

Teoria dos Números e Computação:

Uma abordagem utilizando problemas de competições de programação

Autor: Antonio Roberto de Campos Junior

Supervisor: Carlos Eduardo Ferreira

Instituto de Matemática e Estatística - Universidade de São Paulo



Objetivos

1. Estudar tópicos específicos relacionados à Teoria dos Números;
2. Criar um material que mostre a aplicação direta dessa teoria na solução de problemas de competições de programação;
3. Demonstração da teoria e implementação dos algoritmos que resolvem os problemas que serão abordados;

Introdução

▶ Teoria do 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 do 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.

Crivo de Erastótenes

O *Crivo de Erastótenes* 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.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figure 1: Tabela usado no *Crivo de Erastóteles* com $N = 100$.

Pseudocódigo

```
Algorithm 3 Crivo de Erastótenes para o cálculo de números primos
1: procedure CRIVOERASTÓTENES ( $N$ )
2:    $isPrime[] \leftarrow \text{new Array}[N]$            ▷  $isPrime[]$  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  $isPrime[]$ 
```

Figure 2: Pseudocódigo do *Crivo de Erastóteles*.

Problema Exemplo: Goldbach's Conjecture

Link do Problema: https://uva.onlinejudge.org/index.php?option=onlinejudge&page=show_problem&problem=484

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 **Crivo de Erastótenes** 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.

```
Algorithm 5 Sum of odd primes
1: procedure SumOfPrimes( $n$ )
2:    $isPrime[] \leftarrow \text{CrivoErastotenes}(n)$ 
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"
```

Figure 3: Pseudocódigo da solução acima.

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.

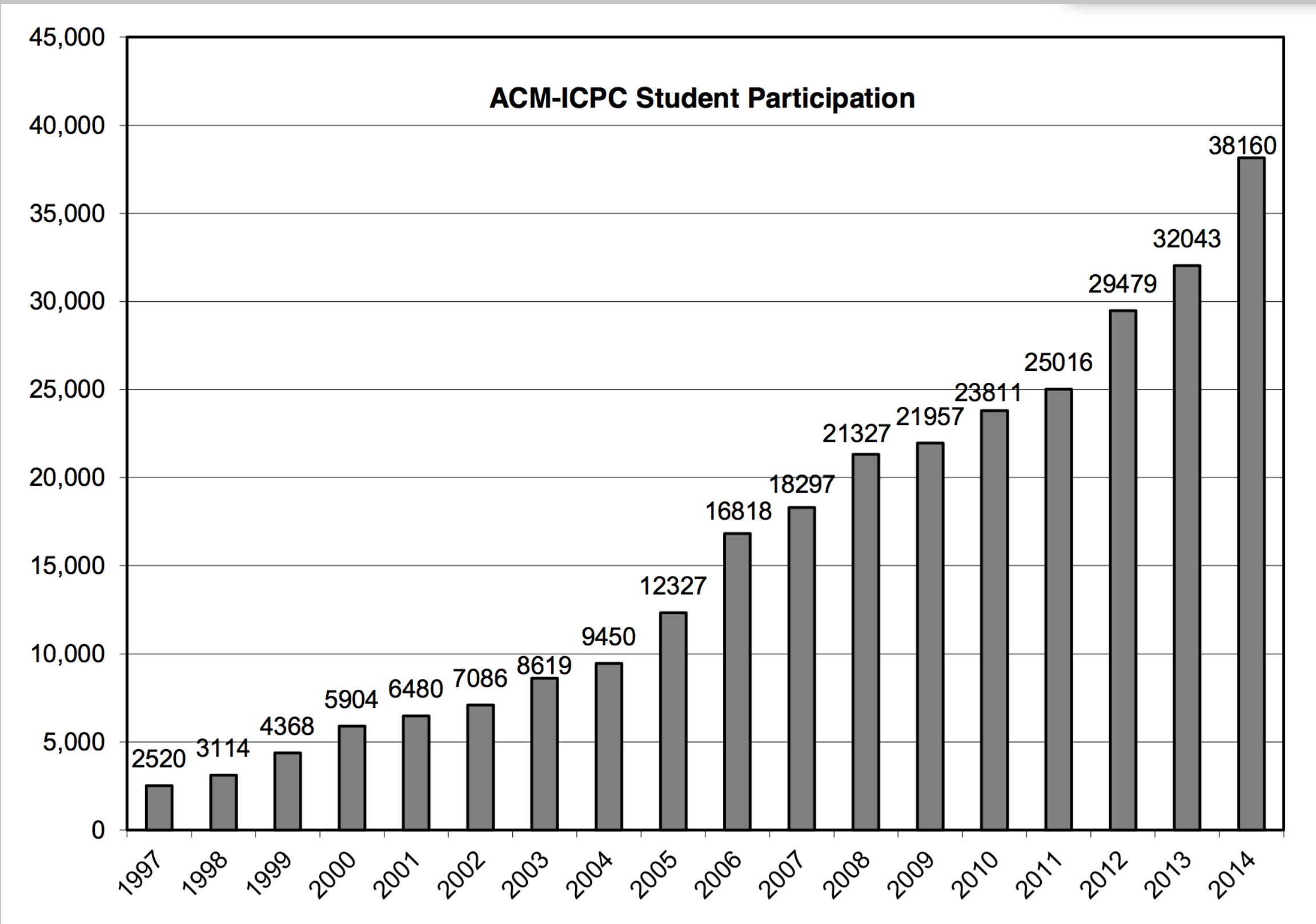


Figure 4: Crescimento do número de participantes por ano.

Acknowledgments

- ▶ Carlos Eduardo Ferreira - Auxílio durante todo o desenvolvimento desse trabalho
- ▶ Renzo Gomez Dias - Revisão dos textos

Informações para Contato

- ▶ Web: <http://www.ime.usp.br/~arcjr>
- ▶ Email: robertojr.bcc@gmail.com