Relatively Prime

Definition

$\forall\, a, b \in \mathbb{Z}$, to say that a and b are *relatively prime* means $(a, b) = 1$.

Corollary: To Bézout

$$\forall\, a, b \in \mathbb{Z}, (a, b) = 1 \iff \exists\, m, n \in \mathbb{Z}, ma + nb = 1$$

Proof

Assume $a, b \in \mathbb{Z}$
$(a, b) = 1 \iff 1 = \min\{ma + nb \in \mathbb{Z}^+ \mid m, n \in \mathbb{Z}\} \iff \exists\, m, n \in \mathbb{Z}, ma + nb = 1$

Theorem

Let $a, b, c \in \mathbb{Z}$ and $a \neq 0$:

$$a \mid bc \text{ and } (a, b) = 1 \implies a \mid c$$

Proof

Assume $a \mid bc$ and $(a, b) = 1$
$\exists\, m, n \in \mathbb{Z}, ma + nb = 1$
$(cm)a + n(bc) = c$
But $a \mid a$ and $a \mid bc$
So $a \mid (cm)a + n(bc)$
$\therefore a \mid c$

Theorem

Let p be a prime number:

$$\forall\, a \in \mathbb{Z}, (p, a) = 1 \iff p \nmid a$$

Proof

Assume $a \in \mathbb{Z}$

$\implies$ Assume $p \mid a$

$p \mid p$
$p \in D_p \cap D_a$
$p > 1$
$\therefore (p, a) \geq p > 1$

$\impliedby$ Assume $p \nmid a$

$D_p = \{\pm 1, \pm p\}$
$D_p \cap D_a = \{\pm 1\}$
$\therefore (p, a) = 1$

Corollary

Let p be a prime number:

$$\forall\, a, b \in \mathbb{Z}, p \mid ab \implies p \mid a \text{ or } p \mid b$$

Proof

Assume $a, b \in \mathbb{Z}$
Assume $p \mid ab$

Case 1: $p \mid a$

Done.

Case 2: $p \nmid a$

(p,a)=1
$\therefore p \mid b$

Corollary

Let $a, b \in \mathbb{Z}$ such that $a \neq 0$ or $b \neq 0$ and $d = (a, b)$:

$$(\frac{a}{d}, \frac{b}{d}) = 1$$

Proof

$$(\frac{a}{d}, \frac{b}{d}) = \frac{d}{d} = 1$$

Corollary

Let $\frac{a}{b} \in \mathbb{Q}$:

$$\exists\, \frac{p}{q} \in \mathbb{Q}, \frac{a}{b} = \frac{p}{q} \text{ and } (p, q) = 1$$

Proof

Let $d = (a, b)$
Let $p = \frac{a}{d}$ and $q = \frac{b}{d}$
$(p, q) = 1$
$\frac{p}{q} = \frac{\frac{a}{d}}{\frac{b}{d}} = \frac{a}{b}$