que nos interessa são aquelas cujo primeiro termo é primo com  $m$  (observe que temos  $\Phi(m)$  linhas que satisfazem essa condição).

Agora, para cada uma dessas  $\Phi(m)$  linhas, queremos saber quantos termos são primos com  $n$ , já que todos elementos na linha são primos com  $m$ . Como  $\text{MDC}(m, n) = 1$ , pelo **Teorema 7** sabemos que os termos  $r, m+r, 2m+r, \dots, (n-1)m+r$  formam um sistema completo de resíduos módulo  $n$ . Assim, cada uma dessas  $\Phi(m)$  linhas contém  $\Phi(n)$  elementos primos com  $n$ , e como eles são primos com  $m$ , são também primos com  $mn$ . E isto nos garante que  $\Phi(mn) = \Phi(m)\Phi(n)$ .  $\square$

**Teorema 13**  $\Phi(p^k) = (p^k - p^{k-1})$ , para  $p$  primo e  $k$  inteiro positivo.

**Demonstração:** Como  $p$  é um número primo, para qualquer inteiro  $n$ , os únicos valores possíveis para  $\text{MDC}(p^k, n)$  são:  $1, p, p^2, \dots, p^k$ , e desse modo, se  $\text{MDC}(p^k, n) \neq 1$  temos que  $p|n$  ( $n$  é múltiplo de  $p$ ). Assim, a quantidade de números não-primos e menores do que  $p^k$  é  $p^{k-1}$ .

Logo, temos que:  $\Phi(p^k) = p^k - p^{k-1}$   $\square$

**Teorema 14 (Fórmula Produto de Euler)**  $\Phi(n) = n \prod_{p|n} (1 - \frac{1}{p}) = n \prod_{p|n} (\frac{p-1}{p})$

**Demonstração:**

$$\Phi(n) = \Phi(p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}) \quad (\triangleright \text{Teorema 3})$$

$$\Phi(n) = \Phi(p_1^{a_1}) \Phi(p_2^{a_2}) \dots \Phi(p_k^{a_k}) \quad (\triangleright \text{Teorema 12})$$

$$\Phi(n) = (p_1^{a_1} - p_1^{a_1-1}) (p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1}) \quad (\triangleright \text{Teorema 13})$$

$$\Phi(n) = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} (1 - 1/p_1) (1 - 1/p_2) \dots (1 - 1/p_k)$$

$$\Phi(n) = n \prod_{p|n} (1 - \frac{1}{p}) \quad \square$$

### 3.1.1 Algoritmo $\Phi$ de Euler

Nessa subseção mostraremos um algoritmo para o cálculo de  $\Phi$  de Euler para os primeiros  $N$  números naturais. O algoritmo baseia-se na idéia do **Crivo de Eratóstenes** e no **Teorema 14**.

**Pseudocódigo:**

---

**Algorithm 17** Calcula os primeiros  $N$  termos da função  $\Phi$

---

```

1: procedure  $\text{PHI}(N)$ 
2:    $\Phi[] \leftarrow \text{newArray}[N]$ 
3:
4:   for ( $p = 1; p \leq N; p++$ ) do
5:      $\Phi[p] \leftarrow p$ 
6:
7:   for ( $p = 2; p \leq N; p++$ ) do
8:     if  $\Phi[p] \neq p$  then                                      $\triangleright \Phi[p] \neq p \Leftrightarrow p$  não é primo
9:       continue
10:
11:     for ( $n = p; n \leq N; n = n + p$ ) do
12:        $\Phi[n] \leftarrow \Phi[n] (\frac{p-1}{p})$ 
13:
14:   return  $\Phi[]$ 

```

---

**Análise:** Deixaremos a demonstração a cargo do leitor.

**Dica:** O laço mais interno, na linha 11 só é executado quando  $p$  é primo, e assim ele executa uma quantida de vezes proporcional à:  $E = \sum_{p \text{ primo} | p \leq N} \frac{N}{p}$ .

Observe também que:  $E \leq \sum_{p=2}^N \frac{N}{p} = O(N \log N)$ .

**Proposição 8**  $\Phi(n^k) = n^{k-1} \Phi(n)$ , para inteiros positivos  $n$  e  $k$ .

**Demonstração:** TODO

### 3.1.2 Teorema de Euler

**Teorema 15 (Teorema de Euler)** Dados números inteiros  $a$  e  $n$  primos entre si, temos que:  $a^{\Phi(n)} \equiv 1 \pmod{n}$ . Observe que esse teorema é uma generalização do **Teorema 8**.

