Math 406 Section 9.1: The Order of an Integer and Primitive Roots

1. **Introduction (to Chapter 9):**

   Consider in basic algebra:

   $$3^x = 7 \quad \Leftrightarrow \quad x = \log_3 7$$

   How might this function, if at all, in modular arithmetic, say mod 10?

   $$3^x \equiv 7 \bmod 10 \quad \Leftrightarrow \quad \text{Hmmm...}$$

   In this example we can find a solution $x = 3$ by trial-and-error. But a different example fails to have a solution:

   $$9^x \equiv 7 \bmod 10 \quad \Leftrightarrow \quad \text{Hmmm...no such } x\text{...}$$

   This notion, of determining when we can find powers in modular arithmetic and what those powers are, is important in mathematics and computer science and is known as the *discrete logarithm problem.* It is extremely difficult when the modulus is large. For example $35^x \equiv 14536 \bmod 34571$ has solution $x = 458$ but that's not obvious at all.

   The approach to understanding these problems is to go back to Euler's Theorem to see, for a given base, what sorts of results we can achieve by raising that base to different powers.

2. **Nonpositive Powers**

   It's worth pausing to note that if $\gcd(a, m) = 1$ then we know that a has a multiplicative inverse mod m and so we can write the notation a^{-1} to refer to that inverse. In other words:

   $$aa^{-1} \equiv 1 \bmod m$$

   From here we can use all sorts of negative powers as long as we understand we mean inverses. So for example a^{-3} can be thought of either as $(a^{-1})^3$ (the cube of the inverse of a) or $(a^3)^{-1}$ (the inverse of the cube of a). These are the same thing.

   Everything is as expected with this notation.

   In addition if we say that $a^0 \equiv 1 \bmod m$ then we can make sense of all exponents when $\gcd(a, m) = 1$.

3. **The Order of an Integer:**

Given a modulus m and an integer a with $\gcd(a, m) = 1$ Euler's Theorem tells us that $a^{\phi(m)} \equiv 1 \bmod m$. 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 $a^n \equiv 1 \bmod m$.

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:

Consider $a = 3$ and $m = 11$. Euler's Theorem (and Fermat's Little Theorem) tell us that $3^{10} \equiv 1 \bmod 11$ but observe that 10 is not the first power for which we get 1.

To find the order of 3 mod 11 we observe:

$$\begin{aligned}
3^1 &\equiv 1 \bmod 11 \\
3^2 &\equiv 9 \bmod 11 \\
3^3 &\equiv 5 \bmod 11 \\
3^4 &\equiv 4 \bmod 11 \\
3^5 &\equiv 1 \bmod 11
\end{aligned}$$

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 $3^4 \equiv 3^9 \bmod 11$ because $4 \equiv 9 \bmod 5$.

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

(b) **Theorem 1:**

For $x \in \mathbb{Z}^+$ and $\gcd(a, m) = 1$ we have:

$$a^x \equiv 1 \bmod m \Longleftrightarrow x \equiv 0 \bmod \mathrm{ord}_m a \Longleftrightarrow \mathrm{ord}_m a \mid x.$$

Example:

We have $3^x \equiv 1 \bmod 11$ iff $x \equiv 0 \bmod 5$ iff $5 \mid x$, so $x = ..., -15, -10, 5, 0, 5, 10, 15, ...$

Proof:

The second $\Longleftrightarrow$ is just the defintion. For the first...

$\Rightarrow$ Assume $a^x \equiv 1 \bmod m$ use the Division Algorithm to write $x = q(\mathrm{ord}_m a) + r$ and then we have:

$$1 \equiv a^x = \left(a^{\mathrm{ord}_m a}\right)^q a^r \equiv a^r \bmod m$$

and since $0 \leq r < \mathrm{ord}_m a$ we have $r = 0$.

$\Leftarrow$ If $\mathrm{ord}_m a \mid x$ then $x = \alpha \cdot \mathrm{ord}_m a$ for some $\alpha \in \mathbb{Z}$ and then $a^x = \left(a^{\mathrm{ord}_m a}\right)^\alpha \equiv 1 \bmod m$.
$\mathcal{QED}$

(c) **Corollary:**

We have $\mathrm{ord}_m a \mid \phi(m)$.

