Number Theory 20

30 March 2024 16:36

$x \equiv 0 \pmod 8$ $\quad x \equiv 8 \pmod{125}$

$8 \equiv 8 \pmod{125}$

$x = 8$

$x \equiv 0 \pmod 8$ $\quad x \equiv 4 \pmod{125}$

$8 \equiv 8 \pmod{125}$

$504 \equiv 4 \pmod{125}$

$x \equiv 0 \pmod 4$ $\quad x \equiv 1 \pmod{25}$

$4 \equiv 4 \pmod{25}$ $\quad x = 76$

$76 \equiv 1 \pmod{25}$

Q) Let a and b be relatively prime positive integers. Prove that there are infinitely many relatively prime terms in the AP, $a, a+b, a+2b, a+3b, \ldots$

Ans:- $\gcd(a,b) = 1$ $\quad S_\infty = \{a_1, a_2, a_3, \ldots \infty\}$

$\gcd(a_i, a_j) = 1 \;\forall i, j$ and $i \neq j$

$S_1 = \{a_1\}$

$S_2 = \{a_1, a_2\}$

Base Case:- S_2 exists

$\gcd(a, a+b) = 1$

Inductive assumption:- S_m exists

Inductive Step:- Let $S_m = \{a+k_1 b, a+k_2 b, \ldots, a+k_m b\}$

Then, let $\{p_1, p_2, \ldots, p_n\}$ be the set of all primes that divides $a+k_i b$ for some $i \in \{1, \ldots, m\}$. Then $\exists$ k_{m+1} such that,

$$a + k_{m+1} b \equiv 1 \pmod{p_1 p_2 \cdots p_n}$$

$\Rightarrow \gcd(a+k_{m+1}b, a+k_i b) = 1 \;\forall i \in \{1, 2, \ldots, m\}$

$\Rightarrow S_{m+1}$ exists

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ \vdots \\ x \equiv a_n \pmod{b_n} \end{cases}$$

$\gcd(b_i, b_j) = 1$, $i \neq j$

$\exists$ one distinct x modulo $b_1 b_2 \cdots b_n$

Theorem :- Chinese Remainder Theorem :-

The system of linear equations

$x \equiv a_1 \pmod{b_1}, \ldots x \equiv a_i \pmod{b_i}, \ldots x \equiv a_n \pmod{b_n}$

where $b_1, b_2, \ldots, b_n$ are pairwise coprime has one distinct solution for x (modulo $b_1 b_2 \ldots b_n$)

$ax \equiv b \pmod m$
$\exists$ a solution
if $\gcd(a,m) \equiv$
(set $x = a^{-1}b$)

Proof :- $x \equiv a_1 \pmod{b_1}$, $x \equiv a_2 \pmod{b_2}$

$S = \{ kb_1 + a_1,\ 0 \le k \le b_2 - 1 \}$

$\exists\ k_1, k_2$ such that $b_1 k_1 + b_2 k_2 = 1$

$\Rightarrow x = a_1 b_2 k_2 + a_2 b_1 k_1$

$= a_1(1 - b_1 k_1) + a_2 b_1 k_1 = a_1 + (a_2 - a_1) b_1 k_1$

$= a_2 + (a_1 - a_2) b_2 k_2$

Now let $x \equiv a_1 \pmod{b_1}, \ldots\ldots, x \equiv a_n \pmod{b_n}$

Let $x_{1,2}$ be the solution for first two equations

$\Rightarrow x \equiv x_{1,2} \pmod{b_1 b_2}$

Let us take $x \equiv x_{1,2} \pmod{b_1 b_2}$ and $x \equiv a_3 \pmod{b_3}$
and apply the same process, then we get,
$x_{1,3}$ as the solution for first three equations and so on.

$\Rightarrow x \equiv x_{1,n} \pmod{b_1 b_2 \ldots b_n}$

Let u and v be two distinct the solutions for $x \equiv x_{1,n} \pmod{b_1 b_2 \ldots b_n}$

$\Rightarrow u - v \equiv 0 \pmod{b_1 b_2 \ldots b_n}$

Now $u, v \le b_1 b_2 \ldots b_n$ but $u, v > 0$ $\Rightarrow u = v$

Hence unique solution exists.

Q> Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ $\forall$ positive integers n. Prove that $a = b$

$(\ldots)\ |\ (b^n \ldots) \Leftrightarrow (a^n + n) \,|\, (b^n - a^n)$

of $a^n + n$ $\forall$ positive ...

Ans:- $(a^n+n) \mid (b^n+n) \iff (a^n+n) \mid (b^n - a^n)$

For $a=1$, $(1+n) \mid (b^n+n)$. We need to show for this case that $b \equiv 1 \pmod p$ $\forall$ primes p

$b^n + n \equiv b^n - 1 \pmod{n+1}$

If $p \mid (n+1) \Rightarrow n \equiv -1 \pmod p$

$n \equiv p-1 \pmod p$

$b^n \equiv 1 \pmod p$

$\Rightarrow b^n \equiv 1 \pmod p$ $\forall$ primes p

$\Rightarrow b = 1$

$b^n \equiv b^n - (n+1) \pmod{n+1}$

$\Rightarrow b^n \equiv b^{(p-1)k+1} \pmod p$ if $n \equiv 1 \pmod{p-1}$

$\equiv b \pmod p$

$\Rightarrow b^n \equiv b \pmod p$ $\forall$ primes p

$\Rightarrow b = 1$ $\Rightarrow a = b = 1$

Let us set $n \equiv -a \pmod p$ and $n \equiv 1 \pmod{p-1}$

$p \mid (a^n+n)$ for $n \equiv -a \pmod p$ $\Rightarrow$ $p \mid (b^n - a^n)$

And, $b^n \equiv b \pmod p$ and $a^n \equiv a \pmod p$

$b - a \equiv (b^n - a^n) \pmod p \equiv 0 \pmod p$

$\Rightarrow b \equiv a \pmod p$ for all primes p

$\Rightarrow b = a$

Homework:- Prove that $\exists$ a x such that $x^2 \equiv -1 \pmod p$ iff $p \equiv 1 \pmod 4$