**Demonstração:** TODO usa residuos completo mod  $m$

### 3.2 Sequência de Fibonacci

**Definição 11** A sequência de Fibonacci  $Fib_n$  é uma sequência de números inteiros positivos em que cada termo subsequente corresponde a soma dos dois termos anteriores.

$$Fib_n := \begin{cases} 0 & \text{se } n = 0 \\ 1 & \text{se } n = 1 \\ Fib_{n-1} + Fib_{n-2} & \text{se } n \geq 2 \end{cases}$$

**Proposição 9**  $MDC(Fib_n, Fib_{n-1}) = 1$ , para  $n \geq 2$

**Demonstração:** Tome os primeiros termos da sequência de fibonacci: 1, 1, 2, 3, 5, 8, .... Claramente a expressão acima funciona para os primeiros termos. Assuma que a expressão funciona para um inteiro qualquer  $(k-1) > 2$ , ou seja,  $MDC(Fib_{k-1}, Fib_{k-2}) = 1$ .

Provaremos por indução que a expressão sempre funciona.

$$MDC(Fib_k, Fib_{k-1}) = MDC(Fib_{k-1} + Fib_{k-2}, Fib_{k-1})$$

$$MDC(Fib_{k-1} + Fib_{k-2}, Fib_{k-1}) = MDC(Fib_{k-2}, Fib_{k-1}) \text{ (Pelo Corolário 7)}$$

Logo, temos que:

$$MDC(Fib_k, Fib_{k-1}) = MDC(Fib_{k-2}, Fib_{k-1}) = 1 \quad \square$$

**Proposição 10**  $Fib_{m+n} = Fib_m Fib_{n+1} + Fib_{m-1} Fib_n$

**Demonstração:** Provaremos esse corolário por indução no índice  $n$ .

A base da indução será,  $n = 2$ :

$$Fib_{m+2} = Fib_m + Fib_{m+1} = Fib_m + Fib_m + Fib_{m-1}$$

$$Fib_{m+2} = 2Fib_m + 1Fib_{m-1} = Fib_m Fib_3 + Fib_{m-1} Fib_2$$

Assumindo que a expressão é válida para todos os valores menores que  $n$ , temos:

$$Fib_{m+n} = Fib_{m+n-2} + Fib_{m+n-1}$$

$$Fib_{m+n} = (Fib_m Fib_{n-1} + Fib_{m-1} Fib_{n-2}) + (Fib_m Fib_n + Fib_{m-1} Fib_{n-1})$$

$$Fib_{m+n} = Fib_m (Fib_{n-1} + Fib_n) + Fib_{m-1} (Fib_{n-2} + Fib_{n-1})$$

$$Fib_{m+n} = Fib_m Fib_{n+1} + Fib_{m-1} Fib_n \quad \square$$

**Teorema 16**  $MDC(Fib_m, Fib_n) = Fib_{MDC(m,n)}$ ,  $\forall m, n \in \mathbb{Z}$

**Demonstração:**

$$MDC(Fib_m, Fib_n) = MDC(Fib_m, Fib_{qm+r}) \text{ (Pelo Teorema 1, } n = qm + r, 0 \leq r < n)$$

$$MDC(Fib_m, Fib_n) = MDC(Fib_m, Fib_{qm} Fib_{r+1} + Fib_{qm-1} Fib_r) \text{ (Pelo Proposição 10).}$$

$$MDC(Fib_m, Fib_n) = MDC(Fib_m, Fib_{qm-1} Fib_r)$$

Pelo Corolário 8 e sabendo que  $MDC(Fib_m, Fib_{qm-1}) = 1$ , temos:

$$MDC(Fib_m, Fib_n) = MDC(Fib_m, Fib_r)$$

$$MDC(Fib_m, Fib_n) = MDC(Fib_m, Fib_{n \bmod m})$$

Se tirarmos o símbolo funcional  $Fib$ , a última equação forma um passo do **Algoritmo de Euclides** ( $MDC(m, n) = MDC(m, n \bmod m)$ ).

Podemos continuar esse processo até que o resto  $r$  se torne 0. O último resto não-nulo será exatamente o Máximo Divisor Comum dos dois números originais.

Desse modo, aplicar o **Algoritmo de Euclides** em  $Fib_m$  e  $Fib_n$  funciona da mesma maneira que aplicar aos índices  $m$  e  $n$ . E assim, ao chegarmos na base da recursão,  $MDC(m, n) = MDC(s, 0) = s$ , teremos também:  $MDC(Fib_m, Fib_n) = MDC(Fib_s, 0) = Fib_s = Fib_{MDC(m,n)} \quad \square$ .

