Chapter 7 of Number Theory with Computer Applications

by Kumanduri and Romero;

University of Windsor 62-322 Course notes by M. Hlynka and

W.L. Yee.

PRIMITIVE ROOTS

7.1 THE CONCEPT OF ORDER

Definition 7.1.1 Let a and n be integers with $(a,n)=1$. Let the *the order of* $a \mod n$ (denoted $ord_n(a)$) be the smallest integer k such that $a^k \equiv 1 \mod n$.

By Euler's Theorem, if $(a,n)=1$, then $a^{\phi(n)}=1$. But there may be integers $k<\phi(n)$ for which $a^k \equiv 1 \mod n$. Let us consider $n=2,3,4,5,6$.

For $n=2$, $1^1 \equiv 1 \mod 2$ so $ord_2(1)=1$.

For $n=3$, $1^1 \equiv 1 \mod 3$ and $2^2 \equiv 1 \mod 3$ so $ord_3(1)=1$, $ord_3(2)=2$.

For $n=4$, $1^1 \equiv 1 \mod 4$ and $3^2 \equiv 1 \mod 4$ so $ord_4(1)=1$, $ord_4(3)=2$.

For $n=5$, $1^1 \equiv 1 \mod 5$, $2^4 \equiv 1 \mod 5$ while $2^2 \equiv 4 \not\equiv 1 \pmod 5$, $3^4 \equiv 1 \mod 5$ while $3^2 \equiv 4 \not\equiv 1 \pmod 5$, and $4^2 \equiv 1 \mod 5$ so $ord_5(1)=1$, $ord_5(2)=4$, $ord_5(3)=4$, $ord_5(4)=2$.

Note that $\phi(5)=4$ so $a^4 \equiv 1 \mod 5$ for $(a,5)=1$. However, $4^2 \equiv 1 \mod 5$ so $ord_5(4)<\phi(5)$.

For $n=6$, $1^1 \equiv 1 \mod 6$ and $5^2 \equiv 1 \mod 6$ so $ord_6(1)=1$, $ord_6(5)=2$.

Note: (a) $ord_n(1)=1 \quad \forall n$.

(b) $ord_n(-1)=2 \quad \forall n>2$.

(c) If $ord_n(a)=k$, then $a^k \equiv 1 \mod n$ so $a^{2k}, a^{3k}, \cdots \equiv 1 \mod n$.

Example: For $n=31$, find $ord_n(2)$, $ord_n(3)$. Find all k such that $2^k \equiv 1 \mod 31$.

SOLUTION: We look at powers of 2: 2,4,8,16,32. Since $32=2^5 \equiv 1 \mod 31$, we have $ord_{31}(2) = 5$. So $2^k \equiv 1 \mod 31$ for $k = 5, 10, 15, 20, 25, 30, \ldots$.

Look at powers of $3 \mod 31$: 3,9,27 $\equiv -4 \mod 31$,-12,$-36 \equiv -5 \mod 31$,-15, $-45 \equiv -14 \mod 31$, $-42 \equiv -11 \mod 31$,$-33 \equiv -2 \mod 31$. How far do we have to check???

Proposition 7.1.3 If $a^m \equiv 1 \mod n$, then $ord_n(a)|m$.

Proof. Let $k = ord_n(a)$. Then $m = kq+r$ for some q and some r with $0 \leq r < k$ (note typo in text). If $k \nmid m$, then $0 < r < k$. So

$$1 \equiv a^m \equiv a^{kq+r} \equiv (a^k)^q a^r \equiv 1^q a^r \equiv a^r.$$

Since $0 < r < k$ and $a^r \equiv 1 \mod n$, this contradicts the definition of $k = ord_n(a)$ as being the smallest value j such that $a^j \equiv 1 \mod n$. Thus $r = 0$ so $k|m$. ■

Corollary 7.1.4: If $(a, n) = 1$ and $a^i \equiv a^j \mod n$, then $i \equiv j \mod ord_n(a)$.

