MAT115A HW6

Tao Wang

November 22, 2024

(1)

Question:

Find the order of 9 modulo 17.

Answer:

$$\{9^1, 9^2, 9^3, 9^4, 9^5, 9^6, 9^7, 9^8\}(\text{mod } 17) = \{9, 13, 15, 16, 8, 4, 2, 1\}$$

By Definition 4.1.1, $\text{ord}_m a$ is the n where $a^n \equiv 1(\text{mod } m)$. Since $9^8 \equiv 1(\text{mod } 17)$ and 8 is the least positive integer to satisfy this property, $\boxed{\text{ord}_{17} 9 = 8}$.

(2)

Question:

Find all incongruent primitive roots modulo 18.

Answer:

$$\{5^1, 5^2, 5^3, 5^4, 5^5, 5^6\}(\text{mod } 18) = \{5, 7, 17, 13, 11, 1\}$$

By Corollary 4.1.14.2, the number of incongruent primitive roots modulo 18 is $\phi(\phi(18)) = 2$.

Also,

$$\{11^1, 11^2, 11^3, 11^4, 11^5, 11^6\}(\text{mod } 18) = \{5, 7, 17, 13, 11, 1\}$$

Therefore, the two incongruent primitive roots modulo 18 are $\boxed{\text{5 and 11}}$.

(3)(a)

Proposition:

Let m be a positive integer and let a, b be integers relatively prime to m with $(\text{ord}_m a, \text{ord}_m b) = 1$. Prove that $\text{ord}_m(ab) = (\text{ord}_m a)(\text{ord}_m b)$.

Proof:

We have $\text{ord}_m a = x$ and $\text{ord}_m b = y$.

Therefore, $a^x \equiv 1(\text{mod } m)$ and $b^y \equiv 1(\text{mod } m)$.

$$(ab)^{xy} = (a^x)^y(b^y)^x \equiv 1^y 1^x \equiv 1(\text{mod } m)$$

By Proposition 4.1.1, $\text{ord}_m(ab) \mid xy$ and $\text{ord}_m(ab) \mid (\text{ord}_m a)(\text{ord}_m b)$

Also, let $n = \text{ord}_m(ab)$. Then,

$$((ab)^n)^y = (a^{ny})(b^y)^n = a^{ny} \equiv 1(\text{mod } m)$$

This implies $x \mid ny$, which implies $x \mid n$ because $(x, y) = 1$. Similarly, we could show that $y \mid n$.

Since $(x, y) = 1$, $x \mid n$ and $y \mid n$ implies $xy \mid n$ or $(\text{ord}_m a)(\text{ord}_m b) \mid \text{ord}_m(ab)$

Since we've proven divisibility in both direction, $\text{ord}_m(ab) = (\text{ord}_m a)(\text{ord}_m b)$

□

(3)(b)

Question:

Show that $(\text{ord}_m a, \text{ord}_m b) = 1$ cannot be eliminated from part (a).

Answer:

We need $(\text{ord}_m a, \text{ord}_m b) = 1$ to show that $(\text{ord}_m a)(\text{ord}_m b) \mid \text{ord}_m(ab)$.

(4)

Proposition:

> Show that r is a primitive root modulo the odd prime p if and only if r is an integer with $(r, p) = 1$ such that
>
> $$r^{\frac{p-1}{q}} \not\equiv 1(\text{mod } p)$$
>
> for all prime divisors q of $p - 1$.

Proof:

> We'll first show that r is a primitive root modulo p implies $(r, p) = 1$ and $r^{\frac{p-1}{q}} \not\equiv 1(\text{mod } p)$
>
> r is a primitive root modulo p implies that $(r, p) = 1$ and $r^{\phi(p)} \equiv 1(\text{mod } p)$.
>
> Since $\phi(p) = p - 1$, we have $r^{p-1} \equiv 1(\text{mod } p)$. Assume that $r^{\frac{p-1}{q}} \equiv 1(\text{mod } p)$, then there's a contradiction because $\frac{p-1}{q} < p - 1$ and r is a primitive root guarantees that p - 1 is the smallest integer n to make $r^n \equiv 1(\text{mod } p)$.
>
> Therefore, $r^{\frac{p-1}{q}} \not\equiv 1(\text{mod } p)$.
>
> Next, we'll show that the converse is true. By the Euler's Theorem, $(r, p) = 1$ implies $a^{\phi(p)} \equiv 1(\text{mod } p)$.
>
> By Proposition 4.1.3, $\text{ord}_m r \mid p - 1$.
>
> Assume $\text{ord}_m r < p - 1$ and $p - 1 = bq$ for some integer b and the prime divisor q, then $(\text{ord}_m r)(a) = \frac{p-1}{q}$ for some integer a.
>
> By Definition 4.1.1, $r^{\text{ord}_m r} \equiv 1(\text{mod } p)$, so $r^{(\text{ord}_m r)(a)} = (r^{\text{ord}_m r})^a \equiv r^{\frac{p-1}{q}} \equiv 1(\text{mod } p)$.
>
> This contradicts our hypothesis that $r^{\frac{p-1}{q}} \not\equiv 1(\text{mod } p)$. Therefore, $\text{ord}_m r = p - 1 = \phi(p)$ and r is a primitive root.

$\square$

(5)

Proposition:

> Show that if r is a primitive root modulo the positive integer m, then $\bar{r}$, the inverse of r modulo m, is also a primitive root modulo m.

Proof:

Since $\bar{r}$ is the inverse of r,

$$(r)(\bar{r}) \equiv 1 (\bmod m)$$

$$\implies ((r)(\bar{r}))^{\phi(m)} \equiv 1 (\bmod m)$$

However, r is a primitive root modulo m implies $r^{\phi(m)} \equiv 1 (\bmod m)$.
Both statements are true if and only if $\bar{r}^{\phi(m)} \equiv 1 (\bmod m)$.

$\phi(m)$ must also be the least root for $\bar{r}$.
Assume that there exists $k < \bar{r}$, then $r^k \equiv 1 (\bmod m)$ holds because $(r)(\bar{r}) \equiv 1 (\bmod m)$. However, this contradicts with the fact the r is a primitive root.

As a result, $\bar{r}$ is also a primitive root modulo m.

$\square$