Definition. Let $a,b \in \mathbb{Z}^+$. Let $\gcd(a,b)$ be the greatest common divisor of a and b.

This means Let $d = \gcd(a,b)$. Then

① $d \mid a \wedge d \mid b$.

② $\left.\begin{array}{l} d' \mid a \\ d' \mid b \end{array}\right\} \Rightarrow d' \le d$.

Theorem. Let $a,b \in \mathbb{Z}^+$. Then

$$\gcd(a,b) = \min\left\{ ax+by \;\middle|\; \begin{array}{l} ① \ x,y \in \mathbb{Z} \\ ② \ ax+by > 0 \end{array} \right\}.$$

Proof. Let $d = \gcd(a,b)$ and $d' = \min\left\{ ax+by \;\middle|\; \begin{array}{l} ① \ x,y \in \mathbb{Z} \\ ② \ ax+by > 0 \end{array} \right\}$.

We will show $d' \ge d$ and $d \ge d'$ and deduce $d = d'$.

Why is $d' \ge d$?

$$\left.\begin{array}{l} d \mid a \Rightarrow a \overset{d}{\equiv} 0 \Rightarrow ax \overset{d}{\equiv} 0 \\ d \mid b \Rightarrow b \overset{d}{\equiv} 0 \Rightarrow by \overset{d}{\equiv} 0 \end{array}\right\} \Rightarrow ax+by \overset{d}{\equiv} 0 \Rightarrow d \mid ax+by.$$

So, if $ax+by > 0$, we have $d \le ax+by$.

$$\Rightarrow d \le d' = \min\left\{ ax+by \;\middle|\; \begin{array}{l} ① \ x,y \in \mathbb{Z} \\ ② \ ax+by > 0 \end{array} \right\}.$$

Why is $d \ge d'$?

We will show d' is a common divisor of a and b.

Let's divide a by d' and suppose q, r are the quotient and remainder, respectively. So

$$\begin{cases} 0 \le r < d' \\ a = d'q + r \end{cases}$$

On the other hand, $d' = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$.

$$\Rightarrow a = (ax_0 + by_0)q + r$$

$$\left.\begin{array}{l} \Rightarrow r = a(1 - x_0 q) + b(-y_0 q) < d' \\ \text{Since } d' = \min\left\{ ax+by \;\middle|\; \begin{array}{l} \text{① } x,y\in\mathbb{Z} \\ \text{② } ax+by>0 \end{array} \right\} \end{array}\right\} \Rightarrow r = 0.$$

$$\left.\begin{array}{l} \text{So } d' \mid a. \\ \text{Similarly one can show } d' \mid b. \end{array}\right\} \Rightarrow d' \le \gcd(a,b) = d.$$

■

<u>Corollary</u>. $\forall a,b \in \mathbb{Z}^+$, $\exists x,y \in \mathbb{Z}$, $\gcd(a,b) = ax+by$.

<u>Corollary</u>. $\forall a,b \in \mathbb{Z}^+$, $\left.\begin{array}{l} d \mid a \\ d \mid b \end{array}\right\} \Rightarrow d \mid \gcd(a,b)$.

<u>Proof</u>.

$$\left.\begin{array}{l} \exists x_0, y_0 \in \mathbb{Z},\ \gcd(a,b) = ax_0 + by_0. \\ \left.\begin{array}{l} d \mid a \Rightarrow a \overset{d}{\equiv} 0 \Rightarrow ax_0 \overset{d}{\equiv} 0 \\ d \mid b \Rightarrow b \overset{d}{\equiv} 0 \Rightarrow by_0 \overset{d}{\equiv} 0 \end{array}\right\} \Rightarrow ax_0 + by_0 \overset{d}{\equiv} 0 \end{array}\right\} \Rightarrow d \mid \gcd(a,b).$$

■

<u>Proposition</u>. $\forall a,b \in \mathbb{Z}^+$, $c \in \mathbb{Z}$, $ax+by=c$ has integer solutions

$$\Updownarrow$$

$$\gcd(a,b) \mid c.$$

<u>Proof</u>. ($\Downarrow$) Let $\gcd(a,b) = d$. Then as we have seen above

$$\forall x,y \in \mathbb{Z}, \quad d \mid ax+by \quad ⊛$$

If $c = ax+by$ for some $x,y \in \mathbb{Z}$, then by ⊛ $d \mid c$.

($\Uparrow$) Let $\gcd(a,b) = d$. So $d \mid c \Rightarrow c = dk$ for some $k \in \mathbb{Z}$.

And $\exists x_0, y_0 \in \mathbb{Z}$, $d = ax_0 + by_0$. Hence

$$c = dk = a(x_0 k) + b(y_0 k) \Rightarrow ax+by = c \text{ for some } x,y \in \mathbb{Z}.$$

■

<u>Corollary</u>. Let p be a prime.

$$p \nmid a \Rightarrow \exists x,y \in \mathbb{Z},\ ax+py = 1.$$

<u>Proof</u>. $\gcd(a,p) \mid p \Rightarrow \gcd(a,p) = 1$ or p $\Rightarrow \gcd(a,p) = 1$.

$\Big\} \Rightarrow \gcd(a,p)=1.$

Since $p \nmid a$

$$\Rightarrow \exists x,y \in \mathbb{Z},\ ax+py=1. \qquad \blacksquare$$

<u>Corollary</u>. Let p be a prime.

$$a \overset{p}{\not\equiv} 0 \Rightarrow \exists a' \in \mathbb{Z},\ aa' \overset{p}{\equiv} 1.$$

<u>Proof</u>. $\left.\begin{array}{l} a \overset{p}{\not\equiv} 0 \Rightarrow p \nmid a \\ p: \text{prime} \end{array}\right\} \Rightarrow \exists x,y \in \mathbb{Z},\ ax+py=1$

$$\Rightarrow ax \overset{p}{\equiv} 1. \qquad \blacksquare$$

<u>Warning</u>. In the above corollary it is extremely important that p is prime. For instance $\nexists a' \in \mathbb{Z},\ 2a' \overset{4}{\equiv} 1$.

In fact, using the above proposition one has:

$$\exists x \in \mathbb{Z},\ ax \overset{b}{\equiv} c \iff \gcd(a,b) \mid c.$$

<u>Proposition</u>. Let p be prime.

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

<u>Proof</u>. If not, $\exists a,b \in \mathbb{Z}$ s.t. $p \nmid a$, $p \nmid b$ and $p \mid ab$

$$\Rightarrow \exists a',b' \in \mathbb{Z},\ \left.\begin{array}{l} aa' \overset{p}{\equiv} 1 \\ bb' \overset{p}{\equiv} 1 \end{array}\right\} \Rightarrow \underbrace{ab}_{0}a'b' \overset{p}{\equiv} 1$$

$$\Rightarrow 0 \overset{p}{\equiv} 1$$

which is a contradiction. $\blacksquare$