

# Order of an Integer Modulo $n$

Munir Uz Zaman

Date: March 2, 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  $\text{ord}_n a$  to denote the order of  $a$  modulo  $n$ . For example 2 has order 3 modulo 7. Therefore we can write  $\text{ord}_7 2 = 3$ .

**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 (Fundamental Theorem of Orders)

If  $a$  is an integer then

$$a^k \equiv 1 \pmod{n} \iff \text{ord}_n(a) \mid k$$

**Proof:** For the sake of contradiction, let us assume that  $\text{ord}_n(a) \nmid k$  and

$$k = q \times \text{ord}_n(a) + r$$

where  $0 < r < \text{ord}_n(a)$ . Now

$$\begin{aligned} a^k \equiv 1 \pmod{n} &\implies a^{q \times \text{ord}_n(a)} \times a^r \equiv 1 \pmod{n} \\ &\implies a^r \equiv 1 \pmod{n} \end{aligned}$$

This contradicts the fact that  $\text{ord}_n(a) = x$  is the smallest positive integer such that

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

Therefore  $\text{ord}_n(a) \mid k$ . The converse is trivial!



### Corollary 1.3.1

If  $a$  is an integer then

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

**Proof:**

$$a^{\phi(n)} \equiv 1 \pmod{n} \implies \text{ord}_n(a) \mid \phi(n)$$



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

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

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?).



**Lemma 1.6**

If  $p > 2$  is a prime and  $p \mid x^{2^n} + 1$  where  $n$  is a positive integer, then  $p \equiv 1 \pmod{2^{n+1}}$ .

**Proof:**

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

Therefore  $\text{ord}_p x \mid 2^{n+1}$  which implies  $\text{ord}_p x = 2^t$  where  $1 \leq t \leq n+1$ . If  $t < n+1$  then

$$x^{2^t} \equiv 1 \pmod{p} \implies \left(x^{2^t}\right)^{2^{n-t}} \equiv x^{2^n} \equiv 1 \pmod{p}$$

which contradicts our hypothesis. Therefore  $t = n+1 \implies \text{ord}_p x = 2^{n+1}$ . Hence

$$2^{n+1} \mid p-1 \implies p \equiv 1 \pmod{2^{n+1}}$$



**Remark 1.7.** Why can't  $p = 2$ ? Because if  $p = 2$  then  $1 \equiv -1 \pmod{2}$ .

**Example 1.8**

Find all primes  $p$  and  $q$  such that  $pq \mid 2^p + 2^q$ .

**Solution:** Let us assume that both  $p$  and  $q$  are coprime to 2.

$$\begin{aligned} pq \mid 2^p + 2^q &\implies 2^p + 2^q \equiv 0 \pmod{p} \\ &\implies 2 + 2^q \equiv 0 \pmod{p} \\ &\implies 2(2^{q-1} + 1) \equiv 0 \pmod{p} \\ &\implies 2^{q-1} \equiv -1 \pmod{p} \end{aligned}$$

Likewise  $2^{p-1} \equiv -1 \pmod{q}$ . Suppose  $k$  is the largest integer such that  $2^k \mid p-1$ . That is,  $2^k$  is the largest power of 2 that divides  $p-1$ . Let  $p-1 = 2^k n$ .

$$2^{p-1} \equiv 2^{2^k n} \equiv -1 \pmod{q} \implies 2^{k+1} \mid q-1$$

Therefore  $q-1 = 2^{k+1}m$  where  $m$  is an integer. Now

$$2^{q-1} \equiv 2^{2^{k+1}m} \equiv -1 \pmod{p} \implies 2^{k+2} \mid p-1$$

This contradicts our assumption that  $2^k$  is the largest power of 2 which divides  $p-1$ . Hence both  $p$  and  $q$  cannot be coprime to 2.

Clearly  $p = q = 2$  is a valid solution. Now assume  $q = 2$  and  $p > 2$ .

$$\begin{aligned} 2p \mid 2^p + 4 &\implies p \mid 2^{p-1} + 2 \\ &\implies 2^{p-1} + 2 \equiv 0 \pmod{p} \\ &\implies 3 \equiv 0 \pmod{p} \implies p = 3 \end{aligned}$$

Therefore  $(p, q) = (3, 2), (2, 3)$  are also a valid solutions.

Hence the solutions are  $(2, 2), (3, 2), (2, 3)$ .



**Example 1.9**

Find all positive integers  $m$  and  $n$  such that

$$n \mid 1 + m^{3^n} + m^{2 \cdot 3^n}$$

**Solution:**

$$n \mid 1 + m^{3^n} + m^{2 \cdot 3^n} \implies n \mid m^{3^{n+1}} - 1 \implies m^{3^{n+1}} \equiv 1 \pmod{n}$$

Therefore  $\text{ord}_n(m) \mid 3^{n+1} \implies \text{ord}_n(m) = 3^t$  where  $0 \leq t \leq n+1$ .

