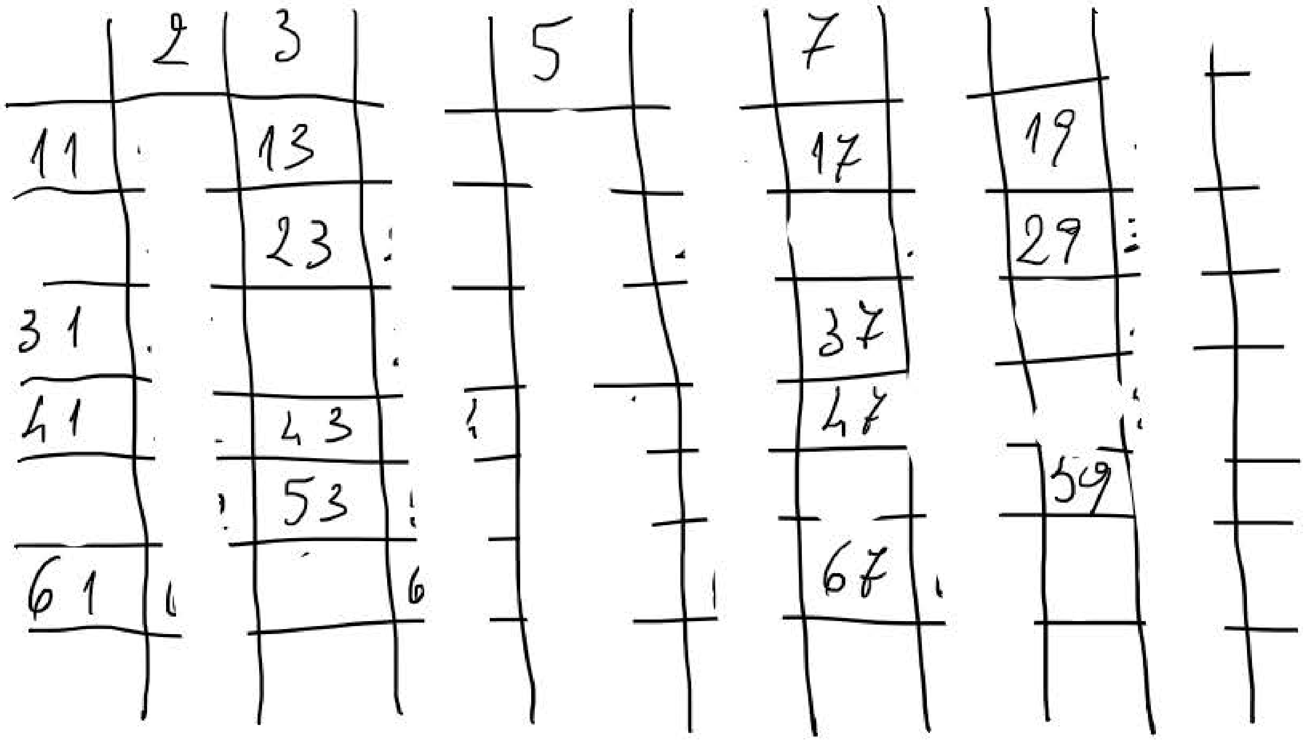
Crivo de Eratóstenes



$a \in \mathbb{N}$

Se $a = bc$ e $b > \sqrt{a}$, então $c < \sqrt{a}$

$8 < \sqrt{70} < 9$

O crivo de Eratóstenes encontra os primos (até um n fixado).

Consideremos os números de 2 a n.

Passo 1: Apaguemos da tabela todos os múltiplos de 2 (maiores que o próprio 2)

Passo k: Apaguemos todos os múltiplos do k-ésimo número ainda presente na lista (maiores do próprio número).

O processo termina com o h-ésimo passo se o h+1-ésimo número ainda presente é $> \sqrt{n}$.

