TÓPICOS EM TEORIA DOS *números*

Aula Prática

Boa noite!

ALEXANDRE HILD AONO

Aluno de graduação na UNIFESP/SJC.
Participante na organização do curso e membro do Projeto de Ensino e Aprendizagem para Olimpíadas.

Você pode me contatar em:
alexandre.aono@gmail.com

CODING IN THE *Cold*

Visando orientar e preparar os alunos dos cursos de graduação e início de pós-graduação da área de computação para a Maratona de Programação, competição organizada pela Sociedade Brasileira de Computação (SBC), o evento é uma iniciativa do "Projeto de Ensino e Aprendizagem de Programação para Olimpíadas", um projeto de extensão do Instituto de Ciência e Tecnologia da Universidade Federal de São Paulo (ICT-UNIFESP) de São José dos Campos, coordenado pelo Prof. Dr. Reginaldo Massanobu Kuroshu

TÓPICOS EM TEORIA DOS NÚMEROS

Profa. Dra. Grasiele Cristiane Jorge

Tópicos abordados:

- Números primos
- Divisibilidade
- MMC e MDC
- Aritmética Modular
- Congruência

AULA PRÁTICA

- Encontrando Primos
- Máximo Divisor Comum
- Problema 1
- Problema 2

Para mais informações acesse nosso site http://programathonunifesp.wix.com/cursodeinverno

FATORAÇÃO EM NÚMEROS PRIMOS

Encontrando Primos

A maneira mais simples de testar se um dado número é primo é realizando divisões repetidas. Comece pelo menor candidato a divisor e então teste todas as divisões a partir dali.

UTILIZANDO *um fato interessante*

- Tendo em vista que o 2 é o único número primo par, só é necessário verificar os números ímpares como possíveis candidatos.

- Um dado número n pode ser considerado primo se esse número não possui fatores primos menores que $\sqrt{n}$.

Suponha que x não é primo e possui um fator primo p maior do que $\sqrt{n}$.

Então, podemos afirmar que x/p também divide x e deve ser maior que p (considerando etapas da fatoração).

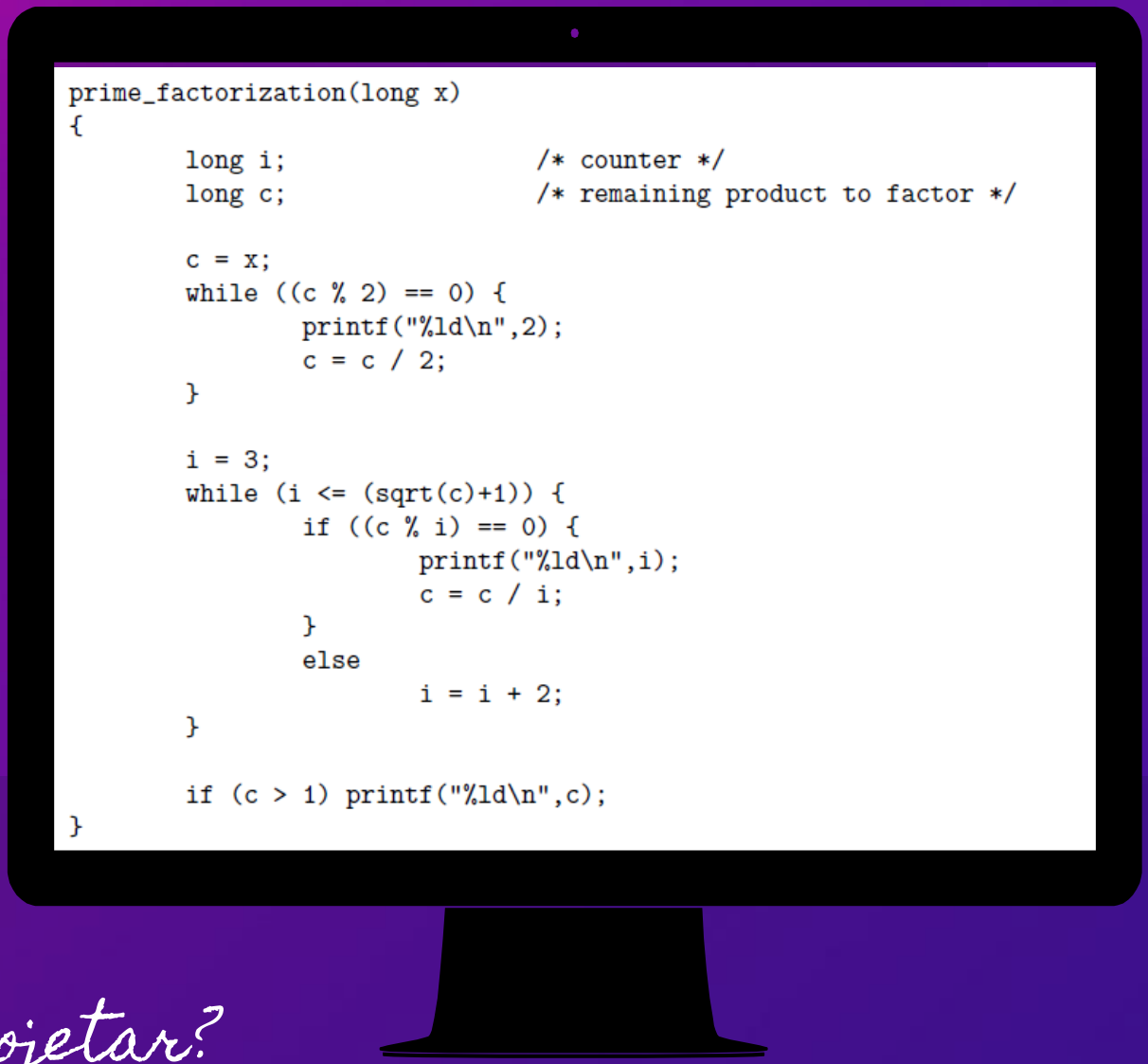
Como temos que $p > \sqrt{n}$ e $\frac{x}{p} > \sqrt{n}$, então temos que o produtos de dois números maiores que $\sqrt{n}$ deve ser maior que n, o que é uma contradição.