If  $t = n+1$  then

$$\text{ord}_n(m) \mid \phi(n) \implies 3^{n+1} \mid \phi(n) \implies 3^{n+1} \leq \phi(n) < n$$

which is impossible.

If  $t < n+1$ , then

$$1 + m^{3^n} + m^{2 \cdot 3^n} \equiv 0 \pmod{n} \implies 3 \equiv 0 \pmod{n} \implies n \in \{1, 3\}$$

If  $n = 1$ , then

$$1 \mid 1 + m^3 + m^6$$

which is true for all positive integer values of  $m$ . If  $n = 3$ , then

$$m^{3^t} \equiv 1 \pmod{3}$$

which is only possible if  $m \equiv 1 \pmod{3}$ . (Why?)

Therefore the solutions are  $(n, m) = (1, k), (3, 3k+1)$ .

**Example 1.10**

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

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

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

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  $n$ .

**Problem 1.11 (China TST 2006)**

Find all positive integers  $a$  and  $n$  such that

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

**Solution:** We are gonna use the same idea as before. Let  $p$  be smallest prime divisor of  $n$ .

$$(a+1)^n \equiv a^n \pmod{p} \implies \left(1 + \frac{1}{a}\right)^n \equiv 1 \pmod{p}$$

Now

$$\begin{aligned} \left(1 + \frac{1}{a}\right)^n &\equiv 1 \pmod{p} \\ \left(1 + \frac{1}{a}\right)^{p-1} &\equiv 1 \pmod{p} \implies \left(1 + \frac{1}{a}\right)^{\gcd(n, p-1)} \equiv 1 \pmod{p} \end{aligned}$$

Since  $\gcd(n, p-1) \mid n$  and  $\gcd(n, p-1) < p$ ,  $\gcd(n, p-1)$  must be 1. Therefore

$$\left(1 + \frac{1}{a}\right) \equiv 1 \pmod{p} \implies a \equiv 1 \pmod{p} \implies a \equiv 1 \pmod{n}$$

Hence

$$2^n \equiv 1 \pmod{n}$$

We've shown earlier that there does not exist any integer  $n$  such that

$$n \mid 2^n - 1$$

Therefore such integers do not exist.



### Theorem 1.12

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

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

### Corollary 1.12.1

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

### Example 1.13

Show that for all  $n$ ,  $3^n - 2^n$  is not divisible by  $n$ .

**Proof:** For the sake of contradiction, assume  $n \mid 3^n - 2^n$ . Let  $p$  be the smallest prime divisor of  $n$ .

$$n \mid 3^n - 2^n \implies p \mid 3^n - 2^n$$

Let  $a$  be an integer such that  $2a \equiv 1 \pmod{p}$ . Now since  $3^n \equiv 2^n \pmod{p}$

$$2a \equiv 1 \pmod{p} \implies (2a)^n \equiv (3a)^n \equiv 1 \pmod{p}$$

Therefore

$$\text{ord}_p(3a) \mid n$$

But since  $\text{ord}_p(3a) < p$  and  $p$  is the smallest prime divisor of  $n$ , we must have  $\text{ord}_p(3a) = 1$ . Thus

$$3a \equiv 1 \pmod{p} \implies a \equiv 0 \pmod{p}$$

This contradicts our assumption that  $2a \equiv 1 \pmod{p}$ . Hence such an integer  $n$  cannot exist.



## §2 Primitive Roots

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

For example, 2 is a primitive root of 5. 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  $g^\alpha$  where  $\alpha \in \{1, 2, \dots, p-1\}$ .

### Lemma 2.4

Let  $p > 2$  be a prime. If  $x$  is an integer, then

$$1^x + 2^x + \dots + (p-1)^x \equiv \begin{cases} -1 & \text{if } (p-1) \mid x \\ 0 & \text{otherwise} \end{cases} \pmod{p}$$

**Proof:** Let  $g$  be a primitive root of  $p$ . If  $(p-1) \mid x$  then

$$1^x + \dots + (p-1)^x \equiv \sum_{\alpha=1}^{p-1} g^{\alpha x} \equiv \sum_{\alpha=1}^{p-1} 1^x \equiv (p-1) \equiv -1 \pmod{p}$$

If  $(p-1) \nmid x$  then

$$1^x + \dots + (p-1)^x \equiv \sum_{\alpha=1}^{p-1} g^{\alpha x} \equiv g^x \left( \frac{g^{(p-1)x} - 1}{g^x - 1} \right) \equiv 0 \pmod{p}$$