Corpo das frações de um domínio de integridade

$(A, \underbrace{+, \cdot}_{\text{bin.}}, \underbrace{-}_{\text{unária}}, \underbrace{0, 1}_{\text{constante}})$ anel é dito íntegro se

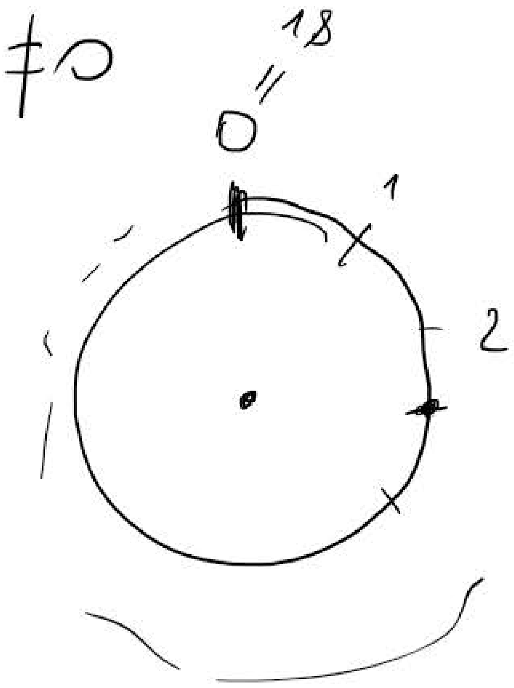
$$\forall a, b \in A \ (ab = 0 \Rightarrow a = 0 \text{ ou } b = 0)$$

$\boxed{\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}}$

não é íntegro

$\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$ mas $\bar{2} \neq 0$

$\mathbb{Z}/_{\text{mod } 4}$ $\quad$ $\mathbb{Z}/_{4\mathbb{Z}}$



$\mathbb{Z}_{18} = \{\bar{0}, \bar{1}, \ldots, \overline{17}\}$

$\bar{6} \cdot \bar{3} = \overline{18} = \bar{0}$

divisores do zero

Um anel íntegro e comutativo é dito domínio de integridade

Consideremos $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ e seja R a relação binária em $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definida por

$(a,b) \, R \, (c,d)$ sse $ad = bc$.

$\forall (a,b) \in X$, $ab = ba \Rightarrow (a,b) \, R \, (a,b) \Rightarrow R$ reflexiva

$\forall (a,b), (c,d) \in X$, se $(a,b) \, R \, (c,d)$, então $ad = bc$. Isso implica que $cb = da$ e, então, $(c,d) \, R \, (a,b)$. Logo, R é simétrica

Sejam $(a,b), (c,d), (e,f) \in X$ t.q. $(a,b) \, R \, (c,d)$ e $(c,d) \, R \, (e,f)$. Então $ad = bc$ e $cf = de$. Mult. membro a membro, segue $adcf = bcde$.

1º caso: $cd \neq 0 \Rightarrow$ cancelo $cd \Rightarrow af = be \Rightarrow (a,b) \, R \, (e,f)$

2º caso: $cd = 0 \Rightarrow$ como $d \neq 0$, $c = 0 \Rightarrow bc = 0 = cf \Rightarrow$

$\Rightarrow ad = 0 = de$, porém $d \neq 0 \Rightarrow a = e = c = 0 \Rightarrow$

$\Rightarrow af = 0 \cdot f = 0$ e $be = b \cdot 0 = 0 \Rightarrow af = be \Rightarrow (a,b) \, R \, (e,f)$

Logo R é transitiva $\Rightarrow R$ é equivalência.

Seja $\mathbb{Q} = \dfrac{\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})}{R}$

Em $\mathbb{Q}$, definimos:

$$\frac{(a,b)}{R} + \frac{(c,d)}{R} = \frac{(ad+bc, bd)}{R}, \quad \frac{(a,b)}{R} \cdot \frac{(c,d)}{R} = \frac{(ac, bd)}{R}$$

$$-\frac{(a,b)}{R} = \frac{(-a,b)}{R}, \quad \boxed{\left(\frac{(a,b)}{R}\right)^{-1} = \frac{(b,a)}{R}}, \quad 0 = \frac{(0,1)}{R}$$

(se $a \neq 0$)

$$1 = \frac{(1,1)}{R}$$

$$\frac{(a,b)}{R} = \frac{(a',b')}{R} \iff ab' = ba'$$

$$\frac{(a,b)}{R} + \frac{(c,d)}{R} = \frac{(ad+bc, bd)}{R}$$

$$\frac{(a',b')}{R} + \frac{(c,d)}{R} = \frac{(a'd+b'c, b'd)}{R}$$

$$(ad+bc) \cdot b'd = ab'd^2 + bb'cd = a'bd^2 + bb'cd = bd(a'd+b'c)$$

$\Rightarrow (ad+bc, bd) \, R \, (a'd+b'c, b'd)$. $+$ é bem definida.

