A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 2EE

Bookmark

Show all steps: ON

Problem

Prove part:

If $p > 2$ is a prime and $a \neq$ (mod p), then

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

Step-by-step solution

Step 1 of 3

Consider any arbitrary odd prime number p, that is, $p > 2$. Suppose that $a \not\equiv 0 \pmod{p}$.

Objective is to prove that

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}.$$

Since $a \not\equiv 0 \pmod{p}$, it show that there is no common factor between a and p. That is, $\gcd(a, p) = 1$. By Fermat's theorem,

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

or

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Comment

Step 2 of 3

Note that, $a^{p-1} - 1$ can be factorise in the following way:

$$a^{p-1} - 1 = \left(a^{(p-1)/2} + 1\right)\left(a^{(p-1)/2} - 1\right),$$

by using the formula $(a^2 - b^2) = (a+b)(a-b)$.

So,

$$(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) \equiv 0 \pmod{p}.$$

It implies that, either $a^{(p-1)/2} + 1 \equiv 0 \pmod{p}$, or $a^{(p-1)/2} - 1 \equiv 0 \pmod{p}$. That is, either $a^{(p-1)/2} \equiv -1 \pmod{p}$, or $a^{(p-1)/2} \equiv +1 \pmod{p}$.

Comment

Step 3 of 3

Hence, if $a \not\equiv 0 \pmod{p}$ then $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

Comment