

# 1 Indices, Index Arithmetic, Discrete Logarithms

How can we solve (or even know if solutions exist) something like

$$3^x \equiv 5 \pmod{22}$$

or -how many solutions there might be, or -if the solutions are mod 22 or something else. In pre-calculus with  $3^x \equiv 5$  we can do  $x = \log_3 5$ , but we cannot do that here (yet).

## 1.1 The Order of an Integer & Primitive Roots

---

1. **Introduction:** The process of exponentiation and its inverse (logarithms) is as essential in modular arithmetic as it is in regular math and forms the basis for various encryption techniques. We begin by taking a base  $a$  which is coprime to a modulus  $m$  and looking at the powers of  $a \pmod{m}$ .
2. **Order:** Given a modulus  $m$  and an integer  $a$  with  $\gcd(a, m) = 1$  Euler's Theorem tells us that  $a^{\phi(m)} \equiv 1 \pmod{m}$ . It does not however tell us that  $\phi(m)$  is the lowest power which yields 1. This leads to the following.
  - (a) **Definition:** Suppose  $\gcd(a, m) = 1$  we define the *order* of  $a \pmod{m}$  as the smallest power  $x$  such that  $a^x \equiv 1 \pmod{m}$ . This is denoted  $\text{ord}_m a$ .  
**Note:**  $\text{ord}_m a \leq \phi(m)$   
**Note:** We can say "order of  $a$ " when  $m$  is contextually obvious.  
**Ex.** Let's find  $\text{ord}_{11} 3$ . Well,

$$3^1 \equiv 3 \pmod{11}$$

$$3^2 \equiv 9 \pmod{11}$$

$$3^3 \equiv 5 \pmod{11}$$

$$3^4 \equiv 4 \pmod{11}$$

$$3^5 \equiv 1 \pmod{11}$$

Thus,  $\text{ord}_{11} 3 = 5$ .

**Note:** We can now start to see that the order gives us a pattern under which  $3^x$  will repeat!

- (b) **Theorem:** For  $x \in \mathbb{Z}^+$  we have  $a^x \equiv 1 \pmod{m}$  if and only if  $x \equiv 0 \pmod{\text{ord}_m a}$  if and only if  $\text{ord}_m a \mid x$ .  
**Ex.** We saw  $\text{ord}_{11} 3 = 5$  so  $3^x \equiv 1 \pmod{11}$  if and only if  $x \equiv 0 \pmod{5}$  if and only if  $5 \mid x$ .

*Proof.*

→ Assume  $a^x \equiv 1 \pmod m$ , use the Division Algorithm to write  $x = q(\text{ord}_m a) + r$ . Observe,

$$1 \equiv a^x \equiv \left(a^{\text{ord}_m a}\right)^q a^r \equiv a^r \pmod m$$

Since  $\text{ord}_m a$  is the smallest positive power, we must have  $r = 0$ . Thus,  $x = q\text{ord}_m a$  so  $\text{ord}_m a \mid x$ .

← Assume  $\text{ord}_m a \mid x$ . Then,

$$a^x \equiv a^{k\text{ord}_m a} \equiv \left(a^{\text{ord}_m a}\right)^k \equiv 1^k \equiv 1 \pmod m$$

□

(c) **Corollary:** We have  $\text{ord}_m a \mid \phi(m)$ .

*Proof.* The proof here is obvious because  $a^{\phi(m)} \equiv 1 \pmod m$ . Apply the theorem. □

So to find  $\text{ord}_m a$  try divisors of  $\phi(m)$  only.

**Ex.** To find  $\text{ord}_{11} 2$  we note that  $\phi(11) = 10$ . So we need to check 1, 2, 5 because if it fails for those,  $\text{ord}_{11} 2 = 10$ .

$$2^1 \equiv 2 \not\equiv 1 \pmod{11}$$

$$2^2 \equiv 4 \not\equiv 1 \pmod{11}$$

$$2^5 \equiv 10 \not\equiv 1 \pmod{11}$$

Aha, from this we can see that  $2^{10} \equiv 1 \pmod{11}$  by Euler's Theorem. So  $\text{ord}_{11} 2 = 10$ .