$$\frac{(a,b)}{R} = \frac{(a',b')}{R} \iff ab' = ba'$$

$$\frac{(a,b)}{R} \cdot \frac{(c,d)}{R} = \frac{(ac,bd)}{R} \quad e \quad \frac{(a',b')}{R} \cdot \frac{(c,d)}{R} = \frac{(a'c,b'd)}{R}$$

$$acb'd = ab'cd = ba'cd = bda'c \Rightarrow (ac,bd)R(a'c,b'd)$$

$\therefore$ é bem definido

$$\frac{(a,b)}{R} + \frac{(-a,b)}{R} = \frac{(ab-ba,b^2)}{R} = \frac{(0,b^2)}{R}$$

$(0,b^2)R(0,1)$, pois $0 \cdot 1 = b^2 \cdot 0$ então $\dfrac{(-a,b)}{R} = -\dfrac{(a,b)}{R}$

$$\frac{(a,b)}{R} \cdot \frac{(b,a)}{R} = \frac{(ab,ba)}{R}$$

$(ab,ba)R(1,1)$ pois $ab \cdot 1 = ba \cdot 1$, então $\dfrac{(b,a)}{R} = \dfrac{(a,b)}{R}^{-1}$

A partir de agora, iremos denotar por $\dfrac{a}{b}$ a classe de equivalência $\dfrac{(a,b)}{R}$.

Teorema A função $i: m \in \mathbb{Z} \mapsto \frac{m}{1} \in \mathbb{Q}$ é uma imersão de anel.

Dem.

Se $m, n \in \mathbb{Z}$ são tais que $i(m) = i(n)$, então $\frac{m}{1} = \frac{n}{1}$, isto é $\overline{(m,1)}_R = \overline{(n,1)}_R \iff m \cdot 1 = 1 \cdot n \iff m = n$.

i é injetora.

$\forall m, n \in \mathbb{Z}$, $i(m+n) = \frac{m+n}{1}$, $i(m) + i(n) = \frac{m}{1} + \frac{n}{1} = \frac{m \cdot 1 + 1 \cdot n}{1 \cdot 1} =$

$= \frac{m+n}{1}$. Logo $i(m+n) = i(m) + i(n)$.

$\forall n \in \mathbb{Z}$, $i(-n) = \frac{-n}{1} = -\frac{n}{1} = -i(n)$.

$\forall m, n \in \mathbb{Z}$, $i(mn) = \frac{mn}{1} = \frac{m}{1} \cdot \frac{n}{1} = i(m) \cdot i(n)$.

Em $\mathbb{Q}$, $\frac{a}{b} \leq \frac{c}{d}$ sse $ad \leq bc$

$\frac{a}{b} \leq \frac{c}{d} \Rightarrow \forall \frac{e}{f} \in \mathbb{Q}$, $\frac{a}{b} + \frac{e}{f} \leq \frac{c}{d} + \frac{e}{f}$

$\frac{a}{b} \leq \frac{c}{d}$ e $\frac{e}{f} \geq 0 \Rightarrow \frac{a}{b} \cdot \frac{e}{f} \leq \frac{c}{d} \cdot \frac{e}{f}$

Em $\mathbb{N}$ e $\mathbb{Z}$, não existe c t.q. $n < c < n+1$ $\forall n$.

Em $\mathbb{Q}$ é diferente: $\forall \underbrace{\frac{a}{b} < \frac{c}{d}}_{ad < bc} \in \mathbb{Q}$ $\exists \frac{e}{f} \in \mathbb{Q} \left(\frac{a}{b} < \frac{e}{f} < \frac{c}{d} \right)$

Por exemplo $\frac{e}{f} = \frac{ad+bc}{2bd}$.

$\boxed{\frac{ad+bc}{2bd} > \frac{a}{b}}$ $\quad 2abd = abd + abd < abd + b^2c \Rightarrow$

$\Rightarrow \frac{a}{b} < \frac{ad+bc}{2bd}$

$\boxed{(\mathbb{Q}, <) \text{ é denso em si.}}$