A. **Order.** We know that if if $a \perp n$, then $a^{\phi(n)} \equiv 1 \mod n$.

But, for a given a, are there smaller positive exponents that produce 1?

Let n be a positive integer and a be an integer such that:

The **order** of a modulo n is the least positive integer k such that

For example, let's calculate the order of 2 and of 3 modulo 7.

By Euler's Theorem, the order an integer $\perp 7$ modulo 7 is always:

The integer 3 achieves this maximal order and hence is called

Let n be a positive integer and $a \perp n$ be an integer.

We call a a **primitive root** modulo n iff

As we shall see, not all integers have primitive roots.

Next let's place a restriction on the order.

Theorem. Let n be a positive integer and $a \perp n$ be an integer with order k.

Let h be another integer.

Then $a^h \equiv 1 \mod n$ if and only if:

Proof. We apply the division algorithm to obtain

Thus working modulo n

$a^h \equiv$

Therefore $a^h \equiv 1$ iff:

which, because r inonnegative and less than the order k of a, occurs iff:

which occurs iff:

□

Corollary. Let n be a positive integer and $a \perp n$ be an integer.

Then, since:

the order of a divides:

Example 1. Show that 2 is a primitive root of 13.

Solution. We compute $\phi(13) =$

The order of 2 must divide $\phi(13)$, thus must be one among the list

To be a primitive root, the order of 2 would have to be the maximum.

Let's compute powers of 2.

Example 2. Show that 8 has no primitive roots.

Solution. We compute $\phi(8) =$

Next we compute the order of each integer $\perp 8$.

B. **Properties of Order.** We next prove a few properties of order.

Theorem. Let n be a positive integer and $a \perp n$ be an integer with order k.

Let i and j be integers. Then

Proof. Because $a \perp n$, we may use its inverse to rewrite

By the theorem from two pages back, this congruence occurs if and only if

□

Consequently, we can enumerate all powers of $a \perp n$ as follows.

Corollary. Let n be a positive integer and $a \perp n$ be an integer with order k.

The integer powers of a modulo n are completely and distinctly listed by

E.g. since the order of 2 modulo 7 is 3, any power of 2 modulo 7 is in the list

Next we prove a result about orders of powers.

Theorem. Let n be a positive integer and $a \perp n$ be an integer with order k.

Let h be an integer. Then a^h has order:

Proof. Let $d =$

We show that the powers of a^h that yield 1 are precisely the multiples of k/d.

Let i be an integer such that

By the theorem from two pages back, this occurs if and only if

But since $k/d \perp h/d$, by Euclid's Lemma this occurs if and only if:

□

Primitive Roots. We apply our theorems to primitive roots.

Theorem. Let n be a positive integer having a primitive root a.

Then the list:

contains, up to congruence mod n, every integer that is:

Among this list, the primitive roots of n are precisely the a^h such that

Thus, if there is at least one primitive root of n, then

[# of primitive roots of n] =