(d) **Theorem:** We have  $a^x \equiv a^y \pmod m$  if and only if  $\text{ord}_m a \mid (x - y)$  if and only if  $x \equiv y \pmod{\text{ord}_m a}$ . i.e. Exponents work mod  $\text{ord}_m a$ .

**Ex.**  $\text{ord}_{11} 3 = 5$  so  $3^x \equiv 3^y \pmod{11}$  if and only if  $x \equiv y \pmod{5}$  ( $x \equiv y \pmod{5}$ ).

*Proof.*

→ Suppose  $a^x \equiv a^y \pmod m$  without loss of generality, assume  $x > y$ . Since  $\gcd(a, m) = 1$  we can cancel  $a^y$  from each side to get  $a^{x-y} \equiv 1 \pmod m$ . By (b) above then  $x - y \equiv 0 \pmod{\text{ord}_m a}$ .

← Suppose  $x \equiv y \pmod{\text{ord}_m a}$ , then  $x = y + k\text{ord}_m a$  for some  $k$ . Then  $a^x \equiv a^y a^{k\text{ord}_m a} \equiv a^y \left(a^{\text{ord}_m a}\right)^k \equiv a^y \cdot 1 \equiv a^y \pmod m$ . □

**Summary Ex.** We saw  $\text{ord}_{11} 3 = 5$ . So  $3^x$  repeats every 5<sup>th</sup> power mod 11 and  $3^5 \equiv 1 \pmod{11}$ .

### 3. Primitive Roots

- (a) **Introduction:** If  $\gcd(a, m) = 1$  we know that  $a^{\phi(m)} \equiv 1 \pmod m$  by Euler's Theorem, but this may not be the smallest power.  
**Ex.**  $\gcd(3, 11) = 1$  and so  $3^{\phi(11)} \equiv 1 \pmod{11}$  so  $3^{10} \equiv 1 \pmod{11}$ , but in fact  $3^5 \equiv 1 \pmod{11}$  and  $\text{ord}_{11} 3 = 5$  (smaller than 10).  
**Ex.**  $\gcd(6, 11) = 1$  and so  $6^{\phi(11)} \equiv 1 \pmod{11}$  so  $6^{10} \equiv 1 \pmod{11}$  and in fact this is the smallest.  $\text{ord}_{11} 6 = 10 = \phi(11)$ .
- (b) **Definition:** Suppose  $\gcd(a, m) = 1$ , we say  $a$  is a *primitive root* modulus  $m$  if  $\text{ord}_m a = \phi(m)$ .  $a = 3$  is not a primitive root mod 11, but  $r = 6$  is a primitive root mod 11.  
**Intuition:** Having a primitive root as a base results in more results when we raise it to powers.
- (c) **Theorem:** Suppose  $r$  is a primitive root mod  $m$ . Then  $\{r, r^2, \dots, r^{\phi(m)}\}$  is a reduced residue set mod  $m$ , meaning there are  $\phi(m)$  distinct items and all are coprime to  $m$ .

*Proof.* All are distinct because powers all distinct mod  $\phi(m) = \text{ord}_m a$ . All are coprime to  $m$  because all are powers of  $r$  and  $r$  is coprime to  $m$ .  $\square$

**Intuition:** Given an  $m$ , finding a primitive root  $r$  is nice because there will be  $\phi(m)$  distinct powers of  $r$  and that is the most we could have.

Given an  $m$ , can we always find a primitive root? No.  $m = 8$  has no primitive roots, but if  $m$  is prime then we can. If  $m$  has a primitive root, might it have several? It might ...