**Teorema 17**  $Fib_n = \frac{\sqrt{5}}{5} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right)$

**Demonstração:**

A demonstração a seguir foi baseada no livro: OLIVEIRA SANTOS, José Plínio de. *Introdução à Teoria dos Números*. IMPA, 1998. 85 p.

$$Fib_{n+1} = Fib_n + Fib_{n-1}$$

$$Fib_{n+1} - kFib_n = Fib_n + Fib_{n-1} - kFib_n$$

$$Fib_{n+1} - kFib_n = Fib_n + Fib_{n-1} - kFib_n + (kFib_{n-1} - kFib_{n-1}) + (k^2Fib_{n-1} - k^2Fib_{n-1})$$

$$Fib_{n+1} - kFib_n = (1-k)(Fib_n - kFib_{n-1}) + (1+k-k^2)Fib_{n-1}$$

Se denotarmos as raízes de  $k^2 - k - 1 = 0$  por  $k_1$  e  $k_2$ , teremos que  $k_1 = \frac{1+\sqrt{5}}{2}$  e  $k_2 = \frac{1-\sqrt{5}}{2}$ .

$$Fib_{n+1} - k_1Fib_n = k_2(Fib_n - k_1Fib_{n-1})$$

$$Fib_{n+1} - k_2Fib_n = k_1(Fib_n - k_2Fib_{n-1})$$

Por iterações sucessivas dessas duas equações teremos que:

$$Fib_{n+1} - k_1Fib_n = k_2^n(Fib_1 - k_1Fib_0) = k_2^n$$

$$Fib_{n+1} - k_2Fib_n = k_1^n(Fib_1 - k_2Fib_0) = k_1^n$$

Subtraindo membro a membro nos dá:

$$Fib_n(k_2 - k_1) = k_2^n - k_1^n$$

$$Fib_n = \frac{k_2^n - k_1^n}{k_2 - k_1}$$

$$Fib_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)}$$

$$Fib_n = \frac{\sqrt{5}}{5} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right) \square$$

TODO demonstracao analise algoritmo de euclides

### 3.3 Problemas Propostos

#### 3.3.1 UVA-11424

##### 11424 - GCD - Extreme (I)

**Resumo:** É dado um inteiro positivo  $N$  ( $1 < N < 200001$ ). O problema consiste em calcular o mais rápido possível a expressão:

$$G(N) = \sum_{i=1}^{N-1} \sum_{j=i+1}^N MDC(i, j).$$

**Solução:** Trivialmente a expressão acima pode ser calculada em tempo proporcional a  $O(n^2 \log(N))$ , porém essa solução consome muito tempo e não será aceita no Judge Online. Vamos então mostrar uma solução mais eficiente.

Primeiramente reescrevemos a expressão acima da seguinte maneira:

$$G(N) = \sum_{j=2}^N \sum_{i=1}^{j-1} MDC(i, j) \quad (\triangleright \text{Observe que as expressões são equivalentes}).$$

Tome agora a função  $F(M) = \sum_{i=1}^{M-1} MDC(i, M)$ . Com isso,  $G(N) = \sum_{j=2}^N F(j)$ .

Sabemos que todos os valores resultantes do método  $MDC(i, M)$  calculados em  $F(M)$  são divisores de  $M$ . Desse modo, podemos reescrever  $F(M)$  da seguinte maneira:

$F(M) = \sum_{i=1}^{M-1} MDC(i, M) = \sum_{l=1}^n \lambda_l d_l$ , em que,  $d_1, d_2, \dots, d_n$  são os divisores de  $M$ ,  $\lambda_l$  é o número de vezes que o divisor  $d_l$  aparece na somatória  $\sum_{i=1}^{M-1} MDC(i, M)$ , e  $n$  é o número de divisores de  $M$ .



Pelo Corolário 6 temos que:  $MDC(i, M) = d_l \Rightarrow MDC(i/d_l, M/d_l) = 1$ . Logo o número de vezes que o divisor  $d_l$  aparece na somatória, será igual ao número de primos entre si com  $(M/d_l)$ , ie,  $\lambda_l = \Phi(M/d_l)$ .

Reescrevendo novamente  $F(M)$ , temos:

$$F(M) = \sum_{i=1}^{M-1} MDC(i, M) = \sum_{l=1}^n \lambda_l d_l = \sum_{l=1}^n \Phi(M/d_l) d_l.$$

$$G(N) = \sum_{j=2}^N \sum_{l=1}^n \Phi(j/d_l) d_l \quad \square.$$

**Pseudocódigo:**

---

**Algorithm 18** GCD - Extreme(I)

---

```

1: procedure G (N)
2:    $\Phi[] \leftarrow PHI(N)$ 
3:    $solution \leftarrow 0$ 
4:   for  $j := 2$  to  $N$  do
5:     for each divisor  $d$  de  $j$  do
6:        $solution \leftarrow solution + \Phi[j/d]d$ 
7:   return  $solution$ 

```

---

**Análise:** O método  $PHI(N)$  na linha 2 consome tempo proporcional à  $O(N\sqrt{N})$ .

O número de divisores de  $j$  é proporcional à  $O(\sqrt{N})$ , já que  $j \leq N$ .

