Introdução à Teoria dos Números

Números Primos e Teorema Fundamental da Aritmética

Definição 1: Seja n (n > 1) um número inteiro. Dizemos que:

i) n é **primo** se os único divisores positivos de n são 1 e n.

ii) n é **composto** se n não é primo.

Exemplos: 3 é primo pois $D^+(3) = \{1, 3\}$.
6 é composto pois $D^+(6) = \{1, 2, 3, 6\}$.

OBS:

1) 2 é o único número primo par.
2) Em outras palavras: n é primo, se sempre que n = ab necessariamente (n = a e b = 1) ou (n = b e a = 1).

Proposição 1: Seja $n \geq 2$ um número inteiro. Então existe um número primo p tal que $p \mid n$.

Demonstração: Seja $S = \{d \text{ é inteiro} / d \geq 2 \text{ e } d \mid n\}$. $S \neq \varnothing$ pois $n \in S$. Além disso S é subconjunto dos inteiros positivos. Assim, pelo Princípio da Boa Ordenação existe d_0 que é o menor elemento de S.
Provemos que d_0 é primo.
Suponhamos que d_0 seja composto tal que $d_0 = ab$, com $1 < a < d_0$ e $1 < b < d_0$. Como $a \mid d_0$ e $d_0 \mid n$ então $a \mid n$. Como $a \geq 2$ e $a \mid n$ então $a \in S$, o que é absurdo pois a seria maior que d_0 (d_0 é o menor elemento de S). Logo d_0 é primo.

Proposição 2: Se $p \mid ab$ e p é primo então $p \mid a$ ou $p \mid b$.

Demonstração: Se p não divide a então (a, p) = 1. Pelo Teorema 2 (MDC) temos que $p \mid b$.

Proposição 3: Seja $n \geq 2$ um número inteiro. Se n é composto, então existe um primo p tal que $p \mid n$ e $p \leq \sqrt{n}$.

Demonstração: Como n é composto então n = ab com $1 < a < n$ e $1 < b < n$. Suponhamos que $a \leq b$.

Afirmação: $a \leq \sqrt{n}$. De fato $a \leq b \Rightarrow a \leq \frac{n}{a} \Rightarrow a^2 \leq n \Rightarrow \sqrt{a^2} \leq \sqrt{n} \Rightarrow a \leq \sqrt{n}$.
Como $a \geq 2$ então pela proposição 1, existe um primo p tal que p | a. Como a | n então p | n. Além disso $p \leq a \leq \sqrt{n}$.

A proposição 3 tem uma importante aplicação prática. Ela nos diz que, para testarmos se um número é primo, é suficiente testarmos divisibilidade apenas pelos primos $\leq \sqrt{n}$.

Exemplo: Verifique que 101 é primo.

$\sqrt{101} \approx 10$,.....
Se p é primo e $p \leq \sqrt{101}$ então p pode assumir os valores: 2, 3, 5 ou 7.
Como 101 não é divisível por 2, 3, 5 e 7 então pela proposição 3, 101 não pode ser composto. Logo 101 é primo.

Crivo de Eratóstenes

Se desejamos obter a lista de todos os primos menores que n devemos excluir dentre os números ímpares de 2 a n aqueles que são múltiplos de todos primos menores ou iguais a $\sqrt{n}$.

Exemplo: Listar todos os primos menores que 57.

Listar todos os ímpares compreendidos entre 2 e 57:

3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57.

$\sqrt{57} \approx 7$,...
Vamos excluir agora os múltiplos de 3, 5 e 7.
Múltipos de 3: 9, 15, 21, 27, 33, 39, 45, 51, 57.
Múltiplos de 5: 15, 25, 35, 45, 55.
Múltiplos de 7: 21, 35, 49.

Logo todos os primos menores que 57 são:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 e 53.

Teorema 1: Existem infinitos números primos.

Demonstração: Faremos a demonstração por absurdo. Suponhamos que exista somente uma quantidade finita de números primos. Sejam estes números: p_1, p_2, p_3, ..., p_n. Consideremos o número: $k = p_1 . p_2 . p_3 \ldots p_n + 1$. Como k é inteiro e $k \geq 2$, então pela proposição 1, existe um primo p tal que p | k. Segue então que $p = p_i$ para algum i entre 1, 2, 3, ..., n. Logo $p_i \mid k$. Mas $p_i \mid p_1 . p_2 . p_3 \ldots p_n$. Assim $p_i \mid k - p_1 . p_2 . p_3 \ldots p_n$. Como $k - p_1 . p_2 . p_3 \ldots p_n = 1$ então $p_i \mid 1$, o que implica $p_i = 1$, o que é um absurdo pois p_i é primo. Logo existem infinitos primos.