Proof. Assume $i > j$. Since $(a, n) = 1$, we also have $(a^j, n) = 1$. Divide both sides of $a^i \equiv a^j \mod n$ by a^j to get $a^{i-j} \equiv 1 \mod n$. Hence $ord_n(a)|(i - j)$ so $i \equiv j \mod ord_n(a)$. ■

Corollary 7.1.6 If $(a, n) = 1$ and $ord_n(a) = k$, then $1, a, a^2, \ldots, a^{k-1}$ are distinct mod n.

Proof. Assume $a^i \equiv a^j \mod n$ for some i, j with $1 \leq i < j \leq k < n$. Then by Corollary 7.1.4, $i \equiv j \mod k$. Since $1 \leq i < j \leq k$, this is not possible. So $1, a, a^2, \ldots, a^{k-1}$ are distinct mod n. ■

Corollary 7.1.5 (a) If $(a, n) = 1$, then $ord_n(a)|\phi(n)$.

(b) If p is prime, and $(a, p) = 1$, then $ord_n(a)|(p - 1)$.

Proof. (a) By Euler's Theorem, if $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$. By Proposition 7.1.3, $ord_n(a)|\phi(n)$.

(b) If n is prime, then $\phi(n) = n - 1$. So the second part follows. ■

Example Read Example 7.1.7. Beware of typos.

Find $k = ord_{31}(3)$. Since $\phi(31) = 30$, we know that $k|30$. So we need only check if $k = 1, 2, 3, 5, 6, 10, 15, 30$.

$3^1 \equiv 3 \mod 31$. $3^2 \equiv 9 \mod 31$. $3^3 \equiv 27 \mod 31$. $3^5 \equiv -5 \mod 31$, $3^6 \equiv -15 \mod 31$, $3^{10} \equiv 25 \equiv -6 \mod 31$, $3^{15} \equiv 3^{10}3^5 \equiv 30 \mod 31$. So the only possible value of k is $k = 30$.

Exercise, p. 171. Find a such that the powers of a together with 0 form a complete residue system mod 23.

SOLUTION: Note that $\phi(23) = 22$. We want to find a such that $\{a, a^2, \ldots, a^{22}\}$ consists of distinct elements $\mod 23$. Try $a = 2$. Then the powers of a give values $a^1, a^2, \ldots, \mod 23$, namely $2, 4, 8, 16 \equiv -7$, $-14 \equiv 9$, $18 \equiv -5$, -10, $-20 \equiv 3$, 6, 12, $24 \equiv 1 \mod 23$. The length of this cycle is 11, which divides 22. We want a cycle of length 22. We could try powers of 3, and if this does not work, try powers of 4, etc. A more clever idea is to note that $2^{11} \equiv 1$ so $(-2)^{11} \equiv -1 \mod 23$. The powers of -2 will be congruent to the same values as 2 except that the odd powers will give the negative of the previous odd powers. Since $21 \equiv -2 \mod 23$, it follows that $21^1, 21^2, \ldots, 21^{22}$ will give a complete residue system $\mod 23$ (exccept for the missing value 0).

Connections to Abstract Algebra: Algebra is the study of groups, rings, fields, and other algebraic structures. A group G is a collection of objects with some kind of operation $*$ on the elements of G with properties of closure $(a * b \in G)$, an identity element $(a * e = e * a = a)$, an associative property, i.e. $(a * b) * c = a * (b * c)$, and an inverse $(a * a^{-1} = e)$.

A complete residue system mod m forms a group under addition (sometimes written as $\mathbb{Z}/m\mathbb{Z}$).(Here $* = +$, $e = 0$, $a^{-1} = -a$.)

If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a finite field.

The nonzero integers mod p (p prime) form a group under multiplication. (Here $* = \times$, $e = 1$, $a^{-1} = a^{-1}$.)

The nonzero integers mod n and relatively prime to n form a group under multiplication.

If G is a finite group, then the number of elements in G is called the *order of G*

$o(G)$.