Assim a complexidade das linhas 4, 5, 6 do algoritmo é  $O(N\sqrt{N})$ .

Complexidade final do algoritmo:  $O(N\sqrt{N})$ .

**OBS.:** Para resolver o problema no Judge Online será preciso armazenar as soluções usando **Programação Dinâmica**.

### 3.3.2 TJU-3506

#### 3506 - Euler Function

**Resumo:** São dados três números positivos  $n, m$  ( $1 < n < 10^7, 1 < m < 10^9$ ) e  $d = 201004$ . O problema consiste em calcular a expressão:  $\Phi(n^m) \bmod d$ .

**Solução:** Pelo **Proposição 8**, temos:

$$\Phi(n^m) \bmod d = (n^{m-1} \Phi(n)) \bmod d$$

$$\Phi(n^m) \bmod d = ((n^{m-1} \bmod d)(\Phi(n)) \bmod d) \bmod d$$

Desse modo, podemos calcular o primeiro fator do produto  $(n^{m-1} \bmod d)$  usando  $EXPMOD()$  e a segundo fator com o método  $PHI()$ .

**Pseudocódigo:**

---

**Algorithm 19** Euler Functions

---

```

1: procedure  $PhiEulerPotential(n, m, d)$ 
2:    $\Phi[] \leftarrow PHI(n)$ 
3:    $exp \leftarrow EXPMOD(n, m - 1, d)$ 
4:    $solution \leftarrow (exp \Phi[n]) \bmod d$ 
5:   return  $solution$ 

```

---

**Análise:** As linhas 3 e 4 do algoritmo consomem tempo proporcional a  $O(\log m)$  e  $O(1)$  respectivamente. Se precalcularmos o vetor  $\Phi[]$ , temos que a complexidade total para calcular cada instância do problema será:  $O(\log m)$

### 3.3.3 CodeChef-IITK2P05

#### IITK2P05 - Factorization

**Resumo:** É dado um inteiro  $N$  ( $2 \leq N \leq 10^{18}$ ) e o valor de  $\Phi(N)$ . O problema consiste em fatorar  $N$ .

**Solução:** A solução trivial para fatorar  $N$  consome tempo proporcional a  $O(\sqrt{N})$ , porém para uma entrada na ordem de  $10^{18}$  precisamos de um algoritmo mais eficiente.

Se  $N$  for primo, ie,  $\Phi(N) = N - 1$ , já temos a solução.

Assuma então que  $N$  é um número composto. Primeiro vamos iterar nos primeiros  $\sqrt[3]{N}$  inteiros e remover todos os fatores primos de  $N$  nesse intervalo. Tome  $M$  como sendo o valor resultante.

Imagine que  $M$  tenha três ou mais fatores primos. Sabemos que  $M$  não tem nenhum fator primo menor que  $\sqrt[3]{N}$ , temos que:  $M > (\sqrt[3]{N})^3 \Rightarrow M > N$  (contradição). Desse modo, temos que  $M$  tem no máximo dois fatores primos, e esses valores são maiores que  $\sqrt[3]{N}$ .

- **Caso 1:**  $M$  tem só um fator primo, ie,  $M$  é primo: Basta checar se  $\Phi(M) = M - 1$
- **Caso 2:**  $M$  tem dois fatores primos iguais,  $M = p^2$ : Basta verificar se  $M$  é um quadrado perfeito. Pode ser feito facilmente com busca binária.
- **Caso 3:**  $M$  tem dois fatores primos distintos,  $M = pq$ : Se  $M = pq$  então  $\Phi(M) = (p - 1)(q - 1)$ . Temos então um sistema com duas equações e duas incógnitas. Se resolvermos o sistema encontraremos a fatoração de  $M$  e assim a fatoração de  $N$ .

