Aula 10. Fatos sobre números primos

10.1 MDC e MMC atraves os primos

Na aula passada a gente definiu o que são os números primos e vimos as propriedades básicas deles.

Vamos lembrar que um inteiro positivo p e chamado *primo* se tem exatamente dois divisores positivos: 1 e p.

Na aula passada a gente provou o seguinte Teorema Fundamental da Aritmética.

Theorem 10.1: (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.

O Teorema Fundamental da Aritmética desempenha o papel importante na matemática. Por exemplo ela permite calcular o mdc e mmc de dois números dados. Na aula passada vimos que dados dois inteiros a e b positivos diferentes de 1 podemos escrever eles na seguinte forma

$$a = p_1^{\alpha_1} \cdots p_t^{\alpha},$$
$$b = p_1^{\beta_1} \ldots p_t^{\beta_t}$$

onde, $p_1 < p_2 < \cdots < p_t$ primos e $\alpha_1, \alpha_2, \ldots, \alpha_t$ e $\beta_1, \beta_2, \ldots, \beta_t$ são inteiros não-negativo. Por exemplo

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

Anotações MA12 Kostiantyn

Theorem 10.2: (MDC e MMC através TFA)

Sejam

$$a = p_1^{\alpha_1} \cdots p_t^{\alpha},$$
$$b = p_1^{\beta_1} \ldots p_t^{\beta_t}$$

inteiros nas condições acima. Então,

$$\text{mdc}(a,b) = p_1^{\gamma_1} \ldots p_t^{\gamma_t}, \text{ em que } \gamma_j = \min(\alpha_i, \beta_i).$$
$$\text{mmc}(a,b) = p_1^{\delta_1}, \ldots p_t^{\delta_t}, \text{ em que } \delta_i = \max(\alpha_i, \beta_i)$$

A prova sera baseada na seguinte lema

Lemma 10.1

Sejam

$$a = p_1^{\alpha_1} \cdots p_t^{\alpha},$$
$$d = p_1^{\beta_1} \ldots p_t^{\beta_t}$$

inteiros nas condições acima. Assim $d \mid a$ se e somente se $\beta_i \leq \alpha_i$ for all i.

Prova

Se $d \mid a$, existe um inteiro positivo c tal que $a = dc$. Escrevendo $c = p_1^{r_1} \cdots p_t^{r'}$, temos que :
Do Teorema Fundamental de Aritmética, vem que $\alpha_i = \beta_i + r_i$, donde $\alpha_i \geq \beta_i$, $1 \leq i \leq t$.
Reciprocamente, se $\alpha_i \geq \beta_i$ para todos i, chamando $r_i = \alpha_i - \beta_i$ temos que

$$a = p_1^{\beta_1 + r_1} \ldots p_t^{\beta_t + r_t} = d \cdot p_1^{r_1} \ldots p_t^{r_t}$$

Logo, $d \mid a$.

Agora vamos dar esboço da prova do Teorema anterior.

Prova

Bastará provar que os inteiros $p_1^{\gamma_1} \ldots p_t^{\gamma_t}$ e $p_1^{\delta_1}, \ldots p_t^{\delta_t}$ verificam as caracterizações do mdc e mmc respectivamente. Isto seguirá facilmente do uso repetido do lema anterior. Deixamos a tarefa a cargo do leitor.

Anotações de Aula, Prof. Kostiantyn

Exemplo 10.1

Suponha que $a = 30$, e $b = 36$, assim

$$a = 30 = 2 \cdot 3 \cdot 5 = 2 \cdot 3^1 \cdot 5^1,$$
$$b = 36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2 \cdot 5^\circ.$$

Portanto

$$\text{mdc}(30, 36) = 2 \cdot 3^1 \cdot 5^0 = 6,$$
$$\text{mmc}(30, 36) = 2^2 \cdot 3^2 \cdot 5^1 = 180.$$