If G is a group, and if there exists an a such that $G = \{a, a^2, a^3, \ldots, a^{o(G)}\}$, then G is a cyclic group, and a is a generator of G.

If G is a finite group, and $a \in G$, then $S = \{a, a^2, \ldots, a^k = e\}$ is a subgroup of G and $o(S)|o(G)$.

If G is a finite group and $a \in G$, then $a^{o(G)} = e$. (Euler's Theorem)

2001 Putnam A-1. Consider a set S and a binary operation $*$ i.e., for each $a, b \in S$, $a*b \in S$. Assume $(a*b)*a = b$ for all $a, b \in S$. Prove that $a*(b*a) = b$ for all $a, b \in S$.

SOLUTION: $a * (b * a) = ((b * a) * b) * (b * a) = b$.

Lemma 7.1.8 If $(a, n) = 1$, then $ord_n(a^k) = \dfrac{ord_n(a)}{(k, ord_n(a))}$.

Proof. See. text, p. 171. ■

Example:

If $ord_n(a) = 9$, then $ord_n(a^2) = \dfrac{9}{(9,2)} = 9$

If $ord_n(a) = 10$, then $ord_n(a^2) = \dfrac{10}{(10,2)} = 5$

Example: If $ord_n(a) = 12$, then by Corollary 7.1.6, $1, a^1, a^2, \ldots, a^{11}$ are distinct mod n. Since 1=(1,12)=(5,12)=(7,12)=(11,12), we know that a, a^5, a^7, a^{11} all have order 12.

Since 2=(2,12)=(10,12), we know that a^2, a^{10} have order 12/2=6.

Since 3=(3,12)=(9,12), we know that a^3, a^9 have order 12/3=4.

Since 4=(4,12)=(8,12), we know that a^4, a^8 have order 12/4=3.

Finally a^6 has order 12/6=2.

Note: The maximal possible order of an element a mod n is $\phi(n)$. Such a value a is useful. For example, in simulation of pseudo random numbers, a common algorithm uses a seed s and a multiplier a and a modulus m to give $s, as, a^2s, a^3s, \ldots \mod m$. We want this cycle to be as long as possible before repeating. However, for some n, there is no element with the maximal possible order.

Note: If $ord_n(a) = \phi(n)$, then any invertible element (mod n) equals a^r for some r.

Definition 7.1.11: An integer a such that $ord_n(a) = \phi(n)$ is called a primitive root mod n.

Example: 21 is a primitive root mod 23.

Example: $\phi(8) = 4$. Recall that if a is an odd number, then $a^2 \equiv 1 \mod 8$. Thus if $(a, 8) = 1$, then $a^2 \equiv 1 \mod 8$. So $ord_8(a) = 2$ for $a = 3, 5, 7$. So there are NO primitive roots mod 8 since $\phi(8) = 4$.

Proposition 7.1.13. There is no primitive root mod 2^k for $k \geq 3$.

Proof. By contradiction, suppose a is a primitive root modulo 2^k. $\phi(2^k) = 2^{k-1}$, so $ord(a) = 2^{k-1}$ and thus the 2^{k-1} elements $\{a, a^2, a^3, \dots, a^{2^{k-1}}\}$ are distinct modulo 2^k and are all invertible. This implies that there is only one element of order 2 since if $x = a^i$ has order 2, then by Lemma 7.1.8 $ord_{2^k}(a^i) = 2^{k-1}/(i, 2^{k-1}) = 2$ which implies $(i, 2^{k-1}) = 2^{k-2}$ which implies $i = 2^{k-2}$. However, by Exercise 3.4.7, for $k \geq 3$, there are four solutions to the equation $x^2 \equiv 1 \pmod{2^k}$, and so there are three elements of order 2. Contradiction. Therefore there is no primitive root mod 2^k for $k \geq 3$. ∎

Proposition 7.1.14: Suppose p is an odd prime. There can be no primitive root mod m unless $m = 2, 4, p^k, 2p^k$.