O único problema agora é calcular  $\Phi(M)$  a partir de  $\Phi(N)$ . Assuma que  $N = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} M$ , com  $k \geq 0$  e  $p_i$  os fatores primos distintos de  $N$  removidos na primeira etapa do algoritmo. Temos então:

$$\begin{aligned} N &= p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} M \Rightarrow \Phi(N) = \Phi(p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} M) \\ N &= p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} M \Rightarrow \Phi(N) = \Phi(p_1^{a_1}) \Phi(p_2^{a_2}) \dots \Phi(p_k^{a_k}) \Phi(M) \quad (\triangleright \text{Teorema 12}) \\ \Rightarrow \Phi(N) &= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1}) \Phi(M) \quad (\triangleright \text{Teorema 13}) \\ \Rightarrow \Phi(M) &= \frac{\Phi(N)}{(p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1})} \end{aligned}$$

#### Pseudocódigo:

**Análise:** O laço da linha 10 consome tempo proporcional a  $O(\sqrt[3]{N})$ . Já o laço da linha 11 consome tempo proporcional a  $O(\log_p N)$ , pois tem no máximo  $a$  iterações ( $a$  é o número de vezes que o fator primo  $p$  aparece em  $N$ ) e assim,  $p^a < N \Rightarrow a < \log_p N$ .

As linhas 15-16 rodam em  $O(\log_p N)$ , já que o número máximo de elementos distintos em  $S$  é  $\log_p N$  ( $p$  é o menor primo que divide  $N$ ). E as linhas 18-23 rodam em  $O(1)$ .

Assim, o algoritmo total consome tempo proporcional a  $O(\sqrt[3]{N} \log N)$ . Observe que esse algoritmo é bem mais eficiente que o algoritmo trivial para fatoração  $O(\sqrt{N})$ .

### 3.3.4 CodeChef-PUPPYGCD

#### PUPPYGCD - Puppy and GCD

**Resumo:** São dados inteiros positivos  $N$  e  $D$ . O problema consiste em calcular o número de pares não-ordenados  $\{A, B\}$ , tal que  $1 \leq A, B \leq N$  e  $\text{MDC}(A, B) = D$ .

**Algorithm 20** Fatoração de  $N$ 


---

```

1: procedure  $Factorization(N, \Phi_N)$ 
2:    $S \leftarrow \emptyset$  ▷  $S$  contém os fatores primos de  $N$ 
3:    $M \leftarrow N$ 
4:    $\Phi_M \leftarrow \Phi_N$ 
5:
6:   if  $\Phi_N = N - 1$  then ▷ Se  $N$  for primo
7:      $S \leftarrow S \cup \{N\}$ 
8:     return  $S$ 
9:
10:  for each  $p$  primo menor igual à  $\sqrt[3]{N}$  do
11:    while  $M \equiv 0(mod\ p)$  do
12:       $M \leftarrow \frac{M}{p}$ 
13:       $S \leftarrow S \cup \{p\}$ 
14:
15:  for each  $p \in S$  do
16:     $\Phi_M \leftarrow \frac{\Phi_M}{p^a - p^{a-1}}$  ▷  $a :=$  número de vezes que o primo  $p$  é inserido em  $S$ 
17:
18:  if  $\Phi_M = M - 1$  then ▷ Se  $M$  for primo
19:     $S \leftarrow S \cup \{M\}$ 
20:    return  $S$ 
21:
22:   $(p, q) \leftarrow System(M, \Phi_M)$  ▷ Resolve o sistema de 2 equações e 2 incógnitas
23:   $S \leftarrow S \cup \{p, q\}$ 
24:  return  $S$ 

```

---

**Solução:** Claramente se  $D$  for maior que  $N$ , não há nenhum par que satisfaça as condições. Logo, assumiremos que  $D \leq N$ .

Pelo **Corolário 6** sabemos que se  $MDC(A, B) = D$  então  $MDC(\frac{A}{D}, \frac{B}{D}) = 1$ . Assim, podemos reduzir o problema em calcular o número de pares não-ordenados  $\{A, B\}$ , tal que  $1 \leq A, B \leq \frac{N}{D}$  e  $MDC(A, B) = 1$ . Logo o número de pares será igual a somatória de  $\Phi(r)$ , com  $1 \leq r \leq \frac{N}{D}$ , já que  $\Phi(r)$  nos dá a quantidade de números menores ou iguais a  $r$  e primo com entre si com  $r$ . Observe que essa somatória nos dá somente a metade do número de pares, já que o problema consiste em calcular pares não-ordenados.

**Pseudocódigo:**

---

**Algorithm 21** Puppy and GCD

---

```

1: procedure CalculatePairs( $N, P$ )
2:   if  $D > N$  then
3:     return 0
4:
5:    $\Phi[] \leftarrow PHI(\frac{N}{D})$ 
6:    $count \leftarrow 0$ 
7:
8:   for ( $A = 1; A \leq \frac{N}{D}; A++$ ) do
9:      $count \leftarrow count + \Phi[A]$ 
10:
11:    $count \leftarrow 2 \text{ count} - 1$ 
12:   return  $count$ 

```

---

**Análise:** Se precalcularmos  $\Phi[]$  teremos que o fator limitando do algoritmo será o laço da linha 8, e a complexidade do algoritmo será  $O(\frac{N}{D})$ .