Exemplo 10.2

Suponha que $a = 360$, e $b = 152$. Fatorando estes dois numeros, temos

$$\begin{array}{rlrl} 360 = & 2 \cdot 180 & 152 = & 2 \cdot 76 \\ 180 = & 2 \cdot 90 & 76 = & 2 \cdot 38 \\ 90 = & 2 \cdot 45 & 38 = & 2 \cdot 19 \\ 45 = & 3 \cdot 15 & 19 = & 19 \cdot 1 \\ 15 = & 3 \cdot 5 & & \\ 5 = & 5 \cdot 1 & & \end{array}$$

assim

$$a = 360 = 2^3 \cdot 3^2 \cdot 5^1 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 19^0,$$
$$b = 152 = 2^3 \cdot 19^1 = 2^3 \cdot 3^0 \cdot 5^0 \cdot 19^1.$$

Portanto

$$\text{mdc}(360, 152) = 2^3 \cdot 3^0 \cdot 5^0 \cdot 19^0,$$
$$\text{mmc}(360, 152) = 2^3 \cdot 3^2 \cdot 5^1 \cdot 19^1.$$

10.2 *Como decidir se um inteiro dado é primo?*

As questões tratadas nas seções anteriores destacam o papel que os números primos desempenham na Teoria dos Números.

Mas, dado um inteiro positivo em particular, **como decidir se ele é um número primo?** Utilizando ingenuamente a definição, um método possível seria testar se ele ó, ou não, divisível por algum dos inteiros positivos menores que ele próprio (excetuando-se, é claro, 1).

Notamos inicialmente que se $b > 0$ é um divisor próprio de um inteiro positivo a, temos que $a = bc$, em que $c > 1$. Se acontecesse $b > \sqrt{a}$ e $c > \sqrt{a}$, teríamos que $a = bc > \sqrt{a}\sqrt{a} = a$, uma contradição. Demonstramos, assim, que todo número composto a tem um divisor primo menor ou igual a $\sqrt{a}$, Ainda, se b é um divisor de a, e p é um divisor primo de b, temos que $p' a$, logo, todo número composto a tem um divisor primo menor ou igual a $\sqrt{a}$.

Assim isso dá uma receita para decidir se ou não um inteiro dado é primo:

Receita Dividir a pelos primos menores iguais a $\sqrt{a}$. Se nenhum divide a, logo a é primo.

Consideremos, por exemplo, o inteiro $a = 223$. Então, temos que $14 < \sqrt{a} < 15$. Assim, devemos testar se a é, ou não, divisível pelos primos $2, 3, 5, 7, 11, 13$. Uma verificação direta mostra que 223 é primo.

Exemplo 10.3

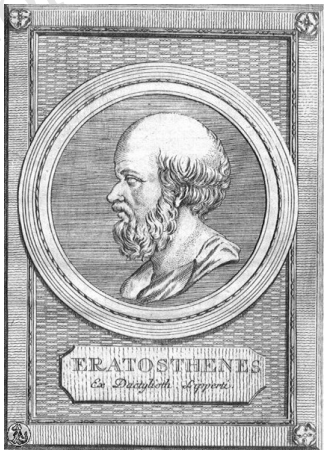
Suponha que $a = 509$. Neste caso $22 < \sqrt{509} < 23$, assim bastará testar os primos $p < 23$, ou seja

$$p = 2, 3, 5, 7, 11, 13, 17, 21.$$

Uma verificação direta mostra que 509 é primo.

10.3 *Crivo de Eratóstenes*

Usando essas idéias, Eratóstenes $(276 - 194\text{a.C.})$, que foi diretor da famosa biblioteca de Alexandria, elaborou um método para determinar todos os primos menores que um certo número dado $n > 0$. Este método é conhecido como o **Crivo de Eratóstenes:**

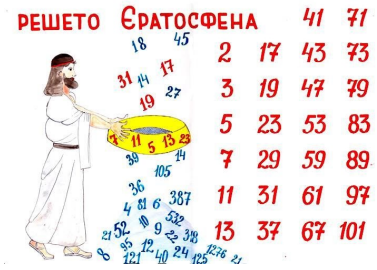


Eratóstenes

- Primeiro se escrevem todos os inteiros positivos menores ou iguais a N.
- Depois, suprimimos todos os múltiplos de 2, diferentes do próprio 2 (para isso, basta ir riscando os números escritos, de dois em dois); depois, os múltiplos de 3 diferentes de 3 e assim sucessivamente.

