Notas sobre teoria dos números (1)

Anjolina Grisi de Oliveira

Teorema 1 (Teorema Fundamental da Aritmética) *Todo inteiro positivo pode ser escrito como o produto de primos, e essa fatoração é única a menos da ordem dos fatores primos.*

Exemplo 1 *Aplique o teorema fundamental da aritmética para provar que* $\sqrt{2}$ *é irracional.*

Teorema 2 *Se* n *é um número composto, então* n *possui um divisor primo menor ou igual a* $\sqrt{n}$

Exemplo 2 *Mostre que 101 é primo.*

Alguns resultados sobre os números primos

Teorema 3 *Existe uma quantidade infinita de números primos.*

Teorema 4 *Para todo inteiro positivo* k *, existem* k *inteiros compostos consecutivos.*

Definição 1 (primos gêmeos) *Dois primos cuja a diferença é dois são chamados de números primos gêmeos.*

Exemplo 3 $(3, 5),\ (5, 47),\ (11, 13)$

Teorema 5 (O teorema do número primo) *Suponha que* $\pi(n)$ *represente a quantidade de primos entre* $1 \ldots n$*. Então* $\pi(n)$ *é aproximadamente igual a* n/lnn*.*

Teorema 6 (O pequeno teorema de Fermat) *Se* p *é primo e* a *é um inteiro, então* $p \mid a^p - a$*. (outra versão: se* p *é um primo e* a *é um inteiro não divisível por* p*, então* $p \mid a^{p-1} - 1$*).*

- Infelizmente, existem números compostos de forma que $n \mid 2^{n-1} - 1$. Esses núemros são chamados de pseudoprimos.

Exemplo 4 *O inteiro 341 é um pseudoprimo pois* $341 \mid 2^{340} - 1$

Maior divisor comum e menor múltiplo comum

Definição 2 (Maior divisor comum) *Sejam a e b inteiros de forma que apenas um dels pode ser zero. O maior inteiro d de foram que $d \mid a$ e $d \mid b$ é chamado de maior divisor comum de a e b, denotado por $mdc(a, b)$.*

- Uma maneira de encontrar o mdc de dois núemros é encontrar a fatoração prima desses números. Portanto sejam as fatorações de a e b dadas como a seguir:
  - $a = p_1^{a1} p_2^{a2} \dots p_n^{an}$
  - $b = p_1^{b1} p_2^{b2} \dots p_n^{bn}$
- $mdc(a, b) = p_1^{min(a1,b1)}, p_2^{min(a_2,b_2)} \dots p_n^{min(an,bn)}$

Definição 3 (primos entre si) *Os inteiros a e b são primos entre si se seu mdc é 1.*

Definição 4 (primos entre si dois a dois) *Os inteiroa $a_1, a_2, \dots a_n$ são primos entre si dois a dois se $mdc(a_i, a_j) = 1$ para $1 \leq i < j \leq n$.*

Definição 5 (o menor múltiplo comum) *O menor múltiplo comum de dois inteiros positivos a e b é o menor inteiro positivo que é divisível pelos dois, a e b. O menor múltiplo comum é denotado por $mmc(a, b)$.*

- $mmc(a, b) = p_1^{max(a1,b1)}, p_2^{max(a_2,b_2)} \dots p_n^{max(an,bn)}$

Exemplo 5 *prove que se a e b são inteiros postivos então $ab = mdc(a, b).mmc(a, b)$*