Obs.: Quando dobramos o valor de  $count$  na linha 11, tem um único  $\{1, 1\}$  que é contado duas vezes, e por isso precisamos subtrair 1 do valor final. Esse par corresponde ao par  $\{D, D\}$  do problema original.

### 3.3.5 CodeChef-MODEFB

#### 71544 - Another Fibonacci

**Resumo:** São dados dois números inteiros  $N, K$  ( $1 \leq N \leq 50000, 1 \leq K \leq N$ ) e um conjunto  $S \subset \mathbb{N}$  com  $N$  elementos, tal que,  $\forall s \in S, 1 \leq s \leq 10^9$ .

Tome a seguinte função:

$$F(S) = \sum_{A \subset S \text{ e } |A|=K} Fib(sum(A)), \text{ onde } sum(A) = \sum_{a \in A} a.$$

O problema consiste em calcular a expressão:  $F(S) \bmod 99991$

**Solução:**

**Pseudocódigo:**

---

**Algorithm 22** Another Fibonacci

---

```

1: procedure F ( $S$ )

```

---

**Análise:**

### 3.3.6 Codeforces-227E

#### 227E - Anniversary

**Resumo:** São dados quatro inteiros  $m, l, r, k$  ( $1 \leq m \leq 10^9, 1 \leq l \leq r \leq 10^{12}, 2 \leq k \leq r-l+1$ ), e um conjunto  $A = \{l, l+1, l+2, \dots, r\}$ . Dado um conjunto  $S \subseteq A$  com  $k$  elementos, ie,  $S = \{s_1, s_2, \dots, s_k\}$ , é definido a função  $F(S) = \text{MDC}(\text{Fib}_{s_1}, \text{Fib}_{s_2}, \dots, \text{Fib}_{s_k})$ .

O problema consiste em encontrar tal subconjunto  $S$ , de tal forma que  $F(S)$  seja máxima. No final do algoritmo basta imprimir  $F(S) \bmod m$ .

**Solução:** Pelo **Teorema 16** sabemos que,  $\text{MDC}(\text{Fib}_{s_1}, \text{Fib}_{s_2}, \dots, \text{Fib}_{s_k}) = \text{Fib}_{\text{MDC}(s_1, s_2, \dots, s_k)}$ . Desse modo, para maximizar  $F(S)$ , basta maximizar  $\text{MDC}(s_1, s_2, \dots, s_k)$ , já que  $\text{Fib}_x$  é uma sequência crescente.

Suponha que o valor máximo para  $\text{MDC}(s_1, s_2, \dots, s_k)$  seja  $q$ . Como  $q$  divide todos os  $k$  inteiros  $(s_1, s_2, \dots, s_k)$  no conjunto  $A$ , então  $\lfloor \frac{r}{q} \rfloor - \lceil \frac{l}{q} \rceil + 1 \geq k$ , ie, o número de múltiplos de  $q$  entre  $l$  e  $r$  é maior ou igual a  $k$ .

Todos os valores que  $\lfloor \frac{r}{q} \rfloor$  assume, são da forma:

$$i \in \{1, 2, 3, \dots, \lfloor \sqrt{r} \rfloor\}, \text{ se } \lfloor \frac{r}{q} \rfloor \leq \sqrt{r}$$

$$\lfloor \frac{r}{i} \rfloor, \text{ com } i \in \{1, 2, 3, \dots, \lfloor \sqrt{r} \rfloor\}, \text{ se } \lfloor \frac{r}{q} \rfloor > \sqrt{r}$$

Analogamente, podemos calcular todos os valores que  $\lceil \frac{l}{q} \rceil$  assume.

Tendo todos esses valores armazenados em um conjunto  $Q$ , é possível calcular todos os valores distintos que  $\lfloor \frac{r}{q} \rfloor - \lceil \frac{l}{q} \rceil + 1$  assume, e assim basta escolher o maior  $q \in Q$ , tal que  $\lfloor \frac{r}{q} \rfloor - \lceil \frac{l}{q} \rceil + 1 \geq k$ .