O Crivo de Eratóstenes para os números menores que 100 é o seguinte:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



Anotações MA11-20 (Draft). Prof. Kostiantyn

10.4 Formulas para receber os primos

Durante últimos seculos muitos matemáticos famosos tentaram encontrar os formulas para gerar os primos. A gente vai discutir nessa seção alguns tentarivas famosas.

10.4.1 Formulas polinomiais

Euler em 1772 considerou o seguinte polinomio

$$f(n) = n^2 + n + 41.$$

Ele descobriu que para $0 \leq n \leq 39$ os valores de $f(n)$ são primos. Por exemplo

$$\begin{aligned} f(0) &= 41, \\ f(1) &= 1^2 + 1 + 41 = 43, \\ f(2) &= 2^2 + 2 + 41 = 47, \\ f(3) &= 3^2 + 3 + 41 = 53, \\ &\vdots \end{aligned}$$

E descobriu que já $f(40) = 40^2 + 40 + 41 = 1681$ é um composto. Foi outras tentativas de encontrar uma formula polinomial, mas o Goldbach mostrou o seguinte Teorema.

Theorem 10.3: (Goldbach)

Não há polinômios (com coeficientes inteiros) não-constantes cujos valores são primos para todo n.

10.4.2 Formulas exponenciais

Numeros de Fermat. O Fermat considerou o seguinte sequencia dos numeros

$$F_n = 2^{2^n} + 1.$$

Acontece o seguinte

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3, \\ F_1 &= 2^{2^1} + 1 = 5, \\ F_2 &= 2^{2^2} + 1 = 17, \\ F_3 &= 2^{2^3} + 1 = 257, \\ F_4 &= 2^{2^4} + 1 = 65537. \end{aligned}$$

são todos primos. Assim o Fermat conjecturou que F_n são primos para todos $n \geq 0$. Mas Euler mostrou que

$$F_5 = 2^{2^5} + 1 = 641 \cdot 6700417$$

é um composto. Não há outros primos de Fermat conhecidos F_n com $n > 4$, mas pouco se sabe sobre os números de Fermat para n grande. Na verdade, cada um dos seguintes questões é um problema em aberto:

Anotações MATo... (draft). Prof. Kostiantyn

- O F_n é composto para todos os $n > 4$?
- Existem infinitos primos de Fermat?
- Existem infinitos números de Fermat compostos?

Até 2021, sabe-se que F_n é composto para $5 \leq n \leq 32$, embora destes, as fatorações completas de F_n sejam conhecidas apenas para $0 \leq n \leq 11$, e não há fatores primos conhecidos para $n = 20$ e $n = 24$. O maior número de Fermat conhecido como composto é $F_{18233954}$, e seu fator principal $7 \cdot 2^{18233956} + 1$, um megaprimo, foi descoberto em outubro de 2020.

Números de Mersenne.

Número de Mersenne é todo número natural da forma $M_n = 2^n - 1$ onde n é um número natural. Há Mersennes não-primos e primos. Nos Mersennes primos há maior interesse. È fácil ver que se M_n é primo, assim n deve ser um primo também.

Os números de Mersenne ficaram famosos em conexão com o algoritmo eficaz para verificar a primalidade dos números de Mersenne. Portanto, os primos de Mersenne há muito mantiveram a liderança como os maiores números primos conhecidos.

O maior número primo conhecido (até Maio de 2021) é

$$2^{82.589.933} - 1,$$

um número que tem 24.862.048 dígitos. Foi encontrado por meio de um voluntario Patrick Laroche em Great Internet Mersenne Prime Search em Dezembro de 2018.

Supondo que uma pagina num livro tem na media 3000 letras, e livro é de 500 paginas vai precisar

$$24.862.048/(3000 \cdot 500 \cdot 2) \approx 8.3$$

livros de 500 paginas (de ambos os lados) para escrever tal numero.

Martin Mersenne (1588–1648)

Exercício 10.1: (Trabalho p/ casa)

Verifique se os seguintes números são primos ou compostos:

$$51, 211, 137, 263, 511.$$

Exercício 10.2: (Trabalho p/ casa)

Escreve o crivo de Eratostenes para $n = 200$.

Exercício 10.3: (Trabalho p/ casa)

Mostre que se o numero de Mersenne M_n é primo, assim n é primo também.

Anotações MAT0120 (Draft). Pr...