A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 7EE   Bookmark   Show all steps: ON

Problem

Generalize the result of part 6 to *n* distinct primes, $p_1 \ldots, p_n$. (State your result, but do not prove it.)

Step-by-step solution

Step 1 of 2

(a)

Consider any two distinct prime numbers *p* and *q*. Suppose $(p-1) \mid m$ and $(q-1) \mid m$. Then $a^m \equiv 1 (\bmod pq)$, where $p \nmid a$ and $q \nmid a$.

Objective is to generalize the above statement for *n* distinct primes, $p_1, p_2, \ldots, p_n$.

Consider the *n* distinct primes, $p_1, p_2, \ldots, p_n$, that is, all are relatively primes. Suppose that $(p_1 - 1) \mid m, (p_2 - 1) \mid m, \ldots, (p_n - 1) \mid m$.

Then

$$a^m \equiv 1 (\bmod p_1 p_2 \ldots p_n),$$

provided $p_1 \nmid a, p_2 \nmid a, \ldots, p_n \nmid a$.

Comment

Step 2 of 2

(b)

If $(p-1) \mid m$ and $(q-1) \mid m$. Then $a^{m+1} \equiv a (\bmod pq)$ for integers *a*. Objective is to generalize the above statement for *n* distinct primes, $p_1, p_2, \ldots, p_n$.

Consider the *n* distinct primes, $p_1, p_2, \ldots, p_n$. Suppose that

$(p_1 - 1) \mid m, (p_2 - 1) \mid m, \ldots, (p_n - 1) \mid m$.

Then

$a^{m+1} \equiv a \pmod{p_1 p_2 \ldots p_n}$,

for all integers *a*.

Comment