A partir do momento que calculamos  $q$ , ie, encontramos o valor máximo de  $\text{MDC}(s_1, s_2, \dots, s_k)$ , precisamos de uma maneira eficiente de calcular  $\text{Fib}_q \bmod m$ . E para isso, usaremos **Exponenciação de Matriz** com a seguinte matriz:

$$A_{2,2} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\text{Observe que: } \begin{bmatrix} \text{Fib}_q & \text{Fib}_{q-1} \end{bmatrix} = \begin{bmatrix} \text{Fib}_{q-1} & \text{Fib}_{q-2} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\text{E assim: } \begin{bmatrix} \text{Fib}_q & \text{Fib}_{q-1} \end{bmatrix} = \begin{bmatrix} \text{Fib}_2 & \text{Fib}_1 \end{bmatrix} A^{q-2} = \begin{bmatrix} 1 & 1 \end{bmatrix} A^{q-2}$$

#### Pseudocódigo:

**Análise:** Os laços das linhas 5 e 8 consomem tempo proporcional a  $O(\sqrt{r})$ . O laço da linha 11 consomem tempo proporcional a  $O(\sqrt{l})$ , que por sua vez é  $O(\sqrt{r})$ , já que  $l \leq r$ . Como é inserido um elemento em  $Q$  para cada iteração desses três primeiros laços, temos que no final do algoritmo o número de elementos em  $Q$  é da ordem de  $O(\sqrt{r})$ .

O laço da linha 14 consomem tempo proporcional a  $O(|Q|)$ , ie,  $O(\sqrt{r})$ .

Assim, a complexidade total do algoritmo é  $O(\sqrt{r} + \log r)$ , já que o algoritmo **EXP-MAT()** roda em  $O(\log q)$ , ou melhor,  $O(\log r)$ , pois  $q \leq r$ .

**Algorithm 23** Anniversary

---

```

1: procedure FindMaximumValue( $m, r, l, k$ )
2:    $Q \leftarrow \emptyset$ 
3:    $q \leftarrow 0$ 
4:
5:   for ( $i = 1; i \leq \sqrt{r}; i++$ ) do
6:      $Q \leftarrow Q \cup \{i\}$ 
7:
8:   for ( $i = 1; i \leq \sqrt{r}; i++$ ) do
9:      $Q \leftarrow Q \cup \{\lfloor \frac{r}{i} \rfloor\}$ 
10:
11:   for ( $i = 1; i \leq \sqrt{l}; i++$ ) do
12:      $Q \leftarrow Q \cup \{\lceil \frac{l}{i} \rceil\}$ 
13:
14:   for all  $q^* \in Q$  do
15:     if  $\lfloor \frac{r}{q^*} \rfloor - \lceil \frac{l}{q^*} \rceil + 1 \geq k$  then
16:        $q \leftarrow \max(q, q^*)$ 
17:
18:    $A \leftarrow \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ 
19:
20:    $B \leftarrow \text{EXPMAT}(A, q - 2, m)$ 
21:
22:   return  $(B_{0,0} + B_{1,0}) \bmod m$ 

```

---

## **Capítulo 4**

# **Conclusão**

...





## Apêndice A

### Curiosidades da ACM-ICPC

ACM-ICPC (International Collegiate Programming Contest) é uma competição de programação de várias etapas e baseada em equipe. O principal objetivo é encontrar algoritmos eficientes, que resolvem os problemas abordados pela competição, o mais rápido possível.

Nos últimos anos a ACM-ICPC teve um crescimento significativo. Se compararmos o número de competidores, temos que de 1997 (ano em que começou o patrocínio da IBM) até 2014 houve um aumento maior que 1500%, totalizando 38160 competidores de 2534 universidades em 101 países ao redor do mundo.

Para mais informações sobre as competições passadas acesse [icpc.baylor.edu](http://icpc.baylor.edu).

