Fermat's Theorem

Lemma : (6.1)

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

$$a, \quad 2a, \quad 3a, \quad \dots, \quad (m-1)\,a \mod m$$

are given by

$$1, \quad 2, \quad 3, \quad \dots, \quad m-1$$

in some order

Proof. Note that none of the $m-1$ numbers are congruent to $0 \mod m$

$$a, \quad 2a, \quad 3a, \quad \dots, \quad (m-1)\,a \mod m$$

Hence, each of them is congruent $(\mod m)$ to one of the numbers in

$$1, \quad 2, \quad 3, \quad \dots, \quad m-1$$

Suppose that two of the integers are congruent modulo m

$$ra \equiv sa \mod m$$

Since $(a, n) = 1$, Theorem 4.4 gives us that

$$r \equiv s \mod m$$

Therefore, since r and s are least residues, it follows that $r = s$ $\square$

Theorem : Fermat's Theorem (Little Theorem)

If p is a prime, and $(a, p) = 1$, then

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

Proof. Lemma 6.1 says that if $(a, p) = 1$, then the least residues of

$$a, \quad 2a, \quad 3a, \quad \dots, \quad (p-1)\,a \mod p$$

are a permutation of the set

$$1, \quad 2, \quad 3, \quad \dots, \quad p-1$$

Hence, their products are congruent modulo p

$$a \times 2a \times 3a \times \cdots \times (p-1)\,a \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \mod p$$
$$a^{p-1}\,(p-1)! \equiv (p-1)! \mod p$$

Since p and $(p-1)!$ are relatively prime, the last congruence gives

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

$\square$

Example

Verify that $3^{16} \equiv 1 \mod 17$.

Note that we have the following components of 3^{16}

$$\begin{aligned} 3^3 &\equiv 27 \equiv 10 \mod 17 \\ 3^6 &\equiv \left(3^3\right)^2 \equiv 100 \equiv -2 \mod 17 \\ 3^{12} &\equiv \left(3^6\right)^2 \equiv 4 \mod 17 \end{aligned}$$

Therefore, for the second congruence, we have that

$$\begin{aligned} 3^{16} &\equiv 3^{12} \cdot 3^3 \cdot 3 \\ &\equiv 4 \cdot 10 \cdot 3 \\ &\equiv 1 \mod 17 \end{aligned}$$

Multiplicative Modular Inverses, denoted by a', $\bar{a}$ modulo m, is one such that

$$a \cdot a' \equiv 1 \mod m$$

In general, 1 and $(p-1)$ are there own inverses modulo p

Example

Find all multiplicative modular inverses modulo 7.

A table showing all a and their respective a' is shown below

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Example

Find all multiplicative modular inverses modulo 6.

A table showing all a and their respective a' is shown below

a	1	2	3	4	5
a'	1	DNE	DNE	DNE	5