Proof. Suppose $n = rs$, with r and s greater than 2 and $(r, s) = 1$. (Integers not of this form $2^k, p^b, 2p^b$.) Here $\phi(n) = \phi(r)\phi(s)$. For any $c > 2$, it is easy to check that $\phi(c)$ is even. By Euler's Theorem, we get for any a with $(a, n) = 1$,

$$a^{\phi(r)\phi(s)/2} \equiv \left(a^{\phi(r)}\right)^{\phi(s)/2} \equiv 1 \mod r$$
$$a^{\phi(r)\phi(s)/2} \equiv \left(a^{\phi(s)}\right)^{\phi(r)/2} \equiv 1 \mod s.$$

By the Chinese remainder theorem,
$a^{\phi(r)\phi(s)/2} \equiv 1 \mod n$ for all a such that $(a, n) = 1$, so $a^{\phi(n)/2} \equiv 1 \mod n$. Thus for any a with $(a, n) = 1$, we have $ord_n(a)|\phi(n)/2$ so $ord_n(a) \leq \phi(n)/2 < \phi(n)$. So there is no primitive root mod n. ■

Example: There are no primitive roots mod 16. There are no primitive roots mod 15. There may be primitive roots mod 9 or mod 18.
Note that $\phi(9) = \#\{1, 2, 4, 5, 7, 8\} = 6$. Then, mod 9, $2, 2^2 = 4, 2^3 = 8$ so $ord_9(2) > 3$. But since $ord_9(2)|\phi(9)$, it follows that $ord_9(2) = 6$ so 2 is a primitive root mod 9.
Note that $\phi(18) = \phi(2)\phi(9) = 1(6) = 6$. Try 5 to check if it is a primitive root mod 18. $5, 5^2, 5^3, \ldots$ give 5,7,-1,-5,-7,1 mod 18. So 5 is a primitive root.

Example: Solve $4^x \equiv 5 \mod 19$.
SOLUTION: These values should repeat after $\phi(19) = 18$ steps. We could try each $x \mod 18$. Rather than that, we seek a primitive root and make a table of powers. Try 2. Its powers are 2,4,8,-3,-6,7,-5,9,-1,-2,-4,-8,3,6,-7,5,-9,1. So we get a table

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2^k \mod 19$	1	2	4	8	-3	-6	7	-5	9	-1	-2	-4	-8	3	6	-7	5	-9	1

Our problem converts to $2^{2x} \equiv 2^{16} \mod 19$. Since the powers 2^1 to 2^{18} of 2 are all distinct mod 19, we have $2x \equiv 16 \mod 18$ so $x \equiv 8 \mod 9$.

Example: Use the table above to find the inverse of 6 mod 19.
SOLUTION: Note that $6 \equiv 2^{14} \mod 19$. Since $2^{18} \equiv 1 \mod 19$, the inverse must be $2^4 \equiv -3 \equiv 16 \mod 19$. So the inverse of 6 is $16 \mod 19$.

Exercises: p. 174, # 1, 2,3,4, 5, 6, 9, 10, 17.

Exercise p. 174 1) Determine the order of the following elements.

a) $9 \pmod{17}$

$\phi(17) = 16$ so $ord(9)|16$.

$9^2 \equiv 81 \equiv -4 \pmod{17}$

$9^4 \equiv 16 \equiv -1 \pmod{17}$

$9^8 \equiv 1 \pmod{17}$

Therefore $ord_{17}(9) = 8$.

b) $11 \pmod{47}$

$\phi(47) = 46 = 2 \cdot 23$.

Therefore $ord_{47}(11) = 2, 23$, or 46.

$11^2 \equiv 121 \equiv 27 \pmod{47}$ so the order of 11 isn't 2

$11^4 \equiv 27^2 \equiv 24 \pmod{47}$

$11^8 \equiv 24^2 \equiv 12 \pmod{47}$

$11^{16} \equiv 12^2 \equiv 3 \pmod{47}$

$11^{23} \equiv 11^{16} \times 11^4 \times 11^2 \times 11 \equiv 3 \times 24 \times 27 \times 11 \equiv 21384 \equiv 46 \pmod{47}$

Therefore $ord_{47}(11) = 46$.