Provando o *teorema*

Utilizaremos esse fato para nosso *algoritmo!*

Exercício

Fatore um dado número imprimindo todos os seus componentes primos em ordem crescente.



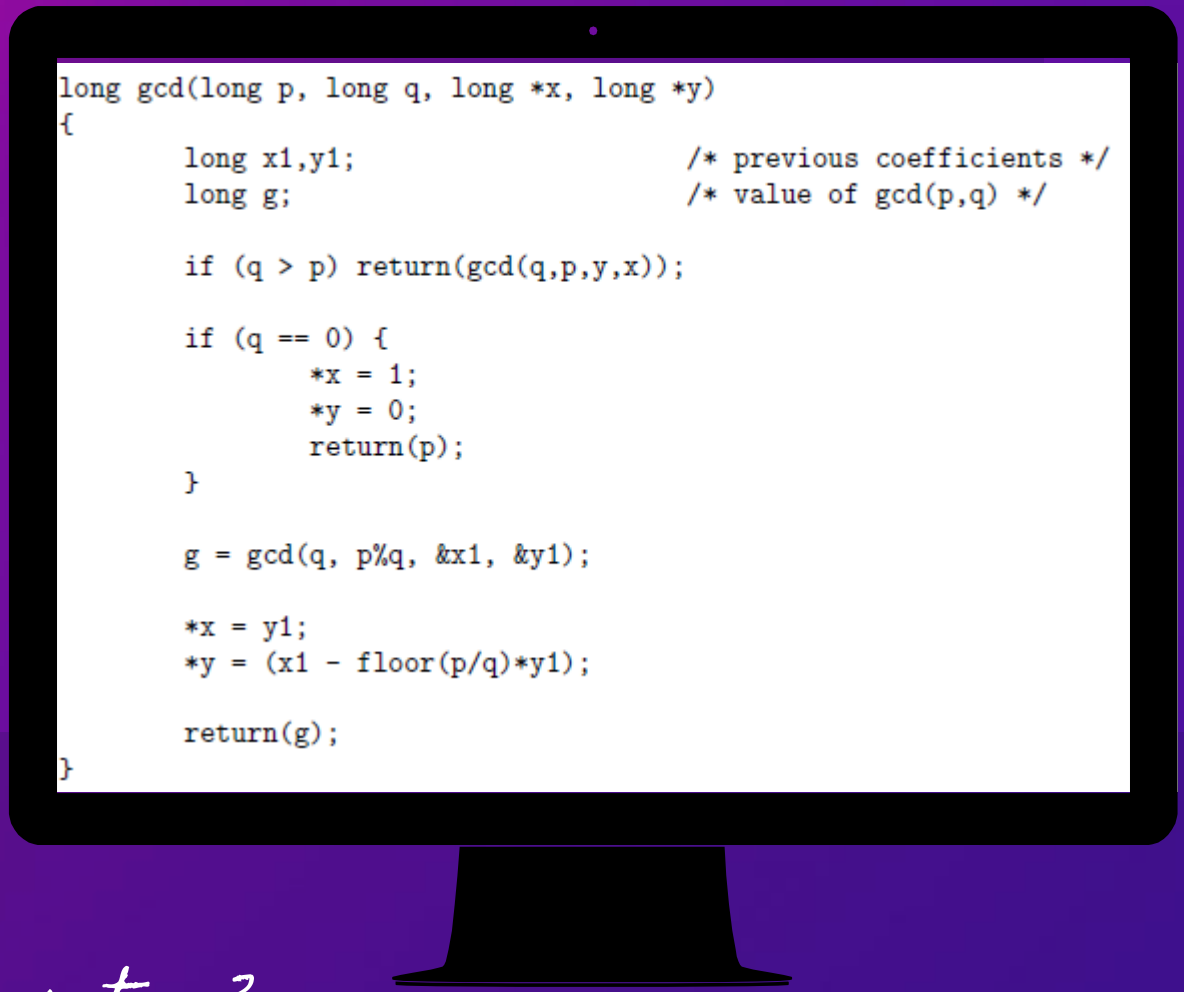
E aí consegue *projetar?*

Pseudocódigo para fatoração de um dado número.

ALGORITMO DE EUCLIDES

MÁXIMO DIVISOR COMUM

Dados dois números inteiros a e b, encontre dois números x e y tais que $a * y + b * y = mdc(a, b)$



```
long gcd(long p, long q, long *x, long *y)
{
        long x1,y1;                     /* previous coefficients */
        long g;                         /* value of gcd(p,q) */

        if (q > p) return(gcd(q,p,y,x));

        if (q == 0) {
                *x = 1;
                *y = 0;
                return(p);
        }

        g = gcd(q, p%q, &x1, &y1);

        *x = y1;
        *y = (x1 - floor(p/q)*y1);

        return(g);
}
```

E aí consegue *projetar?*

Pseudocódigo para o algoritmo de Euclides.

Exercício Final

https://www.urionlinejudge.com.br/judge/pt/problems/view/1307

Obrigado!

ALGUMA PERGUNTA?

Você pode me contatar em:
alexandre.aono@gmail.com