Orders of Elements

In Euler's Theorem, we saw that if $(a, m) = 1$, then there is a positive integer $\phi(m)$ such that

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

If $(a, m) = 1$, then the least residues are all relatively prime elements to m.

$$a, \qquad a^2, \qquad a^3, \qquad \ldots$$

There are $\phi(m)$ least residues $\mod m$ that are relatively prime to m and infinitely many powers of a. It follows that there are positive integers j and k with $j \neq k$ such that

$$a^j \equiv a^k \mod m$$

The smaller power of a in the last congruence may be canceled.

$$a^{j-k} \equiv 1 \mod m \qquad \text{or} \qquad a^{k-j} \equiv 1 \mod m$$

Thus, if $(a, m) = 1$, then there is a positive integer t such that

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

Notice that for any positive integer k

$$\begin{aligned} a^{t+k\cdot\phi(m)} &\equiv a^t \left(a^k\right)^{\phi(m)} \mod m \\ &\equiv a^t \mod m \\ &\equiv 1 \mod m \end{aligned}$$

Definition : Order

The order of a modulo m is the smallest positive integer t such that

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

Example

Find the orders of the least residues modulo 11.

---

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

The residue 1 has order 1, the residue 10 has order 2, the residues, 3, 4, 5, and 9 have order 5, the residues 2, 6, 7, and 8 have order 10.

Theorem : (10.1)

Suppose that $(a, m) = 1$ and a has order t modulo m. Then, $a^n \equiv 1 \mod m$ if and only if n is a multiple of t.

Proof. Suppose that $n = tq$ for some integer q. Then

$$\begin{aligned} a^n &\equiv a^{tq} \mod m \\ &\equiv \left(a^t\right)^q \mod m \\ &\equiv 1^q \mod m \\ &\equiv 1 \mod m \end{aligned}$$

Conversely, suppose that $a^n \equiv 1 \mod m$. Since t is the smallest positive integer such that $a^t \equiv 1 \mod m$, we have that $n \geq t$. We can divide n by t to get $n = tq + r$ with $q \geq 1$ and $0 \leq r < t$. Therefore, we have that

$$\begin{aligned} 1 &\equiv a^n \mod m \\ &\equiv a^{tq+r} \mod m \\ &\equiv \left(a^t\right)^q a^r \mod m \\ &\equiv a^r \mod m \end{aligned}$$

Since t is the smallest positive integer such that $a^t \equiv 1 \mod m$, $a^r \equiv 1 \mod m$ with $0 \leq r < t$ is only possible $r = 0$. Thus $n = tq$. □

Theorem : (10.2)

If $(a, m) = 1$ and a has order t modulo m, then $t \mid \phi(m)$.

Proof. From Euler's Theorem, we know that

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

From Theorem 10.1, $\phi(m)$ is a multiple of t, therefore

$$t \mid \phi(m)$$

□

Example

What order can an integer have modulo 9? Find an example of each possible order.

By Theorem 10.2, the possible orders are the divisors of $\phi(9) = 6$. Therefore, the possible orders are 1, 2, 3, and 6.

a	Order of a
1	1
8	2
4	3
2	6

Theorem : (10.3)

If p and q are odd primes and $q \mid a^p - 1$, then $q \mid a - 1$ or $q = 2kp + 1$ for some integer k.

Proof. Since $q \mid a^p - 1$, we have that $a^p \equiv 1 \mod q$. Thus, by Theorem 10.1, the order of a modulo q is a divisor of p. That is, a has order 1 or order p. If the order of a is 1, then $a^1 \equiv 1 \mod q$, therefore $q \mid a - 1$.

If the order of a if p, then by Theorem 10.2, $p \mid \phi(q)$. That is, $p \mid (q-1)$. Therefore, $q - 1 = rp$ for some integer r. Since p and q are odd, r must be even, thus $q = 2kp + 1$ for some k. □

Corollary : (10.1)

Any divisor of $2^p - 1$ is of the form $2kp + 1$.

Example

What is the smallest possible prime divisor of $2^{19} - 1$?

By Corollary 10.1, the divisors are of the form $38k + 1$.

k	$38k + 1$	Prime
1	39	No
2	77	No
3	115	No
4	153	No
5	191	Yes

Therefore, the smallest possible prime divisor is 191.