$\text{mdc}(153, 23) = \{\pm 1\}$

153	23	15	8	7	1
	6	1	1	1	

$$1 = 8 - 7 = 23 - 15 - (15 - 8) = 23 - 2 \cdot 15 + 8 =$$

$$= 23 - 2(153 - 6 \cdot 23) + 23 - 15 = -2 \cdot 153 + 14 \cdot 23 - (153 - 6 \cdot 23)$$

$$= -3 \cdot 153 + 20 \cdot 23 \qquad u = -3 \qquad v = 20$$

Se $\text{mdc}(a, b) = \pm 1$, a e b são ditos primos entre si ou coprimos.

Proposição Sejam $a, b \in \mathbb{Z} \setminus \{0\}$ e $d \in mdc(a,b)$. Valem as seguintes.

(1) $\exists a_1, b_1 \in \mathbb{Z} \left(a = a_1 d \text{ e } b = b_1 d \text{ e } mdc(a_1, b_1) = \{\pm 1\}\right)$;

(2) se $d = 1$ e $a \mid bc$, com $c \in \mathbb{Z}$, então $a \mid c$;

(3) $\exists m \left(ab = dm \text{ e } m \in mmc(a,b)\right)$;

(4) se $d = 1$, $ab \in mmc(a,b)$;

(5) se $m \in mmc(a,b)$, $mmc(a,b) = \{\pm m\}$.

---

(1) se $e \mid a_1$ e $e \mid b_1$, então $ed \mid a$ e $ed \mid b$. Como d é um $mdc(a,b)$, $ed \mid d \Rightarrow e \mid 1 \Rightarrow e = \pm 1$.

(2) $d = 1 \Rightarrow \exists u, v \in \mathbb{Z} \ (au + bv = 1)$.

$a \mid bc \Rightarrow \exists e \in \mathbb{Z} \ (ae = bc)$

Multiplicando por c e igualdado $au + bv = 1$, temos $auc + bvc = c$, como $bc = ae$, segue

$$auc + aec = c \Rightarrow a\underbrace{(uc + ec)}_{f} = c$$

Então $\exists f \in \mathbb{Z} \ (af = c)$, ou seja, $a \mid c$.

Indução "forte"

Seja P uma propriedade que depende de uma variável $n\in\mathbb{N}$. Se vale $P(0)$ e, para todo $n\in\mathbb{N}$,

$$\forall k\,((k<n \text{ e } P(k)) \to P(n)),$$

então P vale $\forall n\in\mathbb{N}$.

(PA3) é equivalente à indução forte

Def. Um número inteiro p é dito **primo** se $|p| > 1$ e $\forall a, b \in \mathbb{Z}$, se $p \mid ab$ então $p \mid a$ ou $p \mid b$.

Lema Seja p primo. $\forall n \geq 1$ $\forall a_1, \dots, a_n \in \mathbb{Z}$, se $p \mid a_1 \cdots a_n$ então $\exists i \leq n$ t.q. $p \mid a_i$.

Dem.

Óbvio para $n = 1$. É a própria def. de primo para $n = 2$.

Seja $n > 2$ e suponha-se que a asserção valha para $n-1$. Sejam $a_1, \dots, a_n$ t.q. $p \mid a_1 \cdots a_n$.

Então $p \mid \underbrace{(a_1 \cdots a_{n-1})}_{b} a_n$. Como p é primo, $p \mid a_1 \cdots a_{n-1}$ ou $p \mid a_n$. Se $p \mid a_n$, terminamos.

Se $p \mid a_1 \cdots a_{n-1}$, pela hp. de indução, $\exists i \leq n-1$ t.q. $p \mid a_i$. Então vale o lema $\forall n \in \mathbb{N}$.

Teorema Seja $p \in \mathbb{Z}$ t.q. $|p| > 1$.

Então p é primo sse todos seus divisores são $1, -1, p$ e $-p$.

Dem.

$\boxed{\Rightarrow}$ p primo e seja a um divisor de p. Então $\exists b \in \mathbb{Z}$ t.q. $ab = p \Rightarrow p \mid ab$. Como p é primo, $p \mid a$ ou $p \mid b$. Se $p \mid a$, então $a = \pm p$. Se $p \mid b$, então como $b \mid p$, segue $b = \pm p$ e, consequentemente, $a = \pm 1$.

$\boxed{\Leftarrow}$ $\forall d \in \mathbb{Z}$, se $d \mid p$ então $d \in \{1, -1, p, -p\}$.

Se $p \mid ab$ e $p \nmid a$, $mdc(a, p) = \{\pm 1\}$ pois, por hipótese, p tem apenas ± 1 e $\pm p$ como divisores. Já que $p \nmid a$, $p \notin mdc(a, p) \Rightarrow mdc(a, b) = \{\pm 1\}$. Pela prop. (2) já demonstrada, segue $p \mid b$. Logo, p é primo.

Def. Uma permutação de um conjunto X é uma função bijetora de X em si.

Teorema Fundamental da Aritmética

Seja $n \in \mathbb{Z}$, $|n| > 1$. Então n é primo ou é produto de potências de primos dois a dois distintos: $n = p_1^{k_1} \cdots p_t^{k_t}$, os p_i primos e $k_1, \ldots, k_t \in \mathbb{N} \setminus \{0\}$.

Além disso, se $n = p_1^{k_1} \cdots p_t^{k_t} = q_1^{h_1} \cdots q_s^{h_s}$, com os p_i e os q_j primos e $k_1, \ldots, k_t, h_1, \ldots, h_s \in \mathbb{N} \setminus \{0\}$ ($p_{i_1} \neq p_{i_2}$ se $i_1 \neq i_2$ e $q_{j_1} \neq q_{j_2}$ se $j_1 \neq j_2$), então:

(1) $s = t$, e

(2) $\exists\, \sigma$ permutação do conjunto $\{1, \ldots, t\}$ t.q. $\forall i = 1, \ldots, t$, $p_i = \pm q_{\sigma(i)}$ e $k_i = h_{\sigma(i)}$.

<u>Teorema de Euclides</u> O conjunto dos números primos é infinito.

<u>Dem.</u>

Seja $P = \{p \in \mathbb{N} : p \text{ é primo}\}$. $P \neq \emptyset$ e, por absurdo, vamos supor que seja finito. Então $\exists t \in \mathbb{N}$ t.q. $P = \{p_1, \dots, p_t\}$. Consideremos o número $a = p_1 \cdots p_t + 1$. Como $a > 1$, pelo T.F.A., $\exists p \in P$ t.q. $p | a$, então $\exists i \leq t$ t.q. $p_i | a = p_1 \cdots p_t + 1$.

Como $p_i | p_1 \cdots p_t$, $p_i | a - p_1 \cdots p_t = 1$ e isso é absurdo pois os únicos divisores de 1 são ± 1.

Logo P é infinito.