Student Information

Full Name : Batuhan Karaca

Id Number : 2310191

Answer 1

We know if $a \equiv 1 \ (mod \ p)$, $a^2 \ mod \ p = (a \ mod \ p)(a \ mod \ p) = 1$. Similarly, $a^3 \ mod \ p = (a^2 \ mod \ p)(a \ mod \ p) = 1$, $a^4 \ mod \ p = (a^3 \ mod \ p)(a \ mod \ p)$. We have:

$$a^n \ mod \ p = (a^{n-1} \ mod \ p)(a \ mod \ p) = 1 \quad (n \in \mathbb{Z}^+)$$
$$a^n \equiv 1 \ (mod \ p)$$

We know, $x^y \equiv 1 \ (mod \ p)$. Substituting:

$$(x^y)^n \equiv 1 \ (mod \ p)$$
$$x^{ny} \equiv 1 \ (mod \ p)$$

Assume, there exists $b \in \mathbb{Z}^+$ such that $y \nmid b$, $b > y$ and $x^b \equiv 1 \ (mod \ p)$. Then b is of the form $n_0 y + k$ such that $k, n_0 \in \mathbb{Z}^+$ and $k < y$:

$$x^{n_0 y + k} \equiv 1 \ (mod \ p)$$
$$x^{n_0 y} x^k \equiv 1 \ (mod \ p)$$
$$x^{n_0 y} x^k \ mod \ p = (x^{n_0 y} \ mod \ p)(x^k \ mod \ p) = (x^k mod \ p)$$
$$x^k \equiv 1 \ (mod \ p)$$

However, since $k < y$ and $k \neq 0$, this is not the case. Hence by contradiction, every $s \in \mathbb{Z}^+$ satisfying $x^s \equiv 1 (mod \ p)$ is of the form ny.

Since p is prime such that $p \nmid x$, by Fermat's Little Theorem:

$x^{p-1} \equiv 1 \ (mod \ p)$

Since p is prime, $p > 1$ then $p - 1 \in \mathbb{Z}^+$. Furthermore p satisfies $x^{p-1} \equiv 1 \ (mod \ p)$. Then $p - 1$ is in the set $S = \{s \mid s = ny\}$. Then for some $n = k$:

$p - 1 = ky$
$(p - 1)/y = k$

Since $k \in \mathbb{Z}^+$, $y \mid p - 1$.

Answer 2

Assume $p(n) = 2n^2 + 10n - 7$

$p(n) = 2n^2 + 10n - 7$
$p(n) = 2n^2 + 10n - 72 + 65$
$p(n) = (2n + 18)(n - 4) + 65$
$p(n) = 2(n + 9)(n - 4) + 65$

The Fundemental Theorem Of Arithmetic is defined as

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.

In the textbook (8th Edition) page 272. Then:

$p(n) = p_0^{a_0} * p_1^{a_1} * p_2^{a_2} * ... * p_k^{a_k} \quad (a_i \in \mathbb{N}) \ (1)$

such that p_i is in the set of prime numbers and $p_i < p_{i+1}$. Another theorem from the textbook, page 252 (8th Edition), Theorem 1:

Let a, b, and c be integers, where $a \neq 0$. Then

if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$ (2)

Assume for every $n \in \mathbb{Z}^+$ satisfying $13 \mid p(n)$ holds. Then since $13 \mid p(n)$ and $13 \mid -65$,

$13 \mid p(n) - 65$

$13 \mid 2(n+9)(n-4)$

$13 \mid (n+9)(n-4)$ (*since* $13 \nmid 2$)

