Example 1. Let p be an odd prime and $a \perp p$.

Prove that a is not a quadratic residue of p if and only if

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

Solution. We begin with a lemma.

Lemma. Let $a \perp p$ be given. Then

Proof. Fermat's Theorem implies that $x = a^{(p-1)/2