Modular Exponentiation

Nandana Madhukara

San Diego Math Circle

May 28, 2024

Modular Arithmetic

Review Questions

Question

How many integers between 1000 and 3000 inclusive are congruent to $5 \pmod 7$*?*

Question

Find the smallest natural number n such that

$$617n = 943n \pmod{18}.$$

Question

Find

$$17 + 177 + \cdots + 177777777777777777777 \pmod 8.$$

Review Questions Solutions

Solution 1

- First number is 1006 and last number is 2994.
- Numbers are spaced 7 apart so answer is $\boxed{285}$.

Review Questions Solutions

Solution 1

- First number is 1006 and last number is 2994.
- Numbers are spaced 7 apart so answer is $\boxed{285}$.

Solution 2

- $617 \equiv 5 \pmod{18}$ and $943 \equiv 7 \pmod{18}$
- Therefore, we have $5n \equiv 7n \pmod{18}$ so smallest n is $\boxed{9}$.

Review Questions Solutions

Solution 1

- First number is 1006 and last number is 2994.
- Numbers are spaced 7 apart so answer is $\boxed{285}$.

Solution 2

- $617 \equiv 5 \pmod{18}$ and $943 \equiv 7 \pmod{18}$
- Therefore, we have $5n \equiv 7n \pmod{18}$ so smallest n is $\boxed{9}$.

Solution 3

- $17 \equiv 1 \pmod 8$, $177 \equiv 1 \pmod 8$, $1777 \equiv 1 \pmod 8$, ...
- Therefore the sum is $20 \equiv \boxed{4}$ modulo 8.

More Challenging Questions

Question

The Fibonacci sequence is defined by $F_1 = F_2 = 1$ *and* $F_{n+2} = F_{n+1} + F_n$. *Find the remainder when* F_{2006} *is divided by 5.*

Question

Find all prime numbers p *for which* $p^2 - 1$ *is not a multiple of 24.*

Question

Find the remainder when 3^{31} *is divided by 7.*

Challenge Questions Solutions

Solution 1

- Fibonacci sequence modulo 5:

$$1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, \ldots$$

Challenge Questions Solutions

Solution 1

- Fibonacci sequence modulo 5:

$$1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, \ldots$$

- Repeats every 20 and $2006 \equiv 6 \pmod{20}$.

Challenge Questions Solutions

Solution 1

- Fibonacci sequence modulo 5:

$$1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, \ldots$$

- Repeats every 20 and $2006 \equiv 6 \pmod{20}$.
- Therefore, we have $F_{2006} \equiv \boxed{3} \pmod{5}$.

Challenge Questions Solutions

Solution 1

- Fibonacci sequence modulo 5:

$$1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, \ldots$$

- Repeats every 20 and $2006 \equiv 6 \pmod{20}$.
- Therefore, we have $F_{2006} \equiv \boxed{3} \pmod{5}$.

Solution 2

- Notice that $p = 2$ and $p = 3$ both work since $2^2 - 1 = 3$ and $3^2 - 1 = 8$ are not multiples of 24.

Challenge Questions Solutions

Solution 1

- Fibonacci sequence modulo 5:

$$1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, \ldots$$

- Repeats every 20 and $2006 \equiv 6 \pmod{20}$.
- Therefore, we have $F_{2006} \equiv \boxed{3} \pmod{5}$.

Solution 2

- Notice that $p = 2$ and $p = 3$ both work since $2^2 - 1 = 3$ and $3^2 - 1 = 8$ are not multiples of 24.
- Every primes greater than 3 is next to a multiple of 6 so $p^2 - 1 \equiv 0 \pmod{6}$.

Challenge Questions Solutions (contd.)

Solution 2 (contd.)

- All primes greater than 2 are odd so $p = 2k + 1$.

Challenge Questions Solutions (contd.)

Solution 2 (contd.)

- All primes greater than 2 are odd so $p = 2k + 1$.
- We have

$$p^2 - 1 = (2k+1)^2 - 1 = 4k(k+1) \equiv 0 \pmod 4.$$

Challenge Questions Solutions (contd.)

Solution 2 (contd.)

- All primes greater than 2 are odd so $p = 2k + 1$.
- We have

$$p^2 - 1 = (2k+1)^2 - 1 = 4k(k+1) \equiv 0 \pmod{4}.$$

- Therefore $p^2 - 1 \equiv 0 \pmod{24}$ if $p \neq 2, 3$.

