INTEGERS

Well Ordering Property.

Every non-empty subset of $\mathbb{N}$ contains a least element.

$S \subseteq \mathbb{N}$, there is a natural number a in S such that $a \le x \ \forall \ x \in S$.

Principle of Induction.

$S \subseteq \mathbb{N}$ with the properties:

i) 1 belongs to S

ii) whenever a $k \in S$, then $k+1 \in S$, $k \in \mathbb{N}$

The $S = \mathbb{N}$.

Example: i) Use PMI to prove:

$$1 + 2 + \dots + n = \frac{n(n+1)}{2} \quad \forall \ n \in \mathbb{N}.$$

ii) P.T: $\underbrace{3^{2n}}_{f(n)} - 8n - 1$ is divisible by 64 $\forall \ n \in \mathbb{N}$.

Step 1: $f(1) = 9 - 8 - 1 = 0$. $f(1)$ is divisible by 64

Step 2: Let $f(k)$ is divisible by 64 is true.

Step 2: Let $f(K)$ is divisible by 64 is true.

$$f(K+1) = 3^{2(K+1)} - 8(K+1) - 1.$$

$$= 3^{2K+2} - 8K - 8 - 1$$

$$= 3^{2K+2} - 8K - 9.$$

$$f(K) = 3^{2K} - 8K - 1.$$

Inequality using PMI

P.T : $\boxed{n! > 2^n}$ for all natural no's, $n \geq 4$.

$P(1), P(2), P(3) \ldots$

$4! > 2^4$

$\boxed{24 > 16}$

$P(4)$ is true

$P(K+1) : (K+1)! > 2^{K+1}.$

$P(K)$ is true.

$$K! > 2^K$$

$$\Rightarrow (K+1)! > 2^K(K+1). > 2^{K+1}$$

$$= 2^K \cdot 2$$

$$= 2^{K+1}$$

$K+1 > 2$

Division Algorithm.

Given integers a and b with $b > 0$, there exist unique integers q and r such that $a = bq + r$, where $0 \le r < b$.

Thm: $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for arbitrary integers x and y.

Thm: If a and b are integers not both zero, then there exist integers u and v such that

$$\gcd(a, b) = au + bv. \quad \text{(Bezout's Theorem)}$$

For example:

$$\gcd(\overset{a}{-4}, \overset{b}{20}) = 4$$

$$4 = -4 \times (\overset{u}{-1}) + 20 \cdot \overset{v}{0}$$

$$\gcd(\overset{a}{55}, \overset{b}{35}) = 5, \quad 5 = 55 \cdot 2 + 35 \cdot (-3).$$

If k be a positive integer $\gcd(ka, kb) = k \cdot \gcd(a, b)$.

Proof: Let $d = \gcd(a, b)$. Then there exists integers u and v such that $d = au + bv$.

Since $d = \gcd(a, b)$, $d \mid a$ and $d \mid b$.

$\ldots d \mid b \Rightarrow kd \mid kb$.

Since $d = \gcd(a,b)$, $d | a$ and $d | b$.

$d | a \Rightarrow kd | ka$, $d | b \Rightarrow kd | kb$.

So, kd is a common divisor of ka and kb.

Let, c be a common divisor of ka and kb.

$$c | ka \Rightarrow ka = pc.$$

$$\text{and } c | kb \Rightarrow kb = q.c$$

(By above theorem).

$$kd = k(au + bv).$$

$$= pc.u + qc.v$$

$$= (pu + qv)c.$$

$$\hookrightarrow c | kd.$$

$kd = \gcd(ka, kd) \Rightarrow k.\gcd(a,b) = \gcd(ka, kd)$.

__Co-prime__: $g.c.d(a,b) = 1$.

__Thm__: If $d = g.c.d(a,b)$ then $\boxed{a/d \text{ and } b/d}$ are integers prime to each other.

$$\boxed{g.c.d(a,b) = au + bv}$$

$$\Rightarrow 1 = au + bv.$$

To Prove:

$$\boxed{1 = \frac{a}{d}.u + \frac{b}{d}.v}$$

To Prove:

$$\boxed{1 = \frac{a}{d} \cdot u + \frac{b}{d} \cdot v}$$

Proof: $d = g.c.d(a, b)$

$d \mid a$, $md = a$. $m, n \in \mathbb{Z}$.

$d \mid b$, $nd = b$.

$\frac{a}{d} = m$ | $\frac{b}{d} = n$. $\rightarrow$ a/d, $b/d \in \mathbb{Z}$

$1 = au + bv$.

$= \left(\frac{a}{d}\right) + \left(\frac{b}{d}\right)v$.

Thm: If $a \mid bc$ and $g.c.d(a, b) = 1$, then $a \mid c$.

Thm: If $a \mid c$ and $b \mid c$ with $g.c.d(a, b) = 1$.

So, $ab \mid c$.

$4 \mid 12$ and $6 \mid 12$ $g.c.d(4, 6) = 2$.

$(4, 6) = 1$

$\Rightarrow 4 \cdot 6 \nmid 12$.

$(2, 3) = 1$

$(4, 6)$. $(5, 7)$

$5 \mid 35$, $7 \mid 35$ $\quad g.c.d(5,7) = 1$

$\Rightarrow$ $5 \mid 35$

Thm: a prime b and a prime to c then a is also prime to bc.

Try: a is prime b, P.T

i) a^2 is prime to b.

ii) a^2 is prime to b^2.