- (d) **Theorem:** Given a modulus  $m$  and an integer  $a$  with  $\gcd(a, m) = 1$  we have:

$$\text{ord}_m(a^k) = \frac{\text{ord}_m a}{\gcd(\text{ord}_m a, k)}$$

**Note:** In MATH403 this is the same result as the result from cyclic groups which states that if  $|g| = n$  then  $|g^k| = \frac{n}{\gcd(n, k)}$ .

**Ex.**  $\text{ord}_{11} 6 = 10$ . Look at  $\text{ord}_{11}(6^2)$ , intuitively it should be 5.

$$\text{ord}_{11}(6^2) = \frac{\text{ord}_{11} 6}{\gcd(\text{ord}_{11} 6, 2)} = \frac{10}{\gcd(10, 2)} = \frac{10}{2} = 5$$

*Proof.* We'll first prove it is  $\leq$  and  $\geq$ , thereby proving it is equal.

- First observe:

$$\begin{aligned} (a^k)^{\text{ord}_m a / \gcd(\text{ord}_m a, k)} &= (a^{\text{ord}_m a})^{k / \gcd(\text{ord}_m a, k)} \\ &\equiv 1^{k / \gcd(\text{ord}_m a, k)} \\ &\equiv 1 \pmod m \end{aligned}$$

So,

$$\text{ord}_m(a^k) \leq \frac{\text{ord}_m a}{\gcd(\text{ord}_m a, k)}$$

- Second observe:

$$\begin{aligned} a^{k \text{ord}_m(a^k)} &= (a^k)^{\text{ord}_m(a^k)} \\ &\equiv 1 \pmod{m} \end{aligned}$$

So then,  $\text{ord}_m a \mid k \text{ord}_m(a^k) \implies \frac{\text{ord}_m a}{\gcd(\text{ord}_m a, k)} \mid \frac{k \cdot \text{ord}_m(a^k)}{\gcd(\text{ord}_m a, k)}$ . Then, because gcd of two fractions is 1 we get,  $\frac{\text{ord}_m a}{\gcd(\text{ord}_m a, k)} \mid \text{ord}_m(a^k)$ , and so  $\frac{\text{ord}_m a}{\gcd(\text{ord}_m a, k)} \leq \text{ord}_m(a^k)$

Thus, the two results together give us that

$$\text{ord}_m(a^k) = \frac{\text{ord}_m a}{\gcd(\text{ord}_m a, k)}$$

□

- (e) **Theorem:** Suppose  $r$  is a primitive root of  $m$ . Then  $r^k$  is a primitive root of  $m$  if and only if  $\gcd(k, \phi(m)) = 1$ .

*Proof.* Well,  $r^k$  is a primitive root mod  $m$  if and only if  $\text{ord}_m(r^k) = \phi(m) = \text{ord}_m a$ , by the theorem this is true if and only if and only if  $\gcd(\text{ord}_m r, k) = 1$  if and only if  $\gcd(\phi(m), k) = 1$ . □

- (f) **Corollary:** If there is a primitive root mod  $m$  then there are  $\phi(\phi(m))$  of them.

*Proof.* Let  $r$  be a primitive root. Since powers of  $r$  form a reduced residue set mod  $m$  we know that all other integers coprime to  $m$  may be written as  $r^k$  for some  $k$ , then by the previous theorem we know that  $r^k$  is also a primitive root if and only if  $\gcd(k, \phi(m)) = 1$  and there are  $\phi(\phi(m))$  such  $k$ . □

**Ex.**  $r = 6$  is a primitive root mod 11. Then it has  $\phi(\phi(11)) = \phi(10) = 4$  primitive roots. What are they? Take  $k$  with  $\gcd(k, \phi(11)) = 1$  i.e.  $k$  with  $\gcd(k, 10) = 1$ . So  $k = 1, 3, 7, 9$ , therefore  $6^1, 6^3, 6^7, 6^9 \implies 6, 7, 8, 2$  are the primitive roots.