The Order of an Integer and Primitive Roots

Let $n \in \mathbb{Z}^+$ and let a be relatively prime to n. Then, by Euler's theorem,

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

4-12-24

Therefore, the equation

$$a^x \equiv 1 \pmod{n}$$

always has a positive solution. By the well-ordering property, there exists a least positive integer that satisfy this congruence.

<u>Definition:</u> Let $a, n \in \mathbb{Z}$ with $a \neq 0$, $n > 0$ and $\gcd(a, n) = 1$. Then, the least positive integer x such that

$$a^x \equiv 1 \pmod{n}$$

is called the order of a modulo n and it is denoted by $\operatorname{ord}_n a$.

<u>ex</u>: Let's find the order of 2 modulo 7. We proceed as follows.

$$2^1 \equiv 2 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7}$$

$\therefore \operatorname{ord}_7 2 = 3$

<u>ex</u>: Let's find $\operatorname{ord}_7 3$.

$3^1 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$,
$3^3 \equiv 6 \pmod 7$, $3^4 \equiv 4 \pmod 7$,
$3^5 \equiv 5 \pmod 7$, $3^6 \equiv 1 \pmod 7$.

$\therefore \operatorname{ord}_7 3 = 6$.

<u>Theorem 9.1</u>: Let $a, n \in \mathbb{Z}$, $a \neq 0$, $n > 0$ and $\gcd(a, n) = 1$. Then, for $x \in \mathbb{Z}^+$,

$$a^x \equiv 1 \pmod n \iff \operatorname{ord}_n a \mid x.$$

Proof: Suppose $\operatorname{ord}_n a \mid x$.

Then $x = k \cdot \operatorname{ord}_n a$ for some $k \in \mathbb{Z}^+$.

$\therefore a^x = a^{k \cdot \operatorname{ord}_n a} = (a^{\operatorname{ord}_n a})^k \equiv 1 \pmod n$

Next, suppose $a^x \equiv 1 \pmod n$ with $x \in \mathbb{Z}^+$.

By the division algorithm,

$$x = q \cdot \operatorname{ord}_n a + r \text{ with } 0 \leq r < \operatorname{ord}_n a$$

Then,

$$a^x = a^{q \cdot \operatorname{ord}_n a + r}$$

$$= \left(a^{\mathrm{ord}_n a}\right)^q \cdot a^r$$

$$\equiv a^r \pmod{n}$$

$$\therefore \quad 1 \equiv a^r \pmod{n} \quad (\because a^x \equiv 1 \pmod{n})$$

$$\therefore \quad a^r \equiv 1 \pmod{n}$$

This is impossible unless $r=0$, because $0 \le r < \mathrm{ord}_n a$ and $\mathrm{ord}_n a$ is the least positive integer that satisfies the equation

$$a^x \equiv 1 \pmod{n}.$$

$\therefore r = 0$

$\therefore x = q \cdot \mathrm{ord}_n a$

$\therefore \mathrm{ord}_n a \mid x$

and the theorem follows.

ex: Determine whether $x = 15$ and $x = 24$ are solutions of $3^x \equiv 1 \pmod{7}$.

We saw above that $\mathrm{ord}_7 3 = 6$.

$6 \nmid 15$, so $x = 15$ is not a solution of $3^x \equiv 1 \pmod{7}$

$6 \mid 24$, so $x = 24$ is a solution of $3^x \equiv 1 \pmod{7}$

Corollary 9.1.1: Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ be such that $\gcd(a,n) = 1$. Then, $\operatorname{ord}_n a \mid \varphi(n)$.

Proof: By Euler's theorem, we have

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Then, by Theorem 9.1, $\operatorname{ord}_n a \mid \varphi(n)$.

ex: Let's find $\operatorname{ord}_9 5$ using the above corollary.
We know,

$$\varphi(9) = 6.$$

The divisors of 6 are 1, 2, 3 and 6.
$\therefore$ these are the only possible values for $\operatorname{ord}_9 5$.
Check each of them.

$$5^1 \equiv 5 \pmod{9}$$
$$5^2 \equiv 7 \pmod{9}$$
$$5^3 \equiv 8 \pmod{9}$$
$$5^6 \equiv (5^3)^2 \equiv 8^2 \equiv 1 \pmod{9}$$

$$\therefore \operatorname{ord}_9 5 = 6.$$

Theorem 9.2: Let $a, n \in \mathbb{Z}$, $n > 0$ and $\gcd(a,n) = 1$. Then, for non-negative integers i and j,

$$a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{\operatorname{ord}_n a}.$$

Proof: Suppose $i \equiv j \pmod{\text{ord}_n a}$.

without loss of generality, assume $i \geq j \geq 0$.