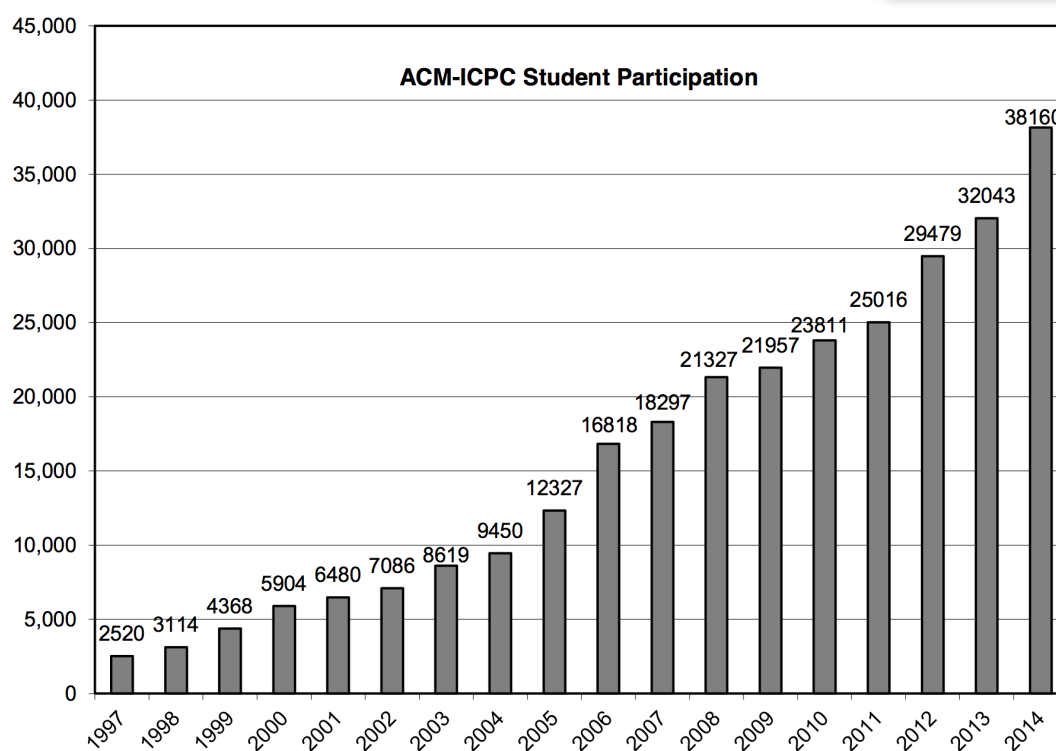


FIGURA A.1: Crescimento do número de participantes por ano.



## Apêndice B

# Juízes Online (Online Judges)

Online Judges são plataformas online que contam com um banco de dados com diversos tipos de problemas de competições de programação, e com um sistema de correção online.

Para afirmar que sua solução está correta, basta enviar o código fonte da sua solução (em geral escrito em C++ ou JAVA) para uma dessas plataformas.

Alguns desses Online Judges são citados em seguida.

### B.1 Ahmed-Aly

Juíz online que permite criar e participar de competições de programação online com problemas de outros *Online Judges*.

Também possibilita o gerenciamento das suas competições de programação e de seus amigos.

Para mais problemas de *Teoria dos Números* acesse <http://a2oj.com/Category.jsp?ID=41>.

Site: <http://a2oj.com/>

### B.2 UVa

Criado em 1995 pelo matemático Miguel Ángel Revilla, é atualmente um dos Online Judges mais famoso entre os participantes da ACM-ICPC.

É hospedado pela [Universidade de Valhadolide](#) e conta com mais de 100000 usuários registrados.

Site: <https://uva.onlinejudge.org/>

### B.3 URI

Projeto desenvolvido pelo Departamento de Ciência da Computação da [Universidade Regional Integrada](#). Contando com um enorme repositório com problemas de competições de programação, o principal objetivo desse projeto é proporcionar uma plataforma para a prática de programação e compartilhamento de conhecimentos.

Site: <https://www.urionlinejudge.com.br/>

### B.4 Topcoder

Empresa que administra competições de programação nas linguagens Java, C++ e C#.

É responsável também por aplicar competições de design e desenvolvimento de software.

Site: <https://www.topcoder.com/>

## B.5 Codeforces

Site Russo dedicado competições de programação.

Em 2013, Codeforces superou Topcoder com relação ao número de usuários ativos, apesar de ter sido criado quase 10 anos depois.

O estilo de problemas que esse site aplica é similar aos problemas encontrados na ACM-ICPC.

Site: <http://codeforces.com/>

## B.6 CodeChef

Iniciativa educacional sem fins lucrativos lançada em 2009 pela [Direct](#).

É uma plataforma de programação competitiva que suporta mais de 35 linguagens de programação.

Site: <https://www.codechef.com/>

# Bibliografia

- Arnold, A. S. et al. (1998). "A Simple Extended-Cavity Diode Laser". Em: *Review of Scientific Instruments* 69.3, pp. 1236–1239. URL: <http://link.aip.org/link/?RSI/69/1236/1>.
- Hawthorn, C. J., K. P. Weber e R. E. Scholten (2001). "Littrow Configuration Tunable External Cavity Diode Laser with Fixed Direction Output Beam". Em: *Review of Scientific Instruments* 72.12, pp. 4477–4479. URL: <http://link.aip.org/link/?RSI/72/4477/1>.
- Wieman, Carl E. e Leo Hollberg (1997). "Using Diode Lasers for Atomic Physics". Em: *Review of Scientific Instruments* 62.1, pp. 1–20. URL: <http://link.aip.org/link/?RSI/62/1/1>.