9 Primitive Roots

9.1 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 mod m.

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

   (a) **Definition:** Suppose $\gcd(a,m) = 1$ we define the *order* of a mod m as the smallest power x such that $a^x \equiv 1 \bmod m$. 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,

   $$3^1 \equiv 3 \bmod 11$$
   $$3^2 \equiv 9 \bmod 11$$
   $$3^3 \equiv 5 \bmod 11$$
   $$3^4 \equiv 4 \bmod 11$$
   $$3^5 \equiv 1 \bmod 11$$

   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 repat!

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

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

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

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

$\leftarrow$ Assume $\mathrm{ord}_m a \mid x$. Then,

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

$\square$

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

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

So to find $\mathrm{ord}_m a$ try divisors of $\phi(m)$ only.
Ex. To find $\mathrm{ord}_{11} 2$ we note that $\phi(11) = 10$. So we need to check $1, 2, 5$ because if it fails for those, $\mathrm{ord}_{11} 2 = 10$.

$$2^1 \equiv 2 \not\equiv 1 \bmod 11$$
$$2^2 \equiv 4 \not\equiv 1 \bmod 11$$
$$2^5 \equiv 10 \not\equiv 1 \bmod 11$$

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

(d) **Theorem:** We have $a^x \equiv a^y \bmod m$ if and only if $\mathrm{ord}_m a \mid (x - y)$ if and only if $x \equiv y \bmod \mathrm{ord}_m a$. i.e. Exponents work mod $\mathrm{ord}_m a$.
Ex. $\mathrm{ord}_{11} 3 = 5$ so $3^x \equiv 3^y \bmod 11$ if and only if $x \equiv y \bmod \mathrm{ord}_{11} 3$ ($x \equiv y \bmod 5$).

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

$\leftarrow$ Suppose $x \equiv y \bmod \mathrm{ord}_m a$, then $x = y + k\mathrm{ord}_m a$ for some k. Then $a^x \equiv a^y a^{k\mathrm{ord}_m a} \equiv a^y \left(a^{\mathrm{ord}_m a}\right)^k \equiv a^y \cdot 1 \equiv a^y \bmod m$. $\square$

Summary Ex. We saw $\mathrm{ord}_{11} 3 = 5$. So 3^x repeats every 5^{th} power mod 11 and $3^5 \equiv 1 \bmod 11$.

3. **Primitive Roots**

(a) **Introduction:** If $\gcd(a, m) = 1$ we know that $a^{\phi(m)} \equiv 1 \bmod m$ by Euler's Theorem, but this may not be the smallest power.
Ex. $\gcd(3, 11) = 1$ and so $3^{\phi(11)} \equiv 1 \bmod 11$ so $3^{10} \equiv 1 \bmod 11$, but in fact $3^5 \equiv 1 \bmod 11$ and $\mathrm{ord}_{11} 3 = 5$ (smallet than 10).
Ex. $\gcd(6, 11) = 1$ and so $6^{\phi(11)} \equiv 1 \bmod 11$ so $6^{10} \equiv 1 \bmod 11$ and in fact this is the smallest. $\mathrm{ord}_{11} 6 = 10 = \phi(11)$.

(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 $\{r, r^2, \cdots, r^{\phi(m)}\}$ 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. □

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:

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

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

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 proof it is $\leq$ and $\geq$, thereby proving it is equal.

- First observe:

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

  So,

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

- Second observe:

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

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

Thus, the two results together give us that

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

□

(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 $\text{ord}_m\left(r^k\right) = \phi(m) = \text{ord}_m a$, 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 is 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.

9.2 Discrete Logarithms

---

1. **Introduction:** Just for reference, sections 9.2 and 9.3 concern themselves with the existence of primitive roots. They are quite technical so we will omit them and go on to section 9.4 which addresses what we can do with them. How can we solve (or even know if solutions exist) something like $3^x \equiv 5 \bmod 22$ 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).

2. **Back to Primitive Roots:** Recall that if $\gcd(r, m) = 1$ and r is a primitive root mod m then the set $\{r^1, r^2, \cdots, r^{\phi(m)}\}$ gets us all integers coprime to m.
   Ex. $r = 3$ is a primitive root of $m = 14$, because $3^1 \equiv 1, 3^2 \equiv 9, 3^3 \equiv 13, 3^4 \equiv 11, 3^5 \equiv 5, 3^6 \equiv 1 \bmod 14$. Note: $\text{ord}_{14}3 = 6 = \phi(14)$ so it is a primitive root. Note: we obtain $3, 9, 13, 1, 5, 1$ are all coprime to 14. Thus, we see that we can solve $3^x \equiv a \bmod 14$ if and only if $\gcd(a, 14) = 1$.

   In general, when r is a primitive root mod m then

   $$r^x \equiv a \bmod m \iff \gcd(a, m) = 1$$

   has solutions.

