Aula 9. Primos e Teorema Fundamental da Aritmética

9.1 Números primos

Definição

Um inteiro positivo p e chamado primo se tem exatamente dois divisores positivos: 1 e p.

Observação 9.1

Observem que $a = 1$ hao é primo, pois tem apenas um divisor positivo 1.

Definição

Um inteiro $m > 1$ é chamado *composto* quando não é primo.

Exemplo 9.1

Temos que

$$2, 3, 5, 7, 11, 13, \ldots$$

são primos, e $4, 6, 8, 9, 10, 12, 14, \ldots$ são compostos

Proposição 9.1

Sejam: p - um primo, e a, b inteiros.Assim

(1) Se $p \nmid a$ assim $\text{mdc}(p, a) = 1$.

(2) Se $p \mid ab$ assim $p \mid a$ ou $p \mid b$.

Prova

(1) Se $p \nmid a$, assim tem apenas um divisor positivo em comum entre p e a é 1. Logo $\text{mdc}(p,a) = 1$.

(2) Seja $p \mid ab$. Suponha que $p \nmid a$, assim usando resultado de (1) temos que $\text{mdc}(p,a) = 1$.
Agora $p \mid ab$ e $\text{mdc}(p,a) = 1$ implicam que (vejam Aula 6, Proposição 6.1) que $p \mid b$ o que precisaremos de provar.

Corolário 9.1

Se um primo p é tal que $p \mid a_1 \cdot \cdots \cdot a_n$, assim $p \mid a_i$ para algum i.

Prova

È exercicio para casa usando (PIF).

Corolário 9.2

Se um primo p é tal que $p \mid q_1 \cdot \cdots \cdot a_n$ com q_i números primos, assim $p = q_i$ paia algum i

Prova

Pelo Corolário 9.1 temos que $p \mid q_1$ para algum i. Como q_i é primo temos que $p = 1$ ou $p = q_i$. Mas p é primo também, assim $p = q_i$.

9.2 *Quantos primos tem? + Exercícios*

Os números primos formar uma sequencia

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

Em principio não é claro que tem numero infinito nessa sequencia.
Mas de fato isso é verdade como o seguinte Teorema diz

Teorema 9.1

Existem numero infinito dos primos

Prova

Suponha que tem numero finito dos primos e sejam

$$p_1, \ldots, p_t$$

todos esses primos. Considere

$$n = p_1 \cdot \ldots \cdot p_t + 1,$$

como $n > p_i$ para todos i temos que n é composto (pois não é primo). Logo existe algum p_i com $p_i \mid n$.
Assim, temos que

$$p_i \mid p_1 \cdot \ldots \cdot p_t$$

e

$$p_i \mid p_1 \cdot \ldots \cdot p_t + 1 = n,$$

portando p_i divide diferença entre estes dois números, ou seja $p_i \mid 1$. È contradição, pois $p_i > 1$.

Exercício 9.1

Mostre que único primo da forma $p = n^3 - 1$ é 7.

Solução 9.1

Temos

$$p = n^3 - 1 = (n-1) \cdot (n^2 + n + 1).$$

Como p é primo assim um dos fatores é 1. Considere duas possibilidades. Se $n - 1 = 1$, assim $n = 2$, logo

$$p = n^3 - 1 = 7.$$

Por outro lado, se $n^2 + n + 1 = 1$, assim $n = 0$, ou $n = -1$. Se $n = 0$, assim

$$p = n^3 - 1 = -1.$$

não é um primo. Se $n = -1$, assim

$$p = n^3 - 1 = -2.$$

não é um primo. Logo única possibilidade possível é $n = 2$ e $p = 7$ neste caso.

Exercício 9.2

Mostre que para todo $n > 1$ o numero $n^4 + 4$ é composto.

Solução 9.2

Complementando para quadrado perfeito, temos

$$\begin{aligned} n^4+4 &= n^4+4n^2+4-4n^2 \\ &= \left(n^2+2\right)^2-(2n)^2 \\ &= \left(n^2+2+2n\right)\cdot\left(n^2+2-2n\right). \end{aligned}$$

Agora, observem que

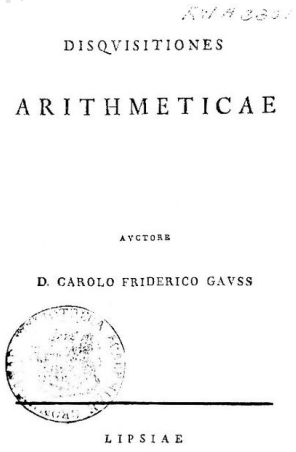
$$n^2+2-2n=(n-1)^2+1>1,$$

para todos $n>1$. Mesmo para n^2+2+2n.

Assim n^4+4 decomponha-se em produto de dois inteiros que não igual a 1, logo n^4+4 é composto.

