14th April
Thursday, April 14, 2022 8:33 PM

ELEMENTARY NUMBER THEORY

LEMMA1 :-
$a,b \in \mathbb{N}$ $\quad a = bq + r$ $\quad b \in \mathbb{Z}$ $\quad r \in \mathbb{N}$ $\quad 0 \le r < b$

Pf :- $S = \{ a - bq : q \in \mathbb{Z},\ a - bq \ge 0 \}$
S is a non-empty set of positive integers.
$a \in S$, $S \neq \phi$. So S has a minimal element (say r_0)
$r_0 = a - bq_0$ for some $q_0 \in \mathbb{Z}$.
We need to show that $0 \le r_0 < b$.
Towards a contradiction, assume $r_0 > b$.
Let $r' = r_0 - b$, $r' > 0$.
$r' = a - bq_0 - b = a - b(q_0 + 1) \in S$ (q')
and $r' < r_0$ which contradicts the minimality of r_0. $(\Rightarrow\Leftarrow)$ ∎

★ GCD $\quad (12,6) = \gcd(12,6) = 6$

Ex:★ $\quad (m,n) = (m-n,n)$ $\quad (12,6) = (12-6,6) = (6,6) = 6$

★ **LEMMA2 :-** (Bezout's Lemma)
If $a,b \in \mathbb{N}$ such that $g = (a,b) = \gcd(a,b)$ then $\exists\ x,y \in \mathbb{Z}$
s.t. $ax + by = g$.

Pf :- $S = \{ ax + by : ax + by > 0,\ x,y \in \mathbb{Z} \}$
S is non empty as $a+b \in S$. So S has a minimal element, say g_0. Then $g_0 = ax_1 + by_1$ for some $x_1, y_1 \in \mathbb{Z}$.
as $\gcd(a,b) = g$, $a = ga'$ $\quad b = gb'$ $\quad g_0 = g(a'x_1 + b'y_1)$
$\Rightarrow$ $\boxed{g \mid g_0}$ (divides)

claim :- $g_0 \mid a$ (g_0 divides a)

Pf :- Suppose not. $a = g_0 q + r$, $0 < r < g_0$
$r = a - g_0 q = a - q(ax_1 + by_1)$
$= a(1 - qx_1) + (-qy_1)\, b$
$= ax_1' + by_1' \in S$
and $r < g_0$, which contradicts minimality of g_0. $(\Rightarrow\Leftarrow)$

Similarly $g_0 \mid b$. $\Rightarrow$ $g_0 \mid \gcd(a,b) = g$ $\Rightarrow$ $\boxed{g_0 \mid g}$

$\Rightarrow$ $\boxed{g_0 = g}$ =

★ TASK :- $x^4 + 3x + 7$ ✓, $\quad x^3 + 1x + 1$ $\quad p(15) = ? = 3408$

$p(x)$ $\quad p(1) = ? = 9$ $\quad p(x) = x^3 + 2x + 3$

$p(x) = x^3 + x + 18$

II :- $\quad p(1) = ?$ $\quad p(1) = 17$ $\quad p(19) = 2477267$

$p(x) = x^5 + 2x^2 + 4x + 9$

$$p(x) = x^5 + 3x^2 + 4x + 9$$

★ Primes :- A number p is prime if the set its divisors $= \{1, p\}$.

★ Thm :- There are infinitely many primes.

Pf :- $p_1, p_2, \ldots, p_n$

$$P = p_1 p_2 \cdots p_n + 1$$

None of p_i's divide p_i. So its smallest prime factor is a prime distinct from $p_1, p_2, \ldots, p_n$. ▤

Thm :- (Dirichlet's Thm) If $(a,b) = 1 = \gcd(a,b)$. then there are infinitely many primes of the form $an+b$.
(Proof is tough).

Ex :- There are infinitely many primes of the form $4n+1$, $4n+3$.

$5, 13, 17, \ldots$ ($4\cdot1+1$; $13 = 4\cdot3+1$, $17 = 4\cdot4+1$)

$7 = 4\cdot1+3$, $19 = 4\cdot4+3$, $23 = 4\cdot5+3$.

Q. Prove that there are infinitely many primes of the form $4n+3$.

Soln :- Suppose there are finitely many primes of the form $4n+3$ say $3 < p_1, p_2, \ldots, p_n$. Then consider the number

$$N = 4p_1p_2\cdots p_n + 3 = 4n'+3$$

also none of p_i's divide N.

[Also all prime factors of N cannot be of the form $4K+1$.
(because had it been the case N would have been of the form $4n+1$.)]

So N has a prime factor of the form $4K+3$. ▤