3. **Indices:**

   (a) **Definition:** Suppose r is a primitive root mod m and $\gcd(a, m) = 1$. The exponent x with $1 \leq x \leq \phi(m)$ satisfying $r^x \equiv a \bmod m$ is the *index* of a mod m with primitive root r. This is denoted $\text{ind}_r a$. Note: m is missing from the notation but it matters, generally it is known in the problem. We could also write $\log_r a$ too but be careful to not think it be a 'normal' log.
   Ex. $r = 3$ is a primitive root mod 14 and:

   $$3^1 \equiv 3 \bmod 14 \leftrightarrow \text{ind}_3 3 = 1$$
   $$3^2 \equiv 9 \bmod 14 \leftrightarrow \text{ind}_3 9 = 2$$
   $$3^3 \equiv 13 \bmod 14 \leftrightarrow \text{ind}_3 13 = 3$$
   $$3^4 \equiv 11 \bmod 14 \leftrightarrow \text{ind}_3 11 = 4$$
   $$3^5 \equiv 5 \bmod 14 \leftrightarrow \text{ind}_3 5 = 5$$
   $$3^6 \equiv 1 \bmod 14 \leftrightarrow \text{ind}_3 1 = 6$$

   Two Immediate Notes: If a, b coprime to m and r is a primitive root then:
   i. $r^{\text{ind}_r a} = a$
   ii. $a \equiv b \bmod m \iff \text{ind}_r a = \text{ind}_r b$. Side note, since indices are always between 1 and $\phi(m)$ we can actually write $a \equiv b \bmod m \iff \text{ind}_r a \equiv \text{ind}_r b \bmod \phi(m)$

   Idea - in pre-calculus we do things like:

   $$3^x = 4^{x-1}$$
   $$\ln 3^x = \ln 4^{x-1}$$
   $$x \ln 3 = (x - 1) \ln 4$$

   So now we can do things like:

   $$11^x \equiv 5^{x-1} \bmod 14$$
   $$\text{ind}_3 11^x \equiv \text{ind}_3 5^{x-1} \bmod \phi(14)$$

Can we know do "log-like" rules?

(b) **Index Rules:** Indices behave like logarithms (think logarithm laws) but there is a quirk that arises from the order of r, that being $\phi(m)$. To see why this is, consider the logarithm rule $\log(ab) = \log a + \log b$. It would be tempting to write: $\text{ind}_r(ab) = \text{ind}_r a + \text{ind}_r b$. However, this is not quite right. Consider that with $m = 14$ and $r = 3$ if we have $a = 13$ and $b = 5$ then $ab \equiv 9 \bmod 14$, the tempting statement would say:

$$\begin{aligned} \text{ind}_3 9 &= \text{ind}_3 13 + \text{ind}_3 5 \\ 2 &= 3 + 5 \\ 2 &= 8 \end{aligned}$$

Which is clearly false. However, we see that $2 \equiv 8 \bmod \phi(14)$.
Theorem: Let m be a modulus, r be a primitive root, and a, b coprime to m. Then we have:

i. $\text{ind}_r 1 \equiv 0 \bmod \phi(m)$

Proof. By Euler's Theorem we know that $r^{\phi(m)} \equiv 1 \bmod m$. So,

$$\text{ind}_r 1 = \phi(m) \equiv 0 \bmod \phi(m)$$

□

ii. $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \bmod \phi(m)$

Proof. Observe that from the definition of index:

$$\begin{aligned} r^{\text{ind}_r(ab)} &\equiv ab \bmod m \\ r^{\text{ind}_r a + \text{ind}_r b} = r^{\text{ind}_r a} r^{\text{ind}_r b} &\equiv ab \bmod m \end{aligned}$$

Then by a theorem from section 9.1 (which states that $a^x \equiv a^y \bmod m$ if and only if $x \equiv y \bmod \text{ord}_m a$) we get:

$$\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \bmod \phi(m)$$

□

iii. $\text{ind}_r a^k \equiv k\text{ind}_r a \bmod \phi(m)$

4. **The Discrete Logarithm Problem:** Given a modulus m and a primitive root r we know how to calculate $r^x \bmod m$ (given x) to reduce it. How hard is it to solve $r^x \equiv y \bmod m$ if y is given and we need x i.e. solving $\text{ind}_r y$. The answer, it is extremely hard. There is no meaningfully better way than trying all $1 \leq x \leq \phi(m)$. In simple cases we can try them all.

5. **Index Arithmetic:** We can use indices to solve modular problems involving exponets. Suppose we work frequently with the modulus $m = 17$. We first find a primitive root mod 17.

   Note: Assuming you know one exists

- Find one by finding r with $\text{ord}_{17} r = \phi(17) = 16$.
- There will be $\phi(\phi(17)) = \phi(16) = 8$ of them.

Turns out $r = 3$ is a primitive root. So let's solve some problems.