Proposição 4: Para qualquer inteiro positivo n, existem n inteiros consecutivos compostos. Em ouras palavras: "Existem saltos arbitrariamente grandes na sequência dos números primos".

Demonstração: Consideremos os números:

$(n+1)! + 2 = (n+1).\ n\ .\ (n-1).\ ...\ .\ 3\ .\ 2 + 2$

$(n+1)! + 3 = (n+1).\ n\ .\ (n-1).\ ...\ .\ 3\ .\ 2 + 3$
.
.
.
$(n+1)! + (n+1) = (n+1).\ n\ .\ (n-1).\ ...\ .\ 3\ .\ 2 + (n+1).$

Temos que:
$2 \mid (n+1)! + 2$
$3 \mid (n+1)! + 3$
.
.
.
$(n+1) \mid (n+1)! + (n+1)$

A sequência de números acima é composta por n números compostos e consecutivos.

Teorema Fundamental da Aritmética

A importância dos números primos de deve ao fato de que qualquer inteiro pode ser construído multiplicativamente a partir deles. Com efeito, se um número não é primo, podemos decompô-lo até que seus fatores sejam todos primos.
Por exemplo:
$360 = 3.\ 120 = 3.\ 30.\ 4 = 3.\ 3.\ 10.\ 2.\ 2 = 3.\ 3.\ 5.\ 2.\ 2.\ 2 = 2^3.\ 3^2.\ 5$

Observemos que se um número foi expresso como produto de primos, podemos dispor estes fatores em uma ordem qualquer. A experiência demonstra que, salvo pela arbitrariedade da ordenação, a decomposição de um número inteiro positivo em fatores primos é única. Esta afirmação parece à primeira vista evidente, entretanto não é uma trivialidade e sua demonstração requer algumas sutilezas. Este resultado é conhecido por:

Teorema 2 (Teorema Fundamental da aritmética): Um número inteiro $n \geq 2$ ou é primo ou pode ser escrito de maneira única, a menos da ordem dos fatores, como produto de números primos.

Demonstração: Para demonstrar este teorema precisamos provar duas coisas:
1ª: Existência da decomposição.

2ª: A unicidade da decomposição.

1ª: Se n é primo, nada há que demonstrar, pois já está fatorado. Suponhamos então que n seja composto. Pela proposição 1, existe um número primo p tal que $p_1 \mid n$. Assim existe x_1 inteiro tal que $n = p_1 . x_1$ onde $1< x_1< n$. Se x_1 é primo então a prova está completa. Se x_1 é composto, então pela proposição 1, existe um número primo p_2 tal que $p_2 \mid x_1$. Assim existe x_2 inteiro tal que $x_1 = p_2 . x_2$ onde $1< x_2< x_1$. Podemos então escrever $n = p_1 . p_2 . x_2$. Se x_2 é primo então a prova está completa. Se x_2 é composto, seguimos o mesmo raciocício. Com isso obteremos uma sequência decrescente: $n > x_1 > x_2 > x_3 > ... > 1$ e como existe um número finito de inteiros positivos menores que n e maiores que 1, existirá um inteiro p_k primo tal que $n = p_1 . p_2 . p_3 .... p_k$.

2ª: Suponhamos que n admite duas decomposições como produto de fatores primos, isto é:

$n = p_1 . p_2 . p_3 . ... p_r = q_1 . q_2 . q_3 .... q_s$ com $r \leq s$ e = $p_1 \leq p_2 \leq p_3 \leq ... \leq p_r$ e $q_1 \leq q_2 \leq q_3 \leq ... \leq q_s$.

Dessa forma $p_1 \mid q_1 . q_2 . q_3 .... q_s \Rightarrow p_1 = q_i$ para algum i $\Rightarrow p_1 \geq q_1$.
Analogamente $q_1 \mid p_1 . p_2 . p_3 . ... p_r \Rightarrow q_1 = p_j$ para algum j $\Rightarrow q_1 \geq p_1$.
Logo $p_1 = q_1$. Assim $p_2 . p_3 . ... p_r = q_2 . q_3 .... q_s$. Com o mesmo raciocínio conclui-se que $p_2 = q_2$ e assim por diante. Então se $r < s$, temos a igualdade
$1 = q_{r+1} . q_{r+2} . ... q_s$, o que é um absurdo pois $q_{r+1}, q_{r+2}, ...$ e q_s são primos.
Portanto $r = s$ e $p_1 = q_1$, $p_2 = q_2$, ..., $p_r = q_r$.

OBS: A decomposição em primos de um inteiro $n \geq 2$ pode ser dada da forma:

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} ... p_r^{a_r}$$

Ou seja, podem existir fatores primos repetidos.

Exemplo: $540 = 2^2 . 3^3 . 5$.