Written by: Matthew Park

Number Theory

Proving Fermat's Theorem

Fermat's Theorem: Given that p is a prime number and the greatest common divisor of (a, p) is 1, it follows that

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

Introduction

Understanding Fermat's theorem opens up understanding to other number theory concepts, like Euler's formula and Euler's theorem.

Proof

To start, this **lemma** must be proved:

If $(a, m) = 1$, then the least residues of

- $a,\ 2a,\ 3a,\ ...,\ (m-1)a$

  are

- $1,\ 2,\ 3, ...,\ m-1$.

__Note:__

Since none of the $(m-1)$ numbers in the first bullet point are congruent to $0\ (mod\ m)$, then they must be congruent $(mod\ m)$ to one of the numbers in the second list.

If we can show that none of the numbers in the first list are congruent to each other, then the elements of the first list map one-to-one with elements in the second list, thus proving the lemma.

__Proof:__

Let $r,\ s$ be least residues of m. Suppose that two of the integers in the first list are congruent.

Then, $ra \equiv sa\ (mod\ m)$. a can be divided out of both sides of the congruency.

Then, $r \equiv s\ (mod\ m)$. Since r, s are less than m, then $r = s$.

Thus, no number in the first list is congruent to another and the lemma is true. ◊

__Fermat's Theorem Proof:__

We take the lemma from above and apply it using $(a, p) = 1$, creating the two lists:

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

  and

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

If we take the products of all elements in each list, the products are congruent to one another. This looks like:

$$a * 2a * ... * (p-1)a \equiv 1 * 2 * ... * (p-1)\ (mod\ p)$$

This can be simplified to:

$$(p-1)!a^{p-1} \equiv (p-1)!\ (mod\ p).$$

$(p-1)!$ can be divided out of both sides of the congruence, simplifying to $a^{p-1} \equiv 1\ (mod\ p)$. ◊

Corollaries

It follows from Fermat's theorem that if p is prime, then $a^p \equiv a\ (mod\ p)$ for all a.

__Proof:__

Case 1: If $(a, p) = 1$, then from Fermat's theorem:

$$a * a^{p-1} \equiv a * 1\ (mod\ p) \text{ or } a^p \equiv a\ (mod\ p).\ ◊$$

Case 2: If $(a, p) = p$, then p divides a, and $a\ (mod\ p) \equiv 0$. Thus, $a^p \equiv 0\ (mod\ p)$ and $0 \equiv 0\ (mod\ p)$. ◊

There are no other cases beyond these two.