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 demostração 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.

Problema exemplo: Skyscraper Floor

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

Solução Parte 1

Proposição 1: Tome $[d, x_0, y_0]$ como sendo a tupla retornada pelo $ExtendedMDC(a,b)$, 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 $q \in \mathbb{Z}$.
Teorema 1: Dados inteiros a, b, c , temos que: $MDC(a,b)|c \Leftrightarrow$ a *Equação Diofantina* $ax+by=c$, tem solução inteira.
Obs.: A proposição e o teorema citados acima foram devidamente demonstrados na monografia correspondente a esse poster encontrada em: https://github.com/AntonioRoberto/monografia/blob/master/main.pdf.

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 $Y_i + X_i t = A$ 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 ($\mathbf{0} \leq t_u \leq \frac{F-\mathbf{1}-Y_u}{X_u}$) e t_v ($\mathbf{0} \leq t_v \leq \frac{F-\mathbf{1}-Y_v}{X_v}$), tal que $Y_u + X_u t_u = Y_v + X_v t_v$, o que nos dá a *Equação Diofantina Linear* $X_u t_u + (-X_v)tv = (Y_v - Y_u)$.

Solução Parte 2

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 1**, 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 t_1, t_2 como sendo uma solução qualquer da equação diofantina $at_1 + bt_2 = MDC(a,b) = d$ (Observe que t_1 e t_2 podem ser calculados com o *Algoritmo Extendido de Euclides*), temos então pelo **Proposição 1** 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:
$t_u = (t_1\frac{c}{d} + \frac{bq}{d}) \Rightarrow \frac{-t_1 c}{b} \leq q \leq \left[(\frac{F-1-Y_u}{X_u})d - t_1 c\right]\frac{1}{b}$, já que $\mathbf{0} \leq t_u \leq \frac{F-1-Y_u}{X_u}$
Analogamente temos:
$t_v = (t_2\frac{c}{d} - \frac{aq}{d}) \Rightarrow \frac{t_2 c}{a} \geq q \geq \left[t_2 c - (\frac{F-1-Y_v}{X_v})d\right]\frac{1}{a}$, já que $\mathbf{0} \leq t_u \leq \frac{F-1-Y_u}{X_u}$
Das duas inequações acima, temos:
$max\left(\frac{-t_1 c}{b}, \left[t_2 c - (\frac{F-1-Y_v}{X_v})d\right]\frac{1}{a}\right) \leq q \leq$
$min\left(\frac{t_2 c}{a}, \left[(\frac{F-1-Y_u}{X_u})d - t_1 c\right]\frac{1}{b}\right)$
Portanto, se a inequação acima tiver solução inteira q, os elevadores u e v serão conectados pelo andar $Y_u + X_u t_u = Y_u + X_u\left[(t_1 + \frac{bq}{d})\frac{c}{d}\right]$.

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 patrocinio 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.

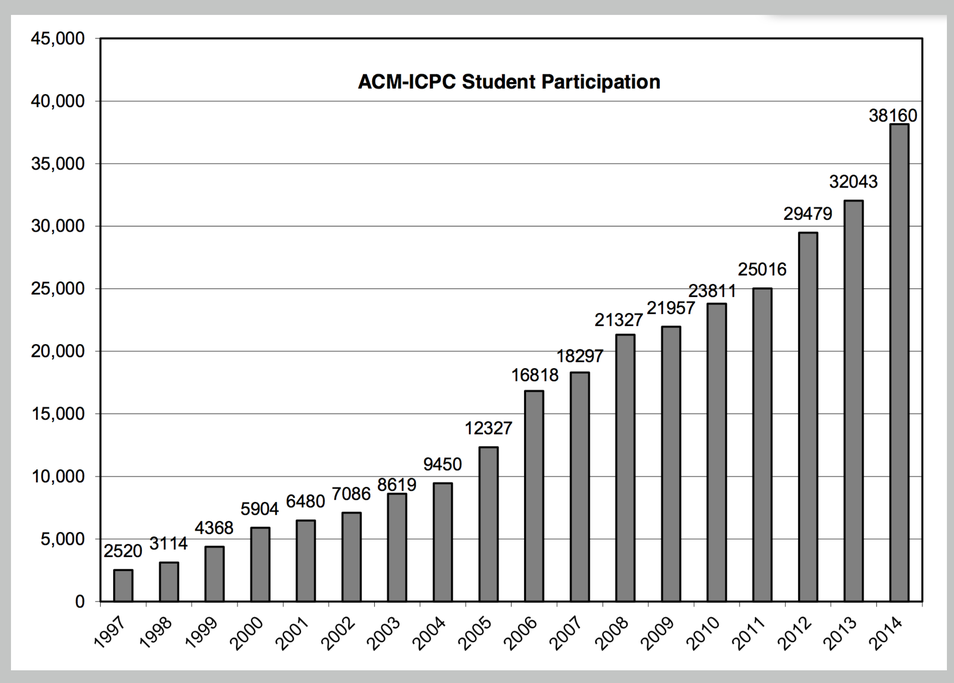

Figure 1: Crescimento do número de participantes por ano.

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