Math 406 Section 9.1: The Order of an Integer and 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 $a \mod m$.

2. **The Order of an Integer:** Given a modulus $m$ and an integer $a$ with $\gcd (a,m) = 1$ Euler’s Theorem tells us that $a^{\phi(m)} \equiv 1 \mod m$. It does not however tell us that $\phi(m)$ is the lowest power which yields 1. This leads to the following:

   (a) **Definition:** Given a modulus $m$ and an integer $a$ with $\gcd (a,m) = 1$ we define the order of $a \mod m$, denoted $\text{ord}_m a$ to be the smallest positive integer $n$ such that $a^n \equiv 1 \mod m$.

   **Note:** The order of $a$ depends not just on $a$ but also on the modulus $m$. Sometimes we say simply “the order of $a$” when the modulus is clear but it’s always relevant.

   **Example:** To find the order of $3 \mod 11$ we observe: $3^1 \equiv 3 \mod 11, 3^2 \equiv 9 \mod 11, 3^3 \equiv 5 \mod 11, 3^4 \equiv 4 \mod 11, 3^5 \equiv 1 \mod 11$. Thus $\text{ord}_{11} 3 = 5$.

   The order of an integer underlies the pattern under which powers of the integer repeat. For example since $\text{ord}_{11} 3 = 5$ this means that $3^x$ repeats when $x$ repeats mod 5, for example $3^4 \equiv 3^9 \mod 11$ because $4 \equiv 9 \mod 5$.

   This idea leads to the following theorems. For all of the following assume $\gcd (a,m) = 1$.

   (b) **Theorem 1:** For $x \in \mathbb{Z}^+$ we have $a^x \equiv 1 \mod m$ iff $x \equiv 0 \mod \text{ord}_m a$ which is iff $\text{ord}_m a | x$.

   **Example:** We have $3^x \equiv 1 \mod 11$ iff $x \equiv 0 \mod 5$ which is iff $5 | x$, so $x = 5, 10, 15,...$

   **Proof:**
   $\Rightarrow$: Assume $a^x \equiv 1 \mod m$ use the Division Algorithm to write $x = q(\text{ord}_m a) + r$ and then we have:
   $$1 \equiv a^x = (a^{\text{ord}_m a})^q a^r = a^r \mod m$$
   and since $0 \leq r < \text{ord}_m a$ we have $r = 0$.

   $\Leftarrow$: If $\text{ord}_m a | x$ then $x = q \text{ord}_m a$ for some $\alpha \in \mathbb{Z}$ and then $a^x = (a^{\text{ord}_m a})^\alpha \equiv 1 \mod m$.

   **QED**

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

   **Proof:** Obvious. **QED**

   **Note:** This can be used to help find orders more quickly. For example if want to know $\text{ord}_m a$ we need only check the divisors of $\phi(m)$.

   **Example:** To find $\text{ord}_{11} 2$ we note $\phi(11) = 10$ so we only need to check $2^1, 2^2$ and $2^5$ since if none of those work then it must be $2^{10}$.

   (d) **Theorem 2:** We have $a^x \equiv a^y \mod m$ iff $x \equiv y \mod \text{ord}_m a$.

   **Proof:**
   $\Rightarrow$: If $a^x \equiv a^y \mod m$ then WLOG assume $x > y$ and then cancel $a^y$ (coprimality guarantees we can) to get $a^{x-y} \equiv 1 \mod m$ and so then $\text{ord}_m a | (x-y)$.