Then,

$$i = j + k \cdot \text{ord}_n a$$

$$\begin{aligned} \therefore \quad a^i &= a^{j + k \cdot \text{ord}_n a} \\ &= a^j \cdot (a^{\text{ord}_n a})^k \\ &\equiv a^j \cdot 1^k \pmod{n} \\ &\equiv a^j \pmod{n} \end{aligned}$$

Conversely, suppose $a^i \equiv a^j \pmod{n}$.

Without loss of generality, assume $i \geq j \geq 0$.

We've $a^j \equiv a^i \pmod{n}$

$$\therefore a^j \equiv a^j \cdot a^{i-j} \pmod{n}$$

Now, since $\gcd(a,n) = 1$, we can easily prove that $\gcd(a^j, n) = 1$ (prove it!).

$\therefore$ we can cancel a^j in the congruence

$$a^j \equiv a^j a^{i-j} \pmod{n}$$

and hence

$$1 \equiv a^{i-j} \pmod{n}$$

or,

$$a^{i-j} \equiv 1 \pmod{n}.$$

Then, by Theorem 9.1, $\text{ord}_n a \mid (i-j)$.

$$\therefore \quad i \equiv j \pmod{\text{ord}_n a}$$

ex: Let $n=14$ and $a=3$.

Then, $\varphi(14)=6$.

$\therefore$ possible values for $\mathrm{ord}_{14}3$ are 1, 2, 3 and 6. It is easy to see that

$$\mathrm{ord}_{14}3 = 6.$$

Hence, $3^5 \equiv 3^{11} \pmod 6$ as $6 \mid (11-5)$

but $3^9 \not\equiv 3^{20} \pmod 6$ as $6 \nmid (20-9)$.

Definition: Let $r, n \in \mathbb{Z}$ with $n>0$ and $\gcd(r,n)=1$. If $\mathrm{ord}_n r = \varphi(n)$, then r is called a primitive root modulo n, or a primitive root of n, and we say that n has a primitive root.

ex: We know $\varphi(7)=6$. Also, we saw above that $\mathrm{ord}_7 3 = 6$. Hence, 3 is a primitive root of 7. Also, it can be easily seen that $\mathrm{Ord}_7 5 = 6$, so 5 is also a primitive root of 7.

ex: 8 does not have a primitive root.

We know $\varphi(8)=4$.

$\therefore$ possible orders are 1, 2 and 4.

Let's find the order of each a such

that $\gcd(9,8)=1$.

$\operatorname{ord}_8 1 = 1 \quad (1^1 \equiv 1 \pmod 8)$

$\operatorname{ord}_8 3 = 2 \quad (3^2 \equiv 1 \pmod 8)$

$\operatorname{ord}_8 5 = 2 \quad (5^2 \equiv 1 \pmod 8)$

$\operatorname{ord}_8 7 = 2 \quad (7^2 \equiv 1 \pmod 8)$

Hence, no integer relatively prime to 8 has order $\varphi(8)=4$.

It can be shown that 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19, 22, 23, 25, 26, 27 and 29 have primitive roots whereas 8, 12, 15, 16, 20, 21, 24, 28 and 30 do not.

It can be proved that $n \in \mathbb{Z}^+$ has a primitive root if and only if n is equal to

$$2,\ 4,\ p^t \text{ or } 2p^t \text{ where } p \text{ is an odd prime.}$$

This will be proved later.

<u>Theorem 9.3:</u> Let $r, n \in \mathbb{Z}$ with $n>0$, $\gcd(r,n)=1$ and r is a primitive root of n. Then, the integers $r, r^2, \ldots, r^{\varphi(n)}$ form a reduced residue system modulo n.

Proof: We show that $\gcd(r^k, n) = 1$ and that $r^i \not\equiv r^j \pmod{n}$ for $1 \le i, j \le \varphi(n)$.

It is easy to see that $\gcd(r^k, n) = 1$ (as discussed in the proof of Theorem 9.2). Therefore, each of $r, r^2, \ldots, r^{\varphi(n)}$ is relatively prime to n.

Next, assume

$$r^i \equiv r^j \pmod{n}.$$

By Theorem 9.2, $i \equiv j \pmod{\operatorname{ord}_n r}$

But r is a primitive root of n, so

$$\operatorname{ord}_n r = \varphi(n).$$

Therefore,

$$i \equiv j \pmod{\varphi(n)}$$

Since $0 \le i, j \le \varphi(n)$, it follows that $i - j = 0$, i.e., $i = j$.

Hence the result.

<u>ex:</u> It can be shown that $\varphi(9) = 6$ and that $\operatorname{ord}_9 2 = 6$. Therefore, 2 is a primitive root of 9.

