MAT115A HW5

Tao Wang

November 12, 2024

(1)

Find the least nonnegative residue modulo m of each integer n below.

(a):

$$n = 29^{202}, m = 13$$

Answer:

$$(29, 13) = 1$$
$$\phi(13) = 12$$
$$202 = (16)(12) + 10$$

Since $(29, 13) = 1$, by Euler's Theorem,

$$29^{12} \equiv 1 (\text{mod } 13)$$

Therefore,

$$29^{12} \equiv 1 \equiv (29^{12})^{16} (\text{mod } 13)$$

$$29^{202} \equiv (29^{12})^{16} 29^{10} \equiv 29^{10} \equiv 3^{10} \equiv 3 (\text{mod } 13)$$

$$\boxed{29^{202} \equiv 3 (\text{mod } 13)}$$

(b):

$$n = 79^{79}, m = 9$$

Answer:

$$(79, 9) = 1$$
$$\phi(9) = 6$$
$$79 = 6(13) + 1$$

$$\text{Since } (79, 9) = 1, \text{ by Euler's Theorem, } 79^6 \equiv 1(\text{mod } 9)$$

$$7^{79} \equiv 79^{6(13)}79 \equiv 79 \equiv 7(\text{mod } 9)$$

$$\boxed{79^{79} \equiv 7(\text{mod } 9)}$$

(c):

$$n = 99^{99999}, m = 26$$

Answer:

$$(99, 26) = 1$$
$$\phi(26) = 12$$
$$99999 = (8333)(12) + 3$$

Since $(99, 26) = 1$, by the Euler's Theorem, $99^{12} \equiv 1(\text{mod } 26)$

$$(99^{12})^{8333}(99^3) \equiv 99^3 \equiv 21^3 \equiv (25)(21) \equiv 5(\text{mod } 26)$$

$$\boxed{99^{99999} \equiv 5(\text{mod } 6)}$$

(2)

Proposition:

$645 = 3 \cdot 5 \cdot 43$ is a pseudoprime (to base 2).

Proof:

645 is a composite because $645 = 3 \cdot 5 \cdot 43$.

$$
\begin{aligned}
2^2 \equiv 1 (\text{mod } 3) &\implies 2^{644} \equiv 1 (\text{mod } 3) \\
2^4 \equiv 1 (\text{mod } 5) &\implies 2^{644} \equiv 1 (\text{mod } 5) \\
2^{42} \equiv 1 (\text{mod } 43) &\implies 2^{644} \equiv 1 (\text{mod } 43)
\end{aligned}
$$

By the Chinese Remainder Theorem,

$$2^{644} \equiv 1 (\text{mod } 645)$$

and

$$\boxed{2^{645} \equiv 2 (\text{mod } 645)}$$

□

Exercise (3)

Proposition:

$2821 = 7 \cdot 13 \cdot 31$ is a Carmichael number.

Proof:

We'll show the proposition is true by Theorem 3.1.42.

First, 2821 is composed of more than 2 distinct primes.

Then,

$$
\begin{aligned}
(7 - 1) &\mid 2820 \\
(13 - 1) &\mid 2820 \\
(31 - 1) &\mid 2820
\end{aligned}
$$

As a result, 2821 is a carmichael number.

□

Exercise (4)

Proposition:

Let p and q be distinct odd prime numbers. Prove $p^{q-1} + q^{p-1} \equiv (\text{mod } pq)$.

Proof:

By the Euler Theorem,

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

By the definition of modulo,

$$p^{q-1} \equiv 0(\text{mod } p)$$

$$q^{p-1} \equiv 0(\text{mod } q)$$

From the results above, for $m, n \in \mathbb{Z}$,

$$p^{q-1} - 1 = qm$$
$$q^{p-1} = qn$$

and

$$p^{q-1} + q^{p-1} - 1 = q(m+n)$$
$$\implies p^{q-1} + q^{p-1} \equiv 1(\text{mod } q)$$

Similarly,

$$p^{q-1} + q^{p-1} \equiv 1(\text{mod } p)$$

Since p and q are co-prime, by the Chinese Remainder Theorem,

$$p^{q-1} + q^{p-1} \equiv 1(\text{mod } pq)$$

□

Exercise (5)

Proposition:

Let p be a prime number. Prove that $2^p - 1$ is either a prime or a pseudoprime (to the base 2).

Proof:

Since $p \nmid 2$, by Fermat's Little Theorem, $2^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

$$2^{p-1} = 1 + mp \implies 2^p = 2 + 2mp \implies 2^p - 2 = 2mp$$

Therefore,

$$2^{2^p-2} = 2^{2mp} = (2^p)^{2m}$$

By the definition of modulo equivalence,

$$\begin{aligned} 2^p &\equiv 1 (\mathrm{mod}\ 2^p - 1) \\ \implies (2^p)^{2m} &\equiv 1 (\mathrm{mod}\ 2^p - 1) \\ \implies 2^{2^p-2} &\equiv 1 (\mathrm{mod}\ 2^p - 1) \\ \implies 2^{2^p-1} &\equiv 2 (\mathrm{mod}\ 2^p - 1) \end{aligned}$$

As a result, when $2^p - 1$ is a composite, it must be a pseudoprime.

$\square$

Exercise (6)

Proposition:

Let n be an integer not divisible by 3. Prove that $n^7 \equiv n (\mathrm{mod}\ 63)$.

Proof:

Since $3 \nmid n$, $(n, 7) = 1$ and $(n, 9) = 1$.
By Euler's Theorem,

$$\begin{aligned} n^{\phi(7)} &\equiv 1 (\mathrm{mod}\ 7) \\ n^6 &\equiv 1 (\mathrm{mod}\ 7) \\ n^7 &\equiv n (\mathrm{mod}\ 7) \end{aligned}$$

and

$$
\begin{aligned}
n^{\phi(9)} &\equiv 1 (\text{mod } 9) \\
n^6 &\equiv 1 (\text{mod } 9) \\
n^7 &\equiv n (\text{mod } 9)
\end{aligned}
$$

Since (7, 9) = 1, by the Chinese Remainder Theorem,

$$n^7 \equiv n (\text{mod } 63)$$

$\square$