Proof:

Since $a^{\phi(m)} \equiv 1 \bmod m$ this follows from the previous theorem. $\mathcal{QED}$

Note:

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

Example:

To find $\mathrm{ord}_{11} 2$ 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 $a^x \equiv a^y \bmod m$ iff $x \equiv y \bmod \mathrm{ord}_m a$.

Proof:

$\Rightarrow$ If $a^x \equiv a^y \bmod m$ then WLOG assume $x > y$ and then cancel a^y (coprimality guarantees we can) to get $a^{x-y} \equiv 1 \bmod m$ and so then $\mathrm{ord}_m a \mid (x - y)$.

$\Leftarrow$ If $\mathrm{ord}_m a \mid (x - y)$ then WLOG assume $x > y$ and then $x = y + \alpha \cdot \mathrm{ord}_m a$ for some $\alpha \in \mathbb{Z}^+$ and then:

$$a^x = a^y \left(a^{\mathrm{ord}_m a}\right)^\alpha \equiv a^y \bmod m$$

$\mathcal{QED}$

Understanding:

This tells us that although the base works mod m, the exponent works mod $\mathrm{ord}_m a$.

Example:

For example when $m = 20$ noting that $\mathrm{ord}_{20} 3 = 4$ and $\mathrm{ord}_{20} 9 = 2$ we can write:

$$63^{102} \cdot 109^{83} \equiv 3^{102} \cdot 9^{83} \equiv 3^2 \cdot 9^1 \bmod 20$$

Here the bases 63 and 109 reduce mod 20, the exponent 102 reduces mod $\mathrm{ord}_{20} 3 = 4$ and the exponent 83 reduces mod $\mathrm{ord}_{20} 9 = 2$.

4. **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) **Importance:**

Think of a primitive root as a "best possible" base in that powers of a primitive root will achieve all values coprime to m.

Example:

We saw that 6 is a primitive root mod 11 and observe that:

$$\{6^1, 6^2, 6^3, 6^4, 6^5, 6^6, 6^7, 6^8, 6^9, 6^{10}\} \equiv \underbrace{\{6, 3, 7, 9, 10, 5, 8, 4, 2, 1\}}_{\text{Got all the coprimes!}} \bmod 11$$

This is clarified in the following theorem:

(c) **Theorem:**

If r is a primitive rood mod m then the set $\left\{r, r^2, r^3, ..., r^{\phi(m)}\right\}$ 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 $r^i \equiv r^j \bmod m$ then $i \equiv j \bmod \text{ord}_m r = \phi(m)$ so that $i = j$ because each is nonstrictly between 1 and $\phi(m)$. $\mathcal{QED}$

(d) **Existence of Primitive Roots:**

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:

(e) **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 $|a^k| = \frac{|a|}{\gcd(|a|,k)}$.

Proof:

First, note that:

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

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:

$$a^{k \,\text{ord}_m\left(a^k\right)} = \left(a^k\right)^{\text{ord}_m\left(a^k\right)} \equiv 1 \bmod m$$

and so:

$$\text{ord}_m a \big| k \,\text{ord}_m\left(a^k\right)$$

From whence it follows that:

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

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

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

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... $\mathcal{QED}$

(f) **Corollary:**

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

Example:

We saw that $r = 6$ is a primitive root mod 11. Thus we know that since $\phi(11) = 10$ that all primitive roots can be found using 6^k with $\gcd(k, \phi(11)) = \gcd(k, 10) = 1$. This yields $k = 1, 3, 7, 9$ and thus the set of primitive roots mod 11 are $\{6^1, 6^3, 6^7, 6^9\} \equiv \{6, 7, 8, 2\}$ mod 11.

Proof:

Well r^k is a primitive root iff $\text{ord}_m\left(r^k\right) = \phi(m) = \text{ord}_m r$ and by the theorem this is iff $\gcd(\text{ord}_m r, k) = 1$ which is iff $\gcd(\phi(m), k) = 1$. $\mathcal{QED}$

(g) **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. $\mathcal{QED}$