Since 13 is a prime number, at least one of the set $\{(n+9), (n-4)\}$ is divisible by 13. Since $(n+9) = (n-4)+13$ and $(n-4) = (n+9)+(-13)$, similarly by (2), if $13 \mid (n-9)$ it also divides $13 \mid (n-4)$ and vice versa. Hence $169 \mid (n+9)(n-4)$, but $169 \nmid 2$ and $169 \nmid 65$, we have

$$p(n) \equiv 65 \ (mod\ 169)$$

for some $t \in \mathbb{N}$. Furthermore:

$$p(n) \equiv 2(n+9)(n-4) \ (mod\ 13)$$

Assume for every $n \in \mathbb{Z}^+$ satisfying $13 \nmid p(n)$ holds. Then using (1)

$$p(n) = p_0^{a_0} * p_1^{a_1} * p_2^{a_2} * ... * 13^0 * ... * p_k^{a_k} \quad (a_i \in \mathbb{N}) \ (1)$$

If $169 \mid p(n)$:

$$p(n) = p_0^{a_0} * p_1^{a_1} * p_2^{a_2} * ... * 13^{2+t} * ... * p_k^{a_k} \quad (a_i \in \mathbb{N}) \ (1)$$

for some $t \in \mathbb{N}$. However, $t + 2 \geq 2 > 0$. Then by contradiction, $169 \nmid p(n)$

We proved $169 \nmid p(n)$ for every $n \in \mathbb{Z}^+$ satisfying $13 \mid p(n)$ holds, and for every $n \in \mathbb{Z}^+$ satisfying $13 \nmid p(n)$ holds . Since every $n \in \mathbb{Z}^+$ satisfying $13 \mid p(n)$ or $13 \nmid p(n)$ comprise the set $\mathbb{Z}^+$,

we proved for every $n \in \mathbb{Z}^+$, $169 \nmid p(n)$.

Answer 3

Since $a \equiv b \ (mod\ m)$, $m \mid a-b$, and since $a \equiv b \ (mod\ n)$, $n \mid a-b$.

The Fundemental Theorem Of Arithmetic is defined as

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.

In the textbook (8th Edition) page 272. Then we can write for all $i \in \mathbb{N}$

$$m = p_0^{a_0} * p_1^{a_1} * p_2^{a_2} * ... * p_k^{a_k} \quad (a_i \in \mathbb{N})$$
$$n = p_0^{c_0} * p_1^{c_1} * p_2^{c_2} * ... * p_k^{c_k} \quad (c_i \in \mathbb{N})$$

such that p_i is in the set of prime numbers and $p_i < p_{i+1}$. We know

$$gcd(m,n) = p_0^{min(a_0,c_0)} * p_1^{min(a_1,c_1)} * p_2^{min(a_2,c_2)} * ... * p_k^{min(a_k,c_k)} = 1$$

Since $a_i, c_i \in \mathbb{N}$, $min(a_i, c_i) \in \mathbb{N}$. If $min(a_j, c_j) \neq 0$ for some j, $gcd(m,n) > 1$. However, $gcd(m,n) = 1$. Hence by contradiction, $min(a_j, c_j) = 0$. Then a_i or c_i is zero. We have also

$$lcm(m,n) = p_0^{max(a_0,c_0)} * p_1^{max(a_1,c_1)} * p_2^{max(a_2,c_2)} * ... * p_k^{max(a_k,c_k)}$$
$$lcm(m,n) = p_0^{z_0} * p_1^{z_1} * p_2^{z_2} * ... * p_k^{z_k}$$

such that z_i is a_i or c_i. We know $m \mid a-b$, then $p_i^{a_i} \mid a-b$ and $n \mid a-b$, then $p_i^{c_i} \mid a-b$. Then $a-b$ has prime factor $p_i^{d_i}$ such that $p_i^{a_i} \mid p_i^{d_i}$ and $p_i^{c_i} \mid p_i^{d_i}$, hence $d_i \geq max(a_i, c_i)$, which is $d_i \geq z_i$. Since we also know a_i or c_i is zero, $a_i + c_i = z_i$. We have $d_i \geq a_i + c_i$. Then $p_i^{a_i+c_i} \mid p_i^{d_i}$,

hence $p_i^{a_i+c_i} \mid a-b$. We know

$$mn = p_0^{a_0+c_0} * p_1^{a_1+c_1} * p_2^{a_2+c_2} * ... * p_k^{a_k+c_k}$$

Then $mn \mid a-b$. Hence $a \equiv b \ (mod\ mn)$. Emphasizing on the fact that i represents every natural number.