Exercise p. 175 4) If a has order k, how many of $1, a, a^2, \ldots, a^{k-1}$ have order k?

$ord(a^j) = \frac{ord(a)}{(j, ord(a))} = \frac{k}{(j,k)} = k$ when $(j, k) = 1$. Therefore $\phi(k)$ of the elements have order k.

Exercise p. 175 5a) Find a primitive root modulo 19 and use it to find all the primitive roots.

Note: to test if a is a primitive root modulo n:

- Find the prime factors $p_1, \ldots, p_k$ of $\phi(n)$

- a is a primitive root if each $a^{\frac{\phi(n)}{p_i}} \not\equiv 1 \pmod{n}$ (see homework Assignment 5 #5)

$ord_{19}(2)|\phi(19) = 18$. $2^8 \equiv 9 \pmod{19}$ so $2^9 \equiv 18 \pmod{19}$ and $2^2 \equiv 4 \pmod{19}$ while $2^{18} \equiv 1 \pmod{19}$. Therefore $ord_{19}(2) = 18$ and 2 is a primitive root. All primitive roots of 19 are 2^j where $(j, 18) = 1$. We have the following table:

$j : (j, 18) = 1$	$2^j \pmod{19}$
1	2
5	$2^5 \equiv 13$
7	$2^7 \equiv 14$
11	$2^{11} \equiv 15$
13	$2^{13} \equiv 3$
17	$2^{17} \equiv 10$

Therefore the primitive roots of 19 are $2, 3, 10, 13, 14, 15$.

Exercise p. 176 17b) Solve $7 \cdot 5^x \equiv 5 \pmod{19}$.

From the previous question, we know that 2 is a primitive root modulo 19. We have the following table:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2^k \mod 19$	1	2	4	8	-3	-6	7	-5	9	-1	-2	-4	-8	3	6	-7	5	-9	1

$5 \equiv 2^{16} \pmod{19}$.

$7 \equiv 2^6 \pmod{19}$. Therefore our equation becomes:

$2^6 \times 2^{16x} \equiv 2^{16} \pmod{19}$ so we need to solve $6 + 16x \equiv 16 \pmod{18}$, i.e. $8x \equiv 5 \pmod{9}$.

This has solution $x \equiv -5 \equiv 4 \pmod{9}$.

7.2 THE PRIMITIVE ROOT THEOREM

We prove the existence of primitive roots when $n = p^k, 2p^k$ for p an odd prime.

Recall **Theorem 4.4.1** Lagrange's Theorem: Let p be a prime number and let $f(x)$ be a polynomial of degree $n \geq 1$, not all of whose coefficients are divisible by p. Then $f(x) \equiv 0 \pmod{p}$ has at most n solutions in a complete residue system modulo p.

Theorem 7.2.8 Let p be a prime number; then there exists a primitive root modulo p.

Proof: Let λ be the minimal universal exponent of p: i.e. it is the smallest integer such that $a^\lambda \equiv 1 \pmod{n}$ for all $(a, n) = 1$. If $\lambda = p - 1$, then there exists an element of order $p-1$, hence there is a primitive root. Assume that $\lambda < p-1$. All $p-1$ invertible elements satisfy $x^{\lambda} \equiv 1 \pmod p$ contradicting Lagrange's Theorem that it has at most λ solutions. Therefore $\lambda = p-1$ and there is a primitive root.

Theorem 7.2.10 Let p be an odd prime.

a) If g is a primitive root modulo p, then either g or $g+p$ is a primitive root modulo p^2.

b) If g is a primitive root modulo p^2, then g is a primitive root modulo p^k for every $k \geq 2$.

c) If g is odd and a primitive root modulo p^k for $k \geq 1$, then g is a primitive root modulo $2p^k$. Otherwise, if g is even, then $g+p^k$ is a primitive root modulo $2p^k$.