First, to find necessary discrete logs (aka indices) we will build a table:

a mod 17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

(a) **Ex.** Solve $3x^{10} \equiv 12 \bmod 17$. Take the ind_3 of both sides.

$$\begin{aligned}
\text{ind}_3(3x^{10}) &\equiv \text{ind}_3(12) \bmod 16 \\
\text{ind}_3 3 + \text{ind}_3 x^{1}0 &\equiv \text{ind}_3 12 \bmod 16 \\
\text{ind}_3 3 + 10(\text{ind}_3 x) &\equiv \text{ind}_3 12 \bmod 16 \\
1 + 10(\text{ind}_3 x) &\equiv 13 \bmod 16 \\
10(\boxed{\text{ind}_3 x}) &\equiv 12 \bmod 16^{*} \qquad \text{treat this as } \textit{one} \text{ variable}
\end{aligned}$$

Recall: $ax \equiv b \bmod m$ has solutions if and only if $\gcd(a,m) \mid b$ and if so, $\exists \gcd(a,m)$ incongruent solutions mod m. Obtain x_0 via guessing or the Euclidean Algorithm, then all solutions have the form $x = x_0 + k\frac{m}{\gcd(a,m)}$. Since $\gcd(10,16) = 2 \mid 12$, $\exists 2$ solutions mod 16. The solutions we get are:

$$\text{ind}_3 x \equiv 6, 14 \bmod 16$$

Use the table to "un-index":

$$x \equiv 15, 2 \bmod 17$$

***Note:** We could, at this point, do

$$\begin{aligned}
5\text{ind}_3 x &\equiv 6 \bmod \frac{16}{\gcd(16,2)} \\
5\text{ind}_3 x &\equiv 6 \bmod 8 \\
\text{ind}_3 x &\equiv 6 \bmod 8
\end{aligned}$$

This is unique mod 8 because $\gcd(5,8) = 1$. To "un-index" we need mod 16.

$$\text{ind}_3 x \equiv 6 \bmod 8 \implies \text{ind}_3 x \equiv 6, 14 \bmod 16$$

Now we can "un-index"

(b) **Ex.** Solve $4^x \equiv 16 \bmod 17$. We will take the ind_3 of both sides.

$$\begin{aligned}
\text{ind}_3(4^x) &\equiv \text{ind}_3(16) \bmod 16\\
x\text{ind}_3 4 &\equiv \text{ind}_3(16) \bmod 16\\
x(12) &\equiv 8 \bmod 16\\
12x &\equiv 8 \bmod 16\\
3x &\equiv 2 \bmod \frac{16}{\gcd(4,16)}\\
3x &\equiv 2 \bmod 4
\end{aligned}$$

Since $\gcd(3,4) = 1 \mid 2$, $\exists$ a solution mod 4.

$$x \equiv 2 \bmod 4$$

Note: Any of $x = \cdots, -6, -2, 2, 6, \cdots$ works.
Note: Could also give as $x \equiv 2, 6, 10, 14 \bmod 16$ ("un-index" back to original mod)

Note: We can do either of these problems again with a completely different primitive root mod 17. As an exercise in understanding, we could do the two examples above with a different primitive root.

9.3 Problems

---

1. Determine the following orders and justify each.
   (a) $\text{ord}_{21}8$
   (b) $\text{ord}_{25}8$
2. Find all primitive roots (reduced mod 50) for $n = 50$ as follows: First find (with justification) the smallest primitive root. Then use the Theorem from class which yields all the remaining ones.
3. Prove that if p is an odd prime and a has $\text{ord}_p a = 2k$ then $a^k \equiv -1 \mod p$
4. Show that if a is relatively prime to m and $\text{ord}_m a = m - 1$ then m is prime.
5. Suppose r is a primitive root of an odd prime p. Prove that:
$$\text{ind}_r(p-a) \equiv \text{ind}_r a + \left(\frac{p-1}{2}\right) \mod p-1$$
6. Show that if n is an integer and a and b are integers which are relatively prime to n with $\gcd(\text{ord}_n a, \text{ord}_n b) = 1$ then $\text{ord}_n(ab) = (\text{ord}_n a)(\text{ord}_n b)$.

7. Let r be a primitive root of the prime p with $p \equiv 1 \mod 4$. Prove that $-r$ is also a primitive root.

8. It's a fact that $r = 7$ is a primitive root mod 13.

   (a) Use this to construct a table of indices for this primitive root.

   (b) Use the table of indices to solve the equation: $x^2 \equiv 12 \mod 13$. Your answer(s) should be mod 13.

   (c) Use the table of indices to solve the equation: $4^x \equiv 12 \mod 13$. Your answer(s) should be mod 12.

9. With logarithms we have $\log_r a - \log_r b = \log_r \left(\frac{a}{b}\right)$

   (a) Why is it not reasonable to write $\equiv \text{ind}_r a - \text{ind}_r b \mod \phi(n) \equiv \text{ind}_r \left(\frac{a}{b}\right)$ when a, b are coprime to n and r is a primitive root?

   (b) What would be a reasonable index substitute for this logarithm rule?

   (c) Prove this substitute.

10. Suppose p is an odd prime and both r_1 and r_2 are primitive roots for p. Prove that $r_1 r_2$ is not a primitive root for p.