A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 1EE

Bookmark

Show all steps: ON

Problem

If *p* is a prime, find *ϕ*(*p*). Use this to deduce Fermat's theorem from Euler's theorem.

Step-by-step solution

Step 1 of 2

Consider any arbitrary prime number *p*. Objective is to find $\phi(p)$. Also deduce Fermat's theorem from Euler's theorem.

If *p* is any prime, then the only divisors of *p* will be 1 and *p* itself. So, the following numbers, that are less than *p*,

$1, 2, 3, \ldots, p-1$

will be relatively prime to *p*.

Thus, by the definition of Euler phi function, $\phi(p) = p-1$.

Comment

Step 2 of 2

If $\gcd(a, n) = 1$, then Euler's theorem states that

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

Suppose that *n* is some arbitrary prime number *p*. Then $\gcd(a, p) = 1$. And by Euler's theorem, it implies that

$a^{\phi(p)} \equiv 1(\bmod p)$.

Use $\phi(p) = p-1$ and get,

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

which is the statement of Fermat's theorem.

Comment