Problem

Prove Fermat's little theorem, which is given in Theorem 10.6. (Hint: Consider the sequence a_1, a_2, ... What must happen, and how?)

THEOREM 10.6

If p is prime and $a \in \mathcal{Z}_p^+$, then $a^{p-1} \equiv 1 \pmod{p}$.

Step-by-step solution

Step 1 of 1

Statement: if p be a prime and $a \in Z^+{}_p$ then $a^{p-1} \equiv 1(\bmod p)$. Here $Z^+{}_p$ is defined as $Z^+{}_p = \{1,\ldots,p-1\}$ and (p,a) is co-prime.

Proof: consider the following first $p-1$ positive multiple of a.

$a, 2a, 3a, \ldots, (p-1)a$.

• As the **little Fermat's theorem** states " (p,a) is co-prime (that is, p is not exactly divisible by a)". Suppose xa and ya are taken in such a way that, the modulo p of xa and ya are equal.

• Now, it can be said that $\mathbf{x} = \mathbf{s}(\bmod p)$. So the $p-1$ multiples by a above are non-zero and distinct; that is, they must be congruent to $a, 2a, 3a, \ldots, (p-1)a$ in the same order. Now, multiply **all these congruence together** and which gives:

$a, 2a, 3a, \ldots, (p-1)a = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)(\bmod p)$

$a^{p-1}(p-1)! = (p-1)!(\bmod p)$

• Now, dividing each side by $(p-1)!$ in the above equality

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

It is also known as a little Fermat's theorem and sometimes it can also be represented as

$a^p = a(\bmod p)$.

Comment