Euler's Theorem

Fermat's Theorem states that if p is prime, then

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

Question: If $(a, m) = 1$, is there a number t such that:

$$a^t \equiv 1 \mod m$$

Let's look at some tables of powers of a modulo m, where $(a, m) = 1$.

$m = 9$

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	8	7	5	1
4	7	1	4	7	1
5	7	8	4	2	1
7	4	1	8	4	1
8	1	8	1	8	1

$m = 6$

a	a^2
1	1
5	1

$m = 10$

a	a^2	a^3	a^4
1	1	1	1
3	9	7	1
7	9	3	1
9	1	9	1

Definition : Euler's ϕ Function / Euler's Totient Function

If m is a positive integer, let $\phi(m)$ denote the number of positive integers less than or equal to m and relatively prime to m.

Lemma : (9.1)

If $(a, m) = 1$ and $r_1, r_2, \ldots, r_{\phi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues modulo m of

$$ar_1, \quad ar_2, \quad \ldots, \quad ar_{\phi(m)}$$

are a permutation of

$$r_1, \quad r_2, \ldots, \quad r_{\phi(m)}$$

Proof. To show they are all different, suppose that for some $1 \leq i, j \leq \phi(m)$,

$$ar_i \equiv ar_j \mod m$$

Since $(a, m) = 1$, we can cancel a from both sides of the congruence

$$r_i \equiv r_j \mod m$$

Since r_i and r_j are the least residues modulo m, it follows that $r_i = r_j$.

To prove that all the numbers are relatively prime to m, suppose that p is a prime common divisor of ar_i and m for some $1 \leq i \leq \phi(m)$. Since p is prime, either $p \mid a$ or $p \mid r_i$. Thus, either p is a common divisor of a and m, or of r_i and m. But $(a, m = 1)$ and $(r_i, m) = 1$, so both cases are impossible. □

Example

Verify Lemma 9.1 if $m = 14$ and $a = 5$.

---

x	$5x$	$5x \mod 14$
1	5	5
3	15	1
5	25	11
9	45	3
11	55	13
13	65	9

Theorem : (9.1) / Euler's Theorem

If $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \mod m$$

Proof. From Lemma 9.1, we know that

$$r_1 r_2 \ldots r_{\phi(m)} \equiv (ar_1)(ar_2)\ldots\left(ar_{\phi(m)}\right) \mod m$$

$$r_1 r_2 \ldots r_{\phi(m)} \equiv a^{\phi(m)} r_1 r_2 \ldots r_{\phi(m)} \mod m$$

Since $(r_i, m) = 1$ for all $1 \leq i \leq \phi(m)$, we can cancel $r_1 r_2, \ldots r_{\phi(m)}$

$$1 \equiv a^{\phi(m)} \mod m$$

□

How do we find $\phi(m)$? We will see later when we show that $\phi(m)$ is multiplicative.

Recall: Perfect numbers are n such that $\sigma(n) = 2n$. Even perfect numbers can be described as $n = 2^{p-1} \cdot (2^p - 1)$, where $2^p - 1$ is prime. We do not know if any odd perfect numbers exist, and numbers up to 10^{2200} have been checked. For even perfect numbers, we do not know if there are infinitely many Mersenne Primes, (primes of the form $2^p - 1$ where p is prime). It was originally conjectured that the only Mersenne Primes corresponded to the following values for p:

$$2, 3, 5, 7, 13, 17, 31, 67, 127, 257$$

In this list, 19, 61, 87, and 107 were missed, and 67 and 257 should not have been included. The largest Mersenne Prime currently known is:

$$2^{136279841-1} \qquad \text{This has 41,000,000+ digits}$$