29/1

Number theory

Division Algorithm

If any int number a is divided by another +ve int b then there exist 2 unique integers q and r, such that $a = bq + r$

where q = quotient, r = remainder.

such that $0 \leq r < b$. if b is a general int except 0. then condition for remainder becomes $0 \leq r < |b|$

Congruend modulo

For two int a, b.

$$a \equiv b \pmod{m}$$

$a - b$ is divisible by m

$$11 \equiv 1 \pmod{2}$$

$$12 \not\equiv -1 \pmod{3}$$

$$12 \equiv 0 \pmod{3}$$

A necessary and sufficient condition basically implies that happening of inference 'a' has impact or happening of

inference 'b' (necessary condition)
On the other hand inference b will happen only if inference a will happen signifies the sufficient condition.

(*) let m be a positive int.
If $a \equiv b \pmod m$ and $c \equiv d \pmod m$
then, $a+c \equiv b+d \pmod m$
$ac \equiv bd \pmod m$

$a-b$ is divisible by m
$\Rightarrow \exists$ another int q_1, s.t $a-b = q_1 m$
$c-d$ is divisible by m
$\Rightarrow \exists$ another int q_2, s.t $c-d = q_2 m$

$$(a-b)+(c-d) = (q_1+q_2)m$$
$$(a+c)-(b+d) = (q_1+q_2)m$$
$$(a+c) \equiv (b+d) \pmod m$$

Similarly