Teoria dos números

Introdução

- **O que é a teoria dos números?**

  - A teoria dos números se distingue não pelos seus métodos mas sim por seus problemas, cujo o tema comum subjacente é o de numero inteiro

  - Sua principal característica é o fato de ser multidisciplinar

Equação Diofantina

- A **Equação Diofantina** é uma equação polinomial que permite a duas ou mais variáveis assumirem apenas valores inteiros

- Os problemas Diofantinos se resumem a achar inteiros que deverão funcionar corretamente para todas as equações.

Teorema de Euler

- o Teorema de Euler estabelece que se *n* é um inteiro positivo e *a* é um inteiro positivo co-primo de *n* então:

$$a^{phi^{\wedge}(n)} \equiv 1 (\text{mod } n)$$

- A expressão

$$a \equiv b (\text{mod } n)$$

significa que a e b se encontram na mesma "classe de congruência" módulo n, ou seja, que ambos deixam o mesmo resto se os dividirmos por n, ou, o que é equivalente, a-b é um múltiplo de n.

Teorema Euclidiano

O teorema euclidiano que garante uma infinidade de números primos pela teoria dos números

- Tomando-se L uma lista finita qualquer de números primos:
- Pode-se mostrar que existem números primos que não estão nessa lista. Da seguinte maneira:
  - Sendo P o produto de todos os números primos na lista: P={p1,p2,p3,...,pn}
  - E sendo q=P+1
  - Então, q pode ser primo ou não:
  - Se q é primo então há pelo menos um número primo a mais que não está listado.
  - Se q não é primo, então algum fator primo p divide q. Esse fator p não está na nossa lista L: se estivesse, ele dividiria P (pois P é o produto de todos os número na lista), mas como sabemos, p divide $P + 1 = q$. Então, para não deixar resto, p teria que dividir a diferença entre os dois números, que é $(P + 1) - P$ ou seja, 1. Mas não existe número primo que divida 1, assim haveria uma contradição, logo, p não pode estar na lista. Isso significa que pelo menos mais um número primo existe além dos que estão na lista.

Funções matemáticas úteis

#include <math.h>

- **Potências**
  - *pow ()*: Retorna o valor da base elevada ao expoente. Recebe dois argumentos ,o primeiro é a base e o segundo o expoente.
  - *sqrt ()*: Retorna o valor da raiz quadrada.
- **Arredondamento**
  - *ceil()*: Retorna o primeiro float sem casas decimais acima. Exemplo: ceil (45.98561) resultaria em 46.
  - *floor()*: Retorna o primeiro float sem casas decimais abaixo. Exemplo: floor (45.98561) resultaria em 45.

Critérios de divisibilidade

- Por 2: Todo número par.
- Por 3: Se a soma dos dígitos for divisível por 3.
- Por 4: Se dois últimos dígitos do número for dívisel por 4.
- Por 5: Quando o número termina com 0 ou 5.
- Por 9: Se a soma dos dígitos for divisível por 9.
- Por 10: Quando o número termina com 0.

Números Primos

- Um número é primo, se somente se, for dívisivel por 1 e por ele mesmo.
  - Primos = {2,3,5,7,11,13,17...}

Converter número real em fração

- $1{,}25 \Rightarrow \frac{125}{100} \Rightarrow \frac{125^{:5}}{100^{:5}} \Rightarrow \frac{25^{:5}}{20^{:5}} \Rightarrow \frac{5}{4}$

- $\frac{5}{4} \Rightarrow 5 : 4 \Rightarrow 1{,}25$

Mediana

- Se o conjunto ordenado de dados for ímpar, a mediana será o elemento central.
- Ex: A = {1,2,3,4,5} Med(A) = 3

- Se o conjunto ordenado de dados for par, a mediana será a média dos dois elementos centrais.
- Ex: A = {1,2,3,4,5,6} Med(A) = 3,5

Multíplos e divisores

- A é multíplo de B, se o produto de um inteiro k por B resulta em A.
- Ex: A = k * B

  6 = 2 * 3

- A é dívisivel por B, se a razão de A por B possui resto 0.
- Ex: A % B == 0

  8 % 4 == 0