Order of an Integer Modulo n

Munir Uz Zaman

Date: February 26, 2022

§1 Orders

Definition 1.1. The order of an integer a modulo n where a and n are coprime integers is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$

We will use the notation $\operatorname{ord}_n a$ to denote the order of a modulo n. For example 2 has order 3 modulo 7. Therefore we can write $\operatorname{ord}_7 2 = 3$.

> **Remark 1.2.** If $\gcd(a, n) \neq 1$ then there does not exist any positive integer k such that $a^k \equiv 1 \pmod{n}$, because the linear congruence $ax \equiv 1 \pmod{n}$ does not have a solution when a and n are not coprime.
> Therefore whenever we are talking about the order of a modulo n, it should be implicitly assumed that a and n are coprime integers.

Theorem 1.3 (Fundatmental Theorem of Orders)

If a is an integer then

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

Proof: TODO

♣

Corollary 1.3.1

If a is an integer then

$$\operatorname{ord}_n a \mid \phi(n)$$

Theorem 1.4

If p is a prime then there exists an x such that

$$p \mid x^2 + 1$$

if and only if $p = 2$ or $p \equiv 1 \pmod{4}$

Proof: We are going to first prove that if $p > 2$ then

$$p \mid x^2 + 1 \implies 4 \mid p - 1$$

Now

$$x^2 \equiv -1 \pmod{p} \implies x^4 \equiv 1 \pmod{p}$$

Therefore $\operatorname{ord}_p x \mid 4 \implies \operatorname{ord}_p x \in \{1, 2, 4\}$. Clearly $\operatorname{ord}_p x$ is not 1 or 2 (why?). Thus $\operatorname{ord}_p x = 4$. Hence

$$\operatorname{ord}_p x \mid \phi(p) \implies 4 \mid p - 1$$

Now we will prove the converse: if $p > 2$ and $p \equiv 1 \pmod{4}$ then there exists an x such that $p \mid x^2 + 1$. For this we take

$$x = \left(\frac{p-1}{2}\right)!$$

Now

$$\begin{aligned}
x &\equiv \left(\frac{p-1}{2}\right)! \pmod{p} \\
&\equiv \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-2}{2}\right) \cdots 2 \cdot 1 \pmod{p} \\
&\equiv \left(-\frac{p+1}{2}\right) \cdot \left(-\frac{p+2}{2}\right) \cdots -(p-2) \cdot -(p-1) \pmod{p} \\
&\equiv (-1)^{\frac{p-1}{2}} \left(\frac{p+1}{2}\right) \cdot \left(\frac{p+2}{2}\right) \cdots (p-2) \cdot (p-1) \pmod{p}
\end{aligned}$$

Therefore

$$\begin{aligned}
x^2 &= \left(\frac{p-1}{2}\right)! \times (-1)^{\frac{p-1}{2}} \left(\frac{p+1}{2}\right) \cdot \left(\frac{p+2}{2}\right) \cdots (p-2) \cdot (p-1) \pmod{p} \\
\implies x^2 &= (-1)^{\frac{p-1}{2}} (p-1)! \pmod{p}
\end{aligned}$$

Using Wilson's Theorem we have

$$x^2 \equiv (-1)^{\frac{p-1}{2}+1} \pmod{p} \implies x^2 \equiv -1 \pmod{p} \implies p \mid x^2 + 1$$

♣

Lemma 1.5 (GCD Trick)

If $a^m \equiv 1 \pmod{N}$ and $a^n \equiv 1 \pmod{N}$ then

$$a^{\gcd(m,n)} \equiv 1 \pmod{N}$$

Proof: This is just the famous fact that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ phrased using modular arithmetic (how?).

♣

Example 1.6

Find all n such that n divides $2^n - 1$.

Solution: Let p be the smallest prime factor of n. Now

$$\begin{matrix} 2^n \equiv 1 \pmod{p} \\ 2^{p-1} \equiv 1 \pmod{p} \end{matrix} \implies 2^{\gcd(p-1,n)} \equiv 1 \pmod{p}$$

Since p is the smallest prime divisor of n and $\gcd(p-1, n) \mid n$, we must have $\gcd(p-1, n) = 1$ (why?). Hence

$$p \mid 2^1 - 1 \implies p \mid 1$$

which is impossible. Therefore there does not exist such an n.

♣

Theorem 1.7

If a is an integer such that $\operatorname{ord}_n a = k$, then

$$a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{k}$$

Corollary 1.7.1

If a has order k modulo n, then the integers $a, a^2, \cdots, a^k$ are incongruent modulo n.

§2 Primitive Roots

Definition 2.1. If the order of g modulo n is $\phi(n)$, then g is called a **primitive root** of n

If n is not a prime, then it is possible that n does not have any primitive root. But for all prime there exists a primitive root.

Theorem 2.2

If p is a prime then the primitive root of p exists.

Lemma 2.3

Given a primitive root g, each nonzero residue modulo p can be expressed uniquely as g^α where $\alpha \in \{1, 2, \cdots, p-1\}$.