Greatest Common Divisor.

① $d|a$ ② $d|b$. ③ $\forall c \in \mathbb{Z}$. $c|a$ $\wedge c|b \Rightarrow c \le d$.

1. Definition: d is said to be $\gcd(a,b)$. if $d|a$ and $d|b$ and if any num c is also a common divisor of a and b, then $c \le d$.

2. Relatively Prime: The integers $a.b.$ is said to be R.P. if their only common divisor is 1, i.e., $\gcd(a,b)=1$.

$\forall m.n \in \mathbb{Z}$. $\gcd(m.n) \ge 1$.

e.g. Let $a.b.n \in \mathbb{N}$. Prove $\gcd(a^n.b^n)=1 \Rightarrow \gcd(a.b)=1$.

proof: WTS: $\gcd(a,b)=1$.

Assume for contradiction. $\gcd(a,b) \ne 1$. gives.

$\exists d \in \mathbb{Z}$. s.t. $d|a$, $d|b$. $d>1$. as. $\gcd(a.b) \ge 1$.

Since $d|a$, $d|b$, gives. $d|a^n$, $d|b^n$. $d>1$. give. $\gcd(a^n,b^n) \ge d > 1$.

contradicts. ∎

e.g. Let $a,b,m,n \in \mathbb{N}$. $m,n>1$. Assume. $m.n$. R.P.; Prove if $a \equiv b \pmod m$ and $a \equiv b \pmod n$. then $a \equiv b \pmod{mn}$.

proof: Assume $a \equiv b \pmod m$. and $a \equiv b \pmod n$.

Since. m, n, R.P. gives. $\gcd(m,n)=1$.

Since $a \equiv b \pmod m$, gives. $mk_1 = a-b$.

Since. $a \equiv b \pmod m$. gives. $nk_2 = a-b$.

Thus. $mk_1 = nk_2$, which $n|mk_1$.

if $n|m$, $n|n$. $\gcd(n,m)=n$. $n>1$. contra.

Since $\gcd(m,n)=1$, and $n>1$, gives. $n|k_1$. $\exists l \in \mathbb{Z}$. s.t. $nl=k_1$

$m \cdot n \cdot l = a-b$. $\Rightarrow m \cdot n | a-b \Rightarrow a \equiv b \pmod{mn}$. ∎

1) Thm 7.2.9: If s divides tu and s is R.P. to u, then s divides t.

proof: Assume $s|tu$ and s is R.P. to u. i.e. $\gcd(s,u)=1$.

WTS: $s|t$.

Since $s \mid tu$. $\exists k \in \mathbb{Z}$. s.t. $sk = tu$.

By FTA: $u = p_1^{\alpha_1} \cdots\cdots p_k^{\alpha_k}$, where p_i are prime and $\alpha_i \in \mathbb{N}$.

$\Rightarrow t p_1^{\alpha_1} \cdots\cdots p_k^{\alpha_k} = sk$.

Since $\gcd(s,u) = 1$, $\forall p_i$, $p_i \nmid s$. $i \in \{1, 2, \ldots, k\}$. ($\because p_i \mid u$).

Thus all factors of s occurs in t, which $s \mid t$.

3. GCD with remainder: If $a = qb + r$, then $\gcd(a,b) = \gcd(b,r)$.

1). Euclid Theorem: Use GCDWR to find $\gcd(a,b)$.

Align with Euclid Theorem.

e.g. find $\gcd(1239, 735)$.

	$a \quad q \quad b \quad r$
$\gcd(1239, 735)$	$1239 = 1 \times 735 + 504$
$= \gcd(735, 504)$	$735 = 1 \times 504 + 231$
$= \gcd(504, 231)$	$504 = 2 \times 231 + 42$
$= \gcd(231, 42)$	$231 = 5 \times 42 + 21$
$= \gcd(42, 21)$	$42 = 2 \times 21$
$= 21$	

e.g. prove $\{\gcd(8n+31, 3n+11) : n \in \mathbb{Z}\} = \{1, 5\}$.

$\gcd(8n+31, 3n+11)$	$8n+31 = 2 \cdot (3n+11) + (2n+9)$
$= \gcd(3n+11, 2n+9)$	$3n+11 = 1 \cdot (2n+9) + (n+2)$
$= \gcd(2n+9, n+2)$	$2n+9 = 2 \cdot (n+2) + 5$
$= \gcd(n+2, 5)$	

Since 5 is prime, its only divisor is 1 or 5. gives

$\gcd(n+2, 5) = 1$ or 5.

e.g. Prove $(5a+2)$ and $(7a+3)$ are R.P. for $a \in \mathbb{N}$.

$\gcd(7a+3, 5a+2)$	$7a+3 = 1 \cdot (5a+2) + (2a+1)$
$= \gcd(5a+2, 2a+1)$	$5a+2 = 2 \cdot (2a+1) + a$
$= \gcd(2a+1, a)$	$2a+1 = 2 \cdot a + 1$
$= \gcd(a, 1)$	
$= 1$	

e.g. Suppose $\exists\, m, n \in \mathbb{Z}$ s.t. $am+bn=1$. Prove a, b are R.P.

WTS: a, b are R.P. i.e. $\gcd(a,b)=1$.

Assume for contradiction $\gcd(a,b) \neq 1$. i.e.

$$\gcd(a,b)=d. \quad d \in \mathbb{N}. \quad d>1.$$

From def^{n}, gives $d \mid a$ and $d \mid b$. which $\exists\, k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 d = a$.
$k_2 d = b$.

Since $am+bn=1$.

$\Rightarrow k_1 dm + k_2 dn = 1$.

$\Rightarrow d(k_1 m + \cancel{t}dn)=1. \quad \Rightarrow d \mid 1.$ which $d=1$. contradicts. ■