A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 8EE

Bookmark

Show all steps: ON

Problem

Use part 6 to explain why the following are true:

(*a*) $a^{19} \equiv a \pmod{133}$.

(*b*) $a^{10} \equiv 1 \pmod{66}$, provided *a* is not a multiple of 2, 3, or 11.

(*c*) $a^{13} \equiv a \pmod{105}$.

(*d*) $a^{49} \equiv a \pmod{1547}$. (HINT: 1547 = 7 × 13 × 17.)

Step-by-step solution

Step 1 of 4

Consider any two distinct prime numbers *p* and *q*. Suppose $(p-1)\mid m$ and $(q-1)\mid m$. Then

$$a^m \equiv 1 \pmod{pq},$$

where $p \nmid a$ and $q \nmid a$. Also

$$a^{m+1} \equiv a \pmod{pq},$$

for integers *a*.

Objective is to use this result and prove the following parts:

(a)

Prove that $a^{19} \equiv a \pmod{133}$.

The $133 = 7 \times 19$. Note that, 18 is divisible by $(7-1)$ and $(19-1)$. So, by using the second part of result, it implies that $a^{19} \equiv a \pmod{133}$. The is so because *a* is some arbitrary integer.

Comment

Step 2 of 4

(b)

Prove that $a^{10} \equiv 1 \pmod{66}$, where *a* is not a multiple of $2, 3$, or 11.

The $66 = 2\times 3\times 11$. Note that, 10 is divisible by $(2-1), (3-1)$ and $(11-1)$. So, by using the first part of result, it implies that $a^{10} \equiv 1 \pmod{66}$.

Comment

Step 3 of 4

(c)

Prove that $a^{13} \equiv a \pmod{105}$.

The $105 = 3\times 5\times 7$. Note that, 12 is divisible by $(3-1), (5-1)$ and $(7-1)$. So, by using the second part of result, it implies that $a^{13} \equiv a \pmod{105}$. The is so because *a* is some arbitrary integer.

Comment

Step 4 of 4

(d)

Prove that $a^{49} \equiv a \pmod{1547}$.

The $1547 = 7\times 13\times 17$. Note that, 48 is divisible by $(7-1), (13-1)$ and $(17-1)$. So, by using the second part of result, it implies that $a^{49} \equiv a \pmod{1547}$. The is so because *a* is some arbitrary integer.

Comment