9.3 *Teorema Fundamental da Aritmética*

As pré-condições do Teorema Fundamental da Aritmética têm suas origens na Grécia antiga. Apesar do fato de que na matemática grega antiga o teorema básico da aritmética na formulação moderna não ocorre, nos "Princípios" de Euclides existem sentenças equivalentes a ele. Seguindo o Euclides, muitos matemáticos ao longo dos séculos contribuíram para a prova do Teorema Fundamental da Aritmética, citando afirmações semelhantes em seus trabalhos. A primeira formulação exata do teorema básico da aritmética e sua prova são dadas por K. Gauss no livro "Arithmetic research" (Latin Disquisitiones Arithmeticae), publicado em 1801. Desde então, muitas novas provas diferentes do teorema apareceram, competindo entre si por beleza e originalidade.


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

Theorem 9.2: (Fundamental da Aritmética)

Qualquer inteiro $n>1$ pode ser escrito como produto dos prinos Tal apresentação é único a menos de ordem dos primos no produto.

Prova

Primeiro vamos mostrar que todo inteiro $n > 1$ decomponha-se em produto dos primos. Usaremos a segunda forma do Princípio de Indução. Para $n = 2$ o anunciado é verdadeiro, já que 2 é, ele próprio, um número primo.
Suponhamos agora que o resultado seja verdadeiro para todo inteiro b com $2 \leq b < n$.
Mostraremos que também vale para n. Se n é primo, assim não há nada para mostrar. Caso contrario, n admite um divisor positivo b tal que $1 < b < n$. Isto é, $n = bc$, e para c temos também $1 < c < n$. Pela hipótese de indução, b e c c podem ser escritos como produto de primos, na forma $b = p_1 \dots p_s, c = q_1 \cdots q_k$. Substituindo, temos $n = p_1 \cdots p_s q_1 \dots q_k$, e o resultado também vale para n.
Agora vamos cuidar unicidade dessa decomposição. Suponha que n decomponha-se em duas maneiras

$$p_1 \cdots p_r = n = q_1 \cdot \dots q_s,$$

com $p_1 < \cdots < p_r$ e $q_1 < \cdots < q_s$. Precisamos mostra que $r = s$ e $p_i = q_i$. Como $p_1 \mid n = q_1 \cdot \dots q_s$ assim pelo Corolário 9.2 temos que $p_1 = q_j$ e portanto $p_1 \geq q_1$ analogamente $q_1 \geq p_1$ logo $p_1 = q_1$. Cancelando, temos

$$p_2 \cdots p_r = q_2 \cdot \dots q_s.$$

Repetindo o processo, e se $r > s$ temos $1 = q_{r+1} \dots q_s$. Assim primos $q_{r+1}, \dots, q_s$ devem ser inversíveis. Contradição, assim $r = s$ e $p_1 = q_1, \dots, p_s = q_s$ pelo analise acima.

Observação 9.2

Claro que alguns dos prinos podem acontecer mais que uma vez na fatoração, por exemplo

$$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3,$$
$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2.$$

Agrupando os primos eventualmente repetidos na decomposição de n (como no observação acima), podemos enunciar o teorema anterior de forma levemente diferente. Também podemos estendê-lo a números negativos.

Theorem 9.3: (Fundamental da Aritmética)

Seja $n > 1$ um inteiro. Assim n pode ser escrito unicamente na sua forma canonica

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k},$$

onde $p_1 < p_2 < \cdots < p_k$ são primos e $\alpha_1, \alpha_2, \dots, \alpha_r$ inteiros positivos.

Consideremos alguns exemplos particulares. A decomposição em fatores primos dos números 360 e 4725 é

$$360 = 2^3 \cdot 3^2 \cdot 5$$
$$4725 = 3^3 \cdot 5^2 \cdot 7$$

Os primos que comparecem numa e noutra decomposição não são todos iguais; porém usando expoentes iguais a 0, podemos dan

decomposições com os mesmos primos:

$$360 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^0$$
$$4725 = 2^0 \cdot 3^3 \cdot 5^2 \cdot 7$$

Naturalmente, isso pode ser feito para qualquer par de números. Tal decomposição permite usar o Teorema Fundamental da Aritmética para encontrar o mdc e mmc de dois números dados, o que vamos ver na próxima aula.

Além disso o teorema facilmente pode ser estendida para números negativos também na seguinte maneira

Theorem 9.4: (Fundamental da Aritmética)

Seja n um inteiro diferente de 0, 1 e -1 . Então, existem primos $p_1 < p_2 < \ldots < p_k$ e inteiros positivos $\alpha_1, \alpha_2, \ldots, \alpha_k$ tais que

$$a = \pm p_1^{\alpha_1} \ldots p_r^{\alpha_k}.$$

Além disso, essa decomposição é única.

Exercício 9.3: (Trabalho p/ casa)

Mostre que se $n > 4$ não é primo, então $n \mid (n-1)!$.

Exercício 9.4: (Trabalho p/ casa)

Prove que nenhum inteiro da forma $8^n + 1$ é primo.

Exercício 9.5: (Trabalho p/ casa)

Mostre que se o inteiro $2'' - 1$ é primo, então n é primo.