Example 1. Find an integer r that is a primitive root for all integers of form $2 \cdot 5^n$.

Solution. First, by inspection the primitive roots of 5 are

The lifting lemma says primitive root r of p will lift to primitive root of p^2 iff

In our case we confirm

A primitive root of $[\text{odd prime}]^2$ is automatically a primitive root of $[\text{odd prime}]^{\geqslant 2}$.

A primitive root r of $[\text{odd prime}]^n$ is a primitive root of $2 \cdot [\text{odd prime}]^n$ iff:

Therefore

A. **Quadratic Congruences.** Consider a **quadratic congruence** modulo a prime.

$x^2 + x + 5 \equiv 0 \mod 7$

If we blindly applied the quadratic formula we would obtain

$x =$

But we want **integer** solutions.

Instead we interpret the quadratic formula in the world of modular arithmetic.

$x \equiv$

Let p be an:

Let a, b, and c be integers so that:

Consider the quadratic congruence

$ax^2 + bx + c \equiv 0 \mod p$

and denote its discriminant $D =$

The quadratic congruence has a solution modulo p if and only if

which means

in which case $ax^2 + bx + c \equiv 0 \mod p$ has solutions

Example 2. Let p be an odd prime. Prove the following always has a solution.

$10x^2 + 9x + 2 \equiv 0 \mod p$

Proof. The quadratic formula for $ax^2 + bx + c$ is useless if

Thuse we separate out this instance.

Case 1. $p =$

Then our congruence becomes

Case 2. p

We calculate the discriminant

$D = b^2 - 4ac =$

Then D is a quadratic residue, because it has a square–root modulo p

Thus the quadratic congruence has a solution, provided by the quadratic formula.
□

B. **Euler's Criterion.** Let us list all quadratic residues modulo 7.

We do this by squaring all integers from $[0 \ldots 6]$ and reducing modulo 7.

Euler developed an alternate means for detecting quadratic residues.

Let p be an:

Let a be an integer such that:

Then a is a quadratic residue modulo p if and only if

Proof. $\Longrightarrow$: Assume a is a quadratic residue. Then

Because $a \perp p$ it follows that also:

Then:

$\Longleftarrow$: Assume $a^{(p-1)/2} \equiv 1 \mod p$.

Select a primitive root r of p.

Because $a \perp p$ it follows that

We will lastly show that:

in which case: $\sqrt{a} \equiv$

Okay, let's rewrite

$a^{(p-1)/2} \equiv 1 \mod p$

Thus the order $p-1$ of the primitive root r must divide:

□