§ Number Theory & Modular Arithmetic.

$\mathbb{N} := \{1, 2, 3, \dots\}$, $\mathbb{Z} := \{\dots -3, -2, -1, 0, 1, 2, 3, \dots\}$

(the set of Natural numbers) (the set of integers)

Defn: Let a & $b \in \mathbb{Z}$. (i.e. a & b are integers or "whole numbers")

We say that b divides a, OR b is a divisor (or factor) of a if $a = bq$ for some $q \in \mathbb{Z}$ & we write $b|a$.

Ex: $3|6$, $2|6$, $1|6$, $6|6$

$(q=2)$ $(q=3)$ $(q=6)$ $(q=1)$

(Aside: Note every integer b divides 0 as $0 = 0 \cdot b$)

(zero)

Defn: Let $a, b, d \in \mathbb{Z}$. If $d|a$ & $d|b$ we say that d is a common divisor of a & b, (or a common factor). If it is the case that d is the biggest (or largest) number that divides a & b we say that d is the greatest common divisor of a & b & we write

$d = \gcd(a, b)$ (or in some books $d = (a, b)$)

or greatest

Ex: $a = 18$, $b = 12$, then $d = 3|12$ & $3|18$ (so 3 is a common factor of 12 & 18)

But $6|12$ & $6|18$ $6 = \gcd(18, 12)$

Defn: Let $p \in \mathbb{N}$ & $p > 1$. We say that p is a prime number if its only divisors are 1 & p.

(ie. if $d > 0$ & $d \mid p \Rightarrow d = 1$ or p)

It is a fact that if a & b are integers with $b > 0$ then there is a unique pair of integers q & r, s.t.

$$a = bq + r \quad \text{with} \quad 0 \leq r < b$$

e.g. $a = 17$ $b = 5$ (5 divides 17, three time & remainder = 2)

$17 = 5(3) + 2$;
($3 = q$, $2 = r$)

$a = 50$ $b = 7$

$50 = 7(7) + 1$;
($7 = q$, $1 = r$)

NOTE: If $a = bq + r$ $0 \leq r < b$

Then $\gcd(a, b) = \gcd(b, r)$

Because $r = a - bq$ so if

$d \mid a$ & $b \Rightarrow d \mid r$

Ex: Find gcd(5, 29) using "Euclid's Algorithm"

(*) $29 = 5(5) + 4$

29 → a, 5 → b, 5 → q, 4 → r

$\therefore \gcd(5, 29) = \gcd(5, 4)$ → go again

(**) $5 = 4(1) + 1$

5 → a, 4 → b, 1 → q, 1 → r

$\therefore \gcd(5, 4) = \gcd(4, 1) = 1$

OR go one MORE time

$4 = 1(4)$ no remainder

$\therefore$ the gcd = last non zero remainder

BACK SUBSTITUTION:

(**) $\Rightarrow 1 = 5 - 4$

& (*) $\Rightarrow 1 = 5 - [29 - 5(5)]$

$\Rightarrow 1 = (-1)29 + (6)5$

i.e. Allows us to express gcd(a, b) as $ma + nb$ with $m \& n \in \mathbb{Z}$ (not unique)

ie as an integer linear combination of a & b.

Ex: Use Euclid's Algorithm to find gcd (1492, 1066)

$1492 = 1006\,(1) + 426 \quad \ldots\ldots \quad (A)$

(a $\quad$ b $\quad$ q $\quad$ r)

(So gcd (1492, 1066) = gcd (1066, 426))

↳ go again

$1066 = 426\,(2) + 214 \quad \ldots\ldots \quad (B)$

(So gcd (1066, 426) = gcd (426, 214))

↳ go again

$426 = 214\,(1) + 212 \quad \ldots\ldots \quad (C)$

(So gcd (426, 214) = gcd (214, 212))

↳ go again.

$214 = 212\,(1) + \boxed{2} \quad \ldots\ldots \quad (D)$

(So gcd (214, 212) = gcd (212, 2))

$212 = 2\,(106)$

(no remainder so last remainder = gcd)

$\therefore$ gcd (1492, 1066) = 2 Now Back substitute

(D) $\Rightarrow$ $2 = 214 - 212$

(C) $\Rightarrow$ $2 = 214 - [426 - 214]$

$= -426 + (2)\,214$

(B) $\Rightarrow$ $2 = -426 + 2[1066 - (2)\,426]$

$\Rightarrow$ $2 = (2)\,1066 - (5)\,426$

(A) $\Rightarrow$ $2 = (2)\,1066 - (5)[1492 - 1066]$

$\Rightarrow$ $2 = -(5)\,1492 + (7)\,1066$

ie gcd $= ma + nb$ $\quad m, n \in \mathbb{Z}$.