$\therefore$ $2, 2^2, 2^3, 2^4, 2^5, 2^6$ form a reduced residue system modulo 9. They are

$$2, 4, 8, 7, 5 \text{ and } 1$$

When an integer possesses a primitive root, it usually has many primitive roots. We first prove the following theorem.

<u>Theorem 9.4</u>: If $\text{ord}_n a = t$ and if u is a positive integer, then

$$\text{ord}_n(a^u) = \frac{t}{\gcd(t,u)}$$

Proof: Let $v = \gcd(t,u)$, $t = t_1 v$ and $u = u_1 v$.

Then, by Theorem 3.6, $\gcd(t_1, u_1) = 1$.

Because $t_1 = \dfrac{t}{\gcd(t,u)}$, we want to show that $\text{ord}_n(a^u) = t_1$.

To do this, we'll show that

$$(a^u)^{t_1} \equiv 1 \pmod{n}$$

and that if $(a^u)^s \equiv 1 \pmod{n}$ then $t_1 \mid s$.

First,

$$(a^u)^{t_1} = (a^{u_1 v})^{t_1} = (a^{t_1 v})^{u_1} = (a^t)^{u_1}$$

$$\equiv 1^{u_1} \equiv 1 \pmod{n} \quad (\because \text{ord}_n a = t)$$

Next, if $(a^u)^s \equiv 1 \pmod{n}$

then $a^{us} \equiv 1 \pmod{n}$

$$\Rightarrow t \mid us$$
$$\Rightarrow t_1 v \mid u_1 v s$$
$$\Rightarrow t_1 \mid u_1 s$$
$$\Rightarrow t_1 \mid s \quad (\because \gcd(t_1, u_1) = 1)$$

$$\therefore \operatorname{ord}_n(a^u) = t / \gcd(t, u).$$

<u>ex</u>: We've shown before that $\operatorname{ord}_7 3 = 6$.

$$\therefore \operatorname{ord}_7 3^4 = \frac{6}{\gcd(6,4)} = \frac{6}{2} = 3.$$

It can be verified directly too.

$$3^4 = 81 \equiv 4 \pmod{7}$$
$$\therefore (3^4)^1 \equiv 4 \pmod{7}$$
$$(3^4)^2 \equiv 2 \pmod{7}$$
$$(3^4)^3 \equiv 4 \cdot 2 \equiv 1 \pmod{7}$$

<u>Corollary 9.4.1</u>: Let r be a primitive root of n, where $n > 1$. Then,

r^u is a primitive root of n

$$\Longleftrightarrow$$

$$\gcd(u, \varphi(n)) = 1$$

Proof: By Theorem 9.4,

$$\operatorname{ord}_n(r^u) = \frac{\operatorname{ord}_n r}{\gcd(\operatorname{ord}_n r, u)}$$

$$= \frac{\varphi(n)}{\gcd(\varphi(n), u)}$$

Now, r^u is a primitive root of n

$$\Longleftrightarrow$$

$$\operatorname{ord}_n(r^u) = \varphi(n)$$

$$\Longleftrightarrow$$

$$\frac{\varphi(n)}{\gcd(\varphi(n), u)} = \varphi(n)$$

$$\Longleftrightarrow$$

$$\gcd(\varphi(n), u) = 1$$

<u>Theorem 9.5</u>: If $n \in \mathbb{Z}^+$ has a primitive root, then it has a total of $\varphi(\varphi(n))$ incongruent primitive roots.

Proof: Let r be a primitive root of n. Then, by Theorem 9.3,

$$r, r^2, \ldots, r^{\varphi(n)}$$

form a reduced residue system modulo n. By Corollary 9.4.1, r^u is a primitive root of n if and only if $\gcd(u, \varphi(n)) = 1$. From the integer $1, 2, 3, \ldots, \varphi(n)$, the number of integers relatively prime to $\varphi(n)$ is $\varphi(\varphi(n))$ and hence the theorem follows.

<u>ex</u>: Let $n = 11$. It can be shown that

$$\operatorname{ord}_{11} 2 = 10 = \varphi(11)$$

so 2 is a primitive root of 11.
Then, by Theorem 9.5, there are $\varphi(\varphi(11)) = 4$ incongruent primitive roots. These 4 primitive roots come from

$$2, 2^2, 2^3, \ldots, 2^{10}.$$

By the proof of Theorem 9.5, these primitive roots are the least non-negative residues of $2^1, 2^3, 2^7$ and 2^9, because 1, 3, 5 and 7 are the integers relatively prime to 10.
The least non-negative residues of $2^1, 2^3, 2^7$ and 2^9 are 2, 8, 7 and 6 respectively.
Hence, 2, 6, 7, 8 form a complete set of incongruent primitive roots modulo 11.