A Book of Abstract Algebra | (2nd Edition)

Problem

Use parts 4 and 6 to explain why the following are true:

(*a*) $a^{12} \equiv 1 \pmod{180}$ for every *a* such that gcd(*a*, 180) = 1.

(*b*) $a^{42} \equiv 1 \pmod{1764}$ if gcd (*a*, 1764) = 1. (REMARK: 1764 = 4 × 9 × 49.)

(*c*) $a^{60} \equiv 1 \pmod{1800}$ if gcd (*a*, 1800) = 1.

Step-by-step solution

Step 1 of 5

Consider the following result:

If $\gcd(m, n) = 1, \gcd(a, mn) = 1$, then

$a^{\phi(m)\phi(n)} \equiv 1(\bmod mn)$.

If *t* is a common multiple of $\phi(m), \phi(n)$, then

$a^{t} \equiv 1(\bmod mn)$.

For some prime *p*,

$\phi(p^n) = p^n - p^{n-1}$.

Comment

Step 2 of 5

(a)

Objective is to show that $a^{12} \equiv 1(\bmod 180)$ for every *a* such that $\gcd(a, 180) = 1$.

The $180 = 2^2 \times 3^2 \times 5$. Let $l = 2^2, m = 3^2, n = 5$ also $\gcd(l, m, n) = 1$. Then,

$$\begin{aligned}\phi(l) &= 2^2 - 2 \\ &= 2, \\ \phi(m) &= 6, \\ \phi(n) &= 4.\end{aligned}$$

Let $t = 12$, which is the common multiple of $\phi(l), \phi(m), \phi(n)$. Then by the above result, it implies that

$$a^{12} \equiv 1 \pmod{180}.$$

Comment

Step 3 of 5

(b)

Objective is to show that $a^{42} \equiv 1 \pmod{1764}$ for every *a* such that $\gcd(a, 1764) = 1$.

The $1764 = 2^2 \times 3^2 \times 7^2$. Let $l = 2^2, m = 3^2, n = 7^2$ also $\gcd(l, m, n) = 1$. Then,

$$\begin{aligned}\phi(l) &= 2^2 - 2 \\ &= 2, \\ \phi(m) &= 6, \\ \phi(n) &= 42.\end{aligned}$$

Let $t = 42$, which is the common multiple of $\phi(l), \phi(m), \phi(n)$. Then by the above result, it implies that

$$a^{42} \equiv 1 \pmod{1764}.$$

Comment

Step 4 of 5

(c)

Objective is to show that $a^{60} \equiv 1 \pmod{1800}$ for every *a* such that $\gcd(a, 1800) = 1$.

The $180 = 2^3 \times 3^2 \times 5^2$. Let $l = 2^3, m = 3^2, n = 5^2$ also $\gcd(l, m, n) = 1$. Then,

$$\begin{aligned}\phi(l) &= 2^3 - 2^2 \\ &= 4, \\ \phi(m) &= 6, \\ \phi(n) &= 20.\end{aligned}$$

Let $t = 60$, which is the common multiple of $\phi(l), \phi(m), \phi(n)$.

Comment

Step 5 of 5

Then by the above result, it implies that $a^{60} \equiv 1 \pmod{1800}$.

Comment