Challenge Questions Solutions (contd.)

Solution 2 (contd.)

- All primes greater than 2 are odd so $p = 2k + 1$.
- We have

$$p^2 - 1 = (2k+1)^2 - 1 = 4k(k+1) \equiv 0 \pmod{4}.$$

- Therefore $p^2 - 1 \equiv 0 \pmod{24}$ if $p \neq 2, 3$.

Solution 3

- $3^3 = 27 \equiv -1 \pmod{7}$
- Therefore, we have $3^{31} \equiv 3 \cdot (3^3)^{10} \equiv \boxed{3} \pmod{7}$.

Fermat's Little Theorem

The Theorem

Theorem (Fermat's Little Theorem)

If a is an integer, p is a prime number, and a is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

The Theorem

Theorem (Fermat's Little Theorem)

If a is an integer, p is a prime number, and a is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Problem

Find

- $3^{31} \pmod{7}$
- $2^{35} \pmod{7}$
- $128^{129} \pmod{17}$
- $2^{1000} \pmod{13}$
- $29^{25} \pmod{11}$

The Proof

Proof.

- We fix a p and do induction on a

The Proof

Proof.

- We fix a p and do induction on a
- Base Case: $1^p \equiv 1 \pmod{p}$

The Proof

Proof.

- We fix a p and do induction on a
- Base Case: $1^p \equiv 1 \pmod{p}$
- Inductive Step: Assume $a^p \equiv a \pmod{p}$ and we have to prove $(a+1)^p \equiv a+1 \pmod{p}$

The Proof

Proof.

- We fix a p and do induction on a
- Base Case: $1^p \equiv 1 \pmod{p}$
- Inductive Step: Assume $a^p \equiv a \pmod{p}$ and we have to prove $(a+1)^p \equiv a+1 \pmod{p}$
- Binomial Theorem:

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots \binom{p}{p-1} a + 1$$

The Proof

Proof.

- We fix a p and do induction on a
- Base Case: $1^p \equiv 1 \pmod{p}$
- Inductive Step: Assume $a^p \equiv a \pmod{p}$ and we have to prove $(a+1)^p \equiv a+1 \pmod{p}$
- Binomial Theorem:

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots \binom{p}{p-1} a + 1$$

- Taking modulo p gives us $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$.

$\blacksquare$

Challenging Problems

Problem

Solve the congruence

$$x^{103} \equiv 4 \pmod{11}.$$

Problem

Find all integers x such that $x^{86} \equiv 6 \pmod{29}$.

Problem

Let

$$a_1 = 4, a_n = 4^{a_{n-1}}, n > 1$$

Find $a_{100} \pmod{7}$.

Very Challenging Problems

Problem

If a googolplex is $10^{10^{100}}$, what day of the week will it be a googolplex days from today?

Problem

Find all positive integers x such that $2^{2^x+1}+2$ is divisible by 17.

Euler's Totient Function

Euler's Totient Function

Definition (Euler's totient function)

Euler's totient function $\phi(n)$ is the number of integers in $\{1, 2, ..., n\}$ that have no common divisors with n.

Problem

Find $\phi(17)$, $\phi(81)$, *and* $\phi(100)$.

Euler's Totient Function

Definition (Euler's totient function)

Euler's totient function $\phi(n)$ is the number of integers in $\{1, 2, ..., n\}$ that have no common divisors with n.

Problem

Find $\phi(17)$, $\phi(81)$, *and* $\phi(100)$.

Proposition

- $\phi(p) = p - 1$
- $\phi(p^n) = p^n - p^{n-1}$
- $\phi(nm) = \phi(n)\phi(m)$ *when* $\gcd n, m = 1$

Euler's Theorem

Proposition

If the prime factorization of n is $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$, then

$$\begin{aligned} \phi(n) &= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

Euler's Theorem

Proposition

If the prime factorization of n is $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$, *then*

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$
$$= n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Theorem (Euler's Theorem)

If a and n have no common divisors, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Challenge Problems

Problem

What is the last digit of 7^{2013}?

Problem

Find the last two digits of 2^{2013}.

Problem

Find the last two digits of $7^{81} - 3^{81}$.

Problem

Find the last two digits of $3^{3^{3^{\cdots}}}$ where there are 2024 3's.

The End

Fin.