Aula [27.03.2020].

Lembrete:

(a) O numero positivo $p \in \mathbb{Z}$ chama-se primo, se p tem exatamente 2 divisores positivos: 1 e p.

(b) Teorema Fundamental de Aritmetica (TFA)

Qualquer $n > 1$ pode ser escrito na forma canônica como

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}, \text{ onde}$$

$p_1 < p_2 < \ldots < p_s$ — são primos

$k_1, k_2, \ldots, k_s$ — inteiros positivos.

MDC, MMC e numeros primos

Vamos descobrir como calcular mdc, mmc atraves a fatoração em primos.

Teorema Sejam: $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$, $p_1, \ldots, p_s$ - primos distintos e $\alpha_i, \beta_j \geq 0$. Então:

$$\text{mdc}(a,b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_s^{\gamma_s}$$
$$\text{mmc}(a,b) = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \ldots \cdot p_s^{\delta_s}, \text{ com}$$

$\gamma_i = \min\{\alpha_i, \beta_i\}$

$\delta_i = \max\{\alpha_i, \beta_i\}$

$1 \leq i \leq s$.

Prova. Seja $d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_s^{\gamma_s}$. Vamos mostrar que $mdc(a,b) = d$.

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} = p_1^{\gamma_1} \cdot p_1^{\alpha_1 - \gamma_1} \cdot \ldots \cdot p_s^{\gamma_s} \cdot p_s^{\alpha_s - \gamma_s}$$

$$= \underbrace{p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}}_{d} \cdot p_1^{\alpha_1 - \gamma_1} \cdot \ldots \cdot p_s^{\alpha_s - \gamma_s}$$

$\Rightarrow d \mid a$. De modo analogo $d \mid b$.

Agora seja $c \mid a$ e $c \mid b$, vamos mostrar que $c \mid d$. Como $c \mid a$, assim $a = c \cdot x$, para algum $x \in \mathbb{Z}$. $c = q_1 \cdot q_2 \cdot \ldots \cdot q_t$, com q_i - primos

Assim $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} = q_1 \cdot q_2 \cdot \ldots \cdot q_s \cdot x$

Por tanto $q_i \mid p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} \Rightarrow q_i = p_j$ para algum j

Assim $c = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdot \ldots \cdot p_s^{\lambda_s}$ e como $c \mid a$ assim $\lambda_i \leq \alpha_i$. Alem disso $c \mid b$, assim $\lambda_i \leq \beta_i$.

Assim $\lambda_i \leq \min\{\alpha_i, \beta_i\} = \gamma_i$. Portanto $c \mid p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}$, ou seja $d = mdc(a,b)$.

Por outro lado $mmc(a,b) = \dfrac{a \cdot b}{mdc(a,b)}$

$$\Rightarrow mmc(a,b) = \frac{p_1^{\alpha_1+\beta_1} \cdot p_2^{\alpha_2+\beta_2} \cdot \ldots \cdot p_s^{\alpha_2+\beta_2}}{p_1^{\min\{\alpha_1,\beta_1\}} \cdot \ldots \cdot p_s^{\min\{\alpha_s,\beta_s\}}} = p_1^{\max\{\alpha_1,\beta_1\}} \cdot \ldots \cdot p_s^{\max\{\alpha_s,\beta_s\}}$$

pois $\alpha_i + \beta_i = \min\{\alpha_i, \beta_i\} + \max\{\alpha_i, \beta_i\}$ ∎.

Exemplo Encontre $mdc(30,36)$ e $mmc(30,36)$.

Solução $a = 30 = 2^1 \cdot 3^1 \cdot 5^1$

$b = 36 = 2^2 \cdot 3^2 \cdot 5^0$

$\Rightarrow mdc(a,b) = 2^1 \cdot 3^1 \cdot 5^0 = 6$

$mmc(a,b) = 2^2 \cdot 3^2 \cdot 5 = 180$ //

Exemplo 2 Encontre $mdc(360, 152)$, $mmc(360, 152)$.

Solução:

$360 = 2 \cdot 180$
$180 = 2 \cdot 90$
$90 = 2 \cdot 45$
$45 = 3 \cdot 15$
$15 = 3 \cdot 5$
$5 = 5 \cdot 1$

$\Rightarrow 360 = 2^3 \cdot 3^2 \cdot 5$

$152 = 2 \cdot 76$
$76 = 2 \cdot 38$
$38 = 2 \cdot 19$
$19 = 19 \cdot 1$

$\Rightarrow 152 = 2^3 \cdot 19$

$360 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 19^0$

$152 = 2^3 \cdot 3^0 \cdot 5^0 \cdot 19^1$

$\Rightarrow mdc(360,152) = 2^3 \cdot 3^0 \cdot 5^0 \cdot 19^0 = 8$

$mmc(360,152) = 2^3 \cdot 3^2 \cdot 5 \cdot 19$

Obs: Considere $P_k = \underbrace{p_1 \cdot p_2 \cdots p_k}_{\text{primeiros primos}} + 1$, isto é

$P_1 = 2 + 1 = 3$
$P_2 = 2 \cdot 3 + 1 = 6 + 1 = 7$
$P_3 = 2 \cdot 3 \cdot 5 + 1 = 31$
$P_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$
$P_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$

} todos os primos.

Mas $P_6 = 2\cdot3\cdot5\cdot7\cdot11\cdot13 + 1 = 59509$ composto

$P_7 = 19\,97\,777$, $P_8 = 247\,27953$ - compostos tmb.

Questão [ainda sem resposta]

Existe numero infinito dos $k>0$, t.q.

$P_k = p_1 \cdots p_k + 1$ — são primos?