Proof: a) $d := ord_{p^2}(g) | p(p-1) = \phi(p^2)$. $g^d \equiv 1 \pmod{p^2} \Rightarrow g^d \equiv 1 \pmod p$ $\Rightarrow p-1 | d \Rightarrow d = p-1$ or $p(p-1)$. If $d = p(p-1)$, then g is a primitive root modulo p^2. So suppose $d = p-1$. We show in this case $g+p$ is a primitive root modulo p^2. Again, since $g+p \equiv g \pmod p$, then $p-1$ divides $ord_{p^2}(g+p)$, so $ord_{p^2}(g+p) = p-1$ or $p(p-1)$. If $ord_{p^2}(g+p) = p-1$, then

$$(g+p)^p \equiv (g+p)(g+p)^{p-1} \equiv g+p \pmod{p^2}.$$

By the Binomial Theorem,

$$(g+p)^p \equiv \sum_{k=0}^{p} \binom{p}{k} g^k p^{p-k} \equiv g^p + p^2 g^{p-1} \equiv g^p \pmod{p^2}.$$

Since $g^{p-1} \equiv 1 \pmod{p^2}$ so that $g^p \equiv g \pmod{p^2}$, our equations give

$$(g+p)^p \equiv g+p \equiv g \pmod{p^2}$$

$\Rightarrow p \equiv 0 \pmod{p^2}$–contradiction. Therefore $g+p$ is a primitive root modulo p^2.

b) Note: textbook has mistakes.

$ord_{p^k}(g)$ divides $\phi(p^k) = p^{k-1}(p-1)$ and $p-1|ord_{p^k}(g)$ since g is a primitive root modulo p. Thus $ord_{p^k}(g) = p^a(p-1)$ for some $0 \leq a \leq k-1$. We wish to show $a = k-1$. Enough to show $g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. Show by induction.

Base case: $k = 2$. Given. g is a primitive root modulo p^2.

Induction step: Assume the result for k. That is, $g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. We need to show that $g^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$. $p^{k-2}(p-1) = \phi(p^{k-1})$ so $g^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}$ while $g^{\phi(p^{k-1})} \not\equiv 1 \pmod{p^k}$. Therefore $g^{\phi(p^{k-1})} = 1 + bp^{k-1}$ where $p \not| b$. Then:

$$\begin{aligned}
g^{p^{k-1}(p-1)} &= (1+bp^{k-1})^p \\
&= 1 + pbp^{k-1} + \binom{p}{2}(bp^{k-1})^2 + \binom{p}{3}(bp^{k-1})^3 + \cdots \\
&\equiv 1 + bp^k \pmod{p^{k+1}}
\end{aligned}$$

so $g^{p^{k-1}(p-1)} \equiv 1 + bp^k \not\equiv 1 \pmod{p^{k+1}}$.

Therefore by induction g is a primitive root modulo p^k for every $k \geq 2$.

c) Note that $\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$.

If g is odd, then $g^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}$ while $g^{p^{k-1}(p-1)/q} \not\equiv 1 \pmod{p^k}$ for $q = p$ and $q =$ primes dividing $p-1$. $g^{p^{k-1}(p-1)} \equiv 1 \pmod 2$ and $g^{p^{k-1}(p-1)/q} \equiv 1 \pmod 2$. Therefore $g^{p^{k-1}(p-1)} \equiv 1 \pmod{2p^k}$ while $g^{p^{k-1}(p-1)/q} \not\equiv 1 \pmod{2p^k}$. Therefore g is a primitive root modulo $2p^k$.

Similarly, if g is even, $g + p^k$ is a primitive root modulo $2p^k$.

Combining Theorems 7.2.8 and 7.2.10 and Proposition 7.1.14,

Theorem: There are primitive roots modulo n only for $n = 2, 4, p^k, 2p^k$ where p is an odd prime.