Powers of Two. We show powers of two generally don't have primitive roots.

Theorem. The only positive powers of 2 that have primitive roots are 2 and 4.

Proof. Evidently 1 is a primitive root of 2, and 3 is a primitive root of 4.

The theorem will then follow from the lemma below, as the lemma would imply

Lemma. Let $k \geqslant 3$ be an integer and a be odd. Then

Proof. Note that $\phi(2^k)/2 =$

So we need to address the congruence

goal $\rightarrow$

We use induction on $k \geqslant 3$.

Base Case. If $k = 3$ then

Inductive Assumption. Let integer $k \geqslant 3$ be given.

assume $\rightarrow$

Inductive Step.

goal $\rightarrow$

Using difference of squares

The first factor is divisible by 2 because:

By induction, the second factor is divisible by:

Hence the product of the factors:

which completes the proof.

□

No Primitive Roots. We finish listing those integers without primitive roots.

Theorem. A positive integer does not have a primitive root if

- either it is a power of 2 greater or equal 8
- or it is divisible by:
- or it is divisible by:

Proof. We addressed the first bullet point on the last page.

An integer satisfying either of the last two bullet points has form

Because m and n are greater than 2, we have seen that $\phi(m)$ and $\phi(n)$ are:

Thus:

Because $m \perp n$, we have: $\phi(mn) =$

Let $a \perp mn$ be given. We will show a is not a primitive root of mn.

We compute

$a^{\phi(mn)/2} \equiv$

$a^{\phi(mn)/2} \equiv$

and so, since:

$a^{\phi(mn)/2} \equiv$

This shows that the order of a is less than:

Thus a is not a primitive root. $\square$

A. **Lifting Lemma.** This lemma helps us "lift" primitive roots to higher powers.

Lifting Lemma. Let n be a positive integer and p prime.

Let r be a primitive root of p satisfying

Then r is automatically a primitive root of p^n.

Proof. The order of r modulo p^n is a divisor of

These divisors can be split into

- either:
- or:

The given congruence asserts that the order of r modulo p^n is not

Therefore the order of r modulo p^{n+1} is of form

Our goal is then to show it must be the case:

By definition of order modulo p^{n+1} we have

which, by reducing the modulus to a divisor, implies

and then apply Fermat's Theorem $a^p \equiv a \mod p$ we have

But r is a primitive root of p and $d \mid p-1$, and thus:

Hence r is a primitive root of p^{n+1}.

□

B. **Prime Squared.** We show the square of a prime has a primitive root.

Theorem. Let p be prime. Then p^2 has a primitive root.

Our proof will show that, if r is a primitive root of p, then at least one of r or $r+p$ is a primitive root of p^2.

Proof. By the lifting lemma with $n = 2$ so:

we need only find a primitive root r of p so

Because p is prime, it has a primitive root r.

Suppose we weren't lucky and:

Then consider $r+p$, which is also a primitive root of p, because:

By the binomial theorem, and that terms involving $p^{\geqslant 2}$ will vanish

$(r+p)^{p-1} \equiv$

but this is not congruent to 1 modulo p^2 because $r \perp p$ implies

□

C. **Prime Powers.** The next results can be proven from the lifting lemma.
We will not prove them, but merely state them.

Theorem. Let p be an odd prime and n be a positive integer. Then

- p^n has a primitive root, namely
- $2p^n$ has a primitive root, namely

This completes our analysis of positive integers having primitive roots.