Como decidir se ou não um inteiro dado $a>0$ é primo?

Se $a>1$, é composto $\Rightarrow a = b\cdot c$ com $1<b<a$ e $1<c<a$. Supondo que $b\leq c$ temos $b^2 \leq b\cdot c = a$ e $b \leq \sqrt{a}$.

Como $b>1$ assim b é multiplo de primo p.

Assim $p \leq b \leq \sqrt{a}$ e como

$p \mid b$, $b \mid a \Rightarrow p \mid a$.

Resumindo, se a é composto assim existir primo $p \leq \sqrt{a}$ que divide a.

Receita: [Para testar se algum inteiro $a>1$ é primo].

Dividir a pelos todos primos que $\leq \sqrt{a}$.

Se nenhum primo divide $a \Rightarrow a$ é primo.

Exemplo: Seja $a = 509$. Temos $22 < \sqrt{509} < 23$, assim é suficiente testar os primos ≤ 23:

$$2, 3, 5, 7, 11, 13, 17, 19.$$

Como nenhum deles divide a, assim

$$a = 509 \text{ é primo} //$$

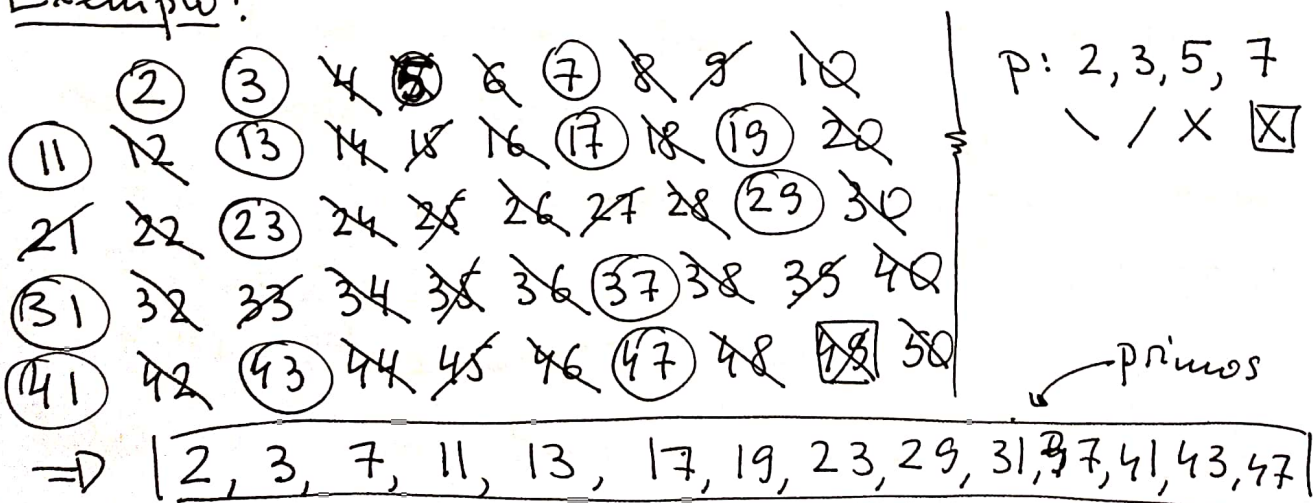
Crivo de Eratóstenes

Eratóstenes (Grego, 276–194, BC) criou um método para obter todos os primos entre 1 e dado inteiro n.

Método [Crivo de Eratóstenes]

- Escrever todos inteiros entre 2 e n
- Eliminar todos compostos da forma $2p, 3p, 4p, \ldots,$ para primos $p \leq \sqrt{n}$.
- Os inteiros que "sobreviveram" são primos.

Exemplo:



Formulas p/ obtenção de primos

① Formulas polinomiais

Euler (1772) mostrou que os valores da função $f(n) = n^2 + n + 41$ são primos para todo $0 \leq n \leq 39$

$f(0) = 41$, $f(1) = 43$, $f(2) = 47$, ...

Proposição [Goldbach]. Não existe um polinomio $f(n)$ não constante, com coeficientes inteiros, cujos valores $f(n)$ são primos para todo $n \geq 1$ inteiro.

② Formulas Exponenciais

a) $F(n) = 2^{2^n} + 1$ (numeros de Fermat).

Fermat conjecturou que $F(n)$ sempre primo para todos $n \geq 0$:

$F(0) = 2^{2^0} + 1 = 3$ – primo, $F(1) = 2^{2^1} + 1 = 5$ – primo

$F(2) = 2^{2^2} + 1 = 17$ – primo, $F(3) = 2^{2^3} + 1 = 257$ – primo

$F(4) = 2^{2^4} + 1 = 65537$ – primo.

Euler provou que $F(5) = 2^{2^5} + 1 = 641 \times 6700417$ – composto //

Ainda os seguintes problemas são abertas:

a) Todos F_n são compostos, com $n > 4$?

b) Existem número infinito dos F_n primos?

c) — // — // — // — // — compostos?

Até hoje é conhecido que $F(n)$ é composto para $5 \leq n \leq 32$.

b) $M(n) = 2^n - 1$ (números de Mersen).

Mersen encontrou todos os primos da forma 2^{p-1} com p primo ≤ 257.

$M(n)$ é primo $\Leftrightarrow$ $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$.

Por exemplo, $M(2) = 3$, $M(3) = 7$, $M(5) = 31$, ...

$M(11) = 23 \times 89$ - composto.

Até hoje esse método ésta usado para encontrar os primos grandes. Por exempo o maior primo conhecido (encontrado 7.12.2018 é $2^{82\,589\,933} - 1$ é primo com 24.862.048 digitos.