Answer 4

Assume $P(n,k) = \sum_{j=1}^{n} \prod_{i=0}^{k-1}(j+i)$ and $Q(n,k) = \frac{(n+k)!}{(n-1)!(k+1)}$.

BASIS STEP

$P(1,k) = \sum_{j=1}^{1} \prod_{i=0}^{k-1}(j+i) = \prod_{i=0}^{k-1}(1+i) = k!$

$Q(1,k) = \frac{(1+k)!}{0!(k+1)} = k!$

$P(1,k) = Q(1,k) \quad (\forall k \in \mathbb{Z}^+)$

INDUCTIVE STEP

Assume $P(n,k) = Q(n,k) \quad (\forall n,k \in \mathbb{Z}^+)$.

$P(n+1,k) = \sum_{j=1}^{n+1} \prod_{i=0}^{k-1}(j+i) = \sum_{j=1}^{n} \prod_{i=0}^{k-1}(j+i) + \frac{(n+k)!}{n!}$

$P(n+1,k) = P(n,k) + \frac{(n+k)!}{n!}$

$P(n+1,k) = Q(n,k) + \frac{(n+k)!}{n!}$

$P(n+1,k) = \frac{(n+k)!}{(n-1)!(k+1)} + \frac{(n+k)!}{n!}$

$P(n+1,k) = \frac{(n+k)!}{(n-1)!}(\frac{1}{k+1} + \frac{1}{n})$

$P(n+1,k) = \frac{(n+k)!}{(n-1)!}(\frac{n+k+1}{n(k+1)})$

$P(n+1,k) = \frac{(n+k+1)!}{n!(k+1)} = \frac{(n+1+k)!}{n!(k+1)} = Q(n+1,k)$

$P(n+1,k) = Q(n+1,k)$

$(P(n,k) = Q(n,k)) \rightarrow (P(n+1,k) = Q(n+1,k))$

Since $P(1,k) = Q(1,k)$ and $(P(n,k) = Q(n,k)) \rightarrow (P(n+1,k) = Q(n+1,k))$ hold for all $n, k \in \mathbb{Z}^+$, by induction, $P(n,k) = Q(n,k)$ for all $n, k \in \mathbb{Z}^+$.

Answer 5

BASIS STEP

$H_0 = 1 \leq 7^1 = 7$, $H_1 = 3 \leq 7^3 = 343$ and $H_2 = 5 \leq 7^5 = 16807$.

INDUCTIVE STEP

Assume for all $a \in \{1, 2, 3, ..., k\}, H_a \leq 7^a$. We have:

$$H_{k+1} = 5H_k + 5H_{k-1} + 63H_{k-2}$$
$$H_k \leq 7^k \rightarrow 5H_k \leq 5(7^k) \quad (1)$$
$$H_{k-1} \leq 7^{k-1} \rightarrow 5H_{k-1} \leq 5(7^{k-1}) \quad (2)$$
$$H_{k-2} \leq 7^{k-2} \rightarrow 63H_{k-2} \leq 63(7^{k-2}) \quad (3)$$

Summing right sides of $(1), (2), (3)$:

$$H_{k+1} = 5H_k + 5H_{k-1} + 63H_{k-2} \leq 5(7^k) + 5(7^{k-1}) + 63(7^{k-2})$$
$$H_{k+1} \leq 7^{k-2}(5(7^2) + 5(7) + 63)$$
$$H_{k+1} \leq 7^{k-2}(343)$$
$$H_{k+1} \leq 7^{k-2}(7^3)$$
$$H_{k+1} \leq 7^{k+1}$$

Completes the proof.