   $\Leftarrow$: If $\text{ord}_m a | (x-y)$ then WLOG assume $x > y$ and then $x = y + q \text{ord}_m a$ for some $\alpha \in \mathbb{Z}^+$ and then:
   $$a^x = a^y (a^{\text{ord}_m a})^\alpha \equiv a^y \mod m$$

   **QED**

3. **Primitive Roots:** We know that given a modulus $m$ and an integer $a$ with $\gcd (a,m) = 1$ we have $\text{ord}_m a \leq \phi(m)$ (in fact it divides $\phi(m)$) but we are especially lucky when we have $\text{ord}_m a = \phi(m)$. The reason why this is lucky will be explained soon.
(a) **Definition:** Given a modulus $m$ and an integer $a$ with $\gcd(a, m) = 1$ we say that $a$ is a **primitive root mod** $m$ if $\text{ord}_m a = \phi(m)$.

**Example:** If $m = 11$ then $a = 6$ is a primitive root mod 11 because $\text{ord}_{11} 6 = 10 = \phi(11)$ which can be verified by noting that $6^1 \equiv 6, 6^2 \equiv 3$ and $6^5 \equiv 10$. Remember why we only need to check these, it’s because we know the order divides $\phi(11) = 10$ and so since it’s not 1, 2 or 5 it must be 10.

(b) **Theorem:** If $r$ is a primitive root mod $m$ then the set $\{r, r^2, r^3, \ldots, r^{\phi(m)}\}$ is a reduced residue set mod $m$.

**Note:** Recall this means that this set contains $\phi(m)$ integers all of which are coprime to $m$ and none of which are equivalent to each other mod $m$.

**Proof:** They are all coprime to $m$ since if $\gcd(m, r^k) \neq 1$ for some $k$ then if some prime $p$ divided both then it would divide $r^k$ and hence it would divide $r$, contradicting $\gcd(r, m) = 1$. If we had $r^i \equiv r^j \mod m$ then $i \equiv j \mod \text{ord}_m r = \phi(m)$ so that $i = j$ because each is nonstrictly between 1 and $\phi(m)$.

Interestingly if we start with a modulus $m$ there may or may not be any primitive roots mod $m$. For example $m = 8$ has no primitive roots since it can be easily checked that $\phi(8) = 4$ but $\text{ord}_8 1 = 1$, $\text{ord}_8 3 = 2$, $\text{ord}_8 5 = 2$ and $\text{ord}_8 7 = 1$ and so we never get $\text{ord}_8 a = \phi(8)$.

However if there is a primitive root then usually there are several. We’ll show how many in steps:

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

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

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

**Proof:** First, note that:

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

$$\equiv 1^{k / \gcd(\text{ord}_m a, k)} \mod m$$

$$\equiv 1 \mod m$$

This tells us that:

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

Second, note that by definition of the order of $a^k$ we have:

$$a^{k \text{ord}_m(a^k)} = (a^k)^{\text{ord}_m(a^k)} \equiv 1 \mod m$$

and so:

$$\text{ord}_m a | k \text{ord}_m(a^k)$$

From whence it follows that:

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

Since the gcd of the two fractions is 1 we then know that:

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

and so:

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

The two results together give us...  

**QED**
(d) **Corollary:** Suppose $r$ is a primitive root mod $m$, then $r^k$ is a primitive root mod $m$ iff $\gcd(k, \phi(m)) = 1$.

**Proof:** Well $r^k$ is a primitive root iff $\text{ord}_m (r^k) = \phi(m) = \text{ord}_m r$ and by the theorem this is iff $\gcd (\text{ord}_m r, k) = 1$ which is iff $\gcd (\phi(m), k) = 1$. \( \Box \)

**Example:** We saw that $r = 6$ is a primitive root mod 11. Thus we know that since $\phi(11) = 10$ then $6^3$ is also a primitive root mod 11 because $\gcd (3, 10) = 1$ whereas $6^4$ is not because $\gcd (4, 10) \neq 1$.

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

**Example:** There are $\phi(\phi(11)) = \phi(10) = 4$ primitive roots mod 11.

**Proof:** Let $r$ be one 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 corollary we know that $r^k$ is also a primitive root iff $\gcd (k, \phi(m)) = 1$ and there are $\phi(\phi(m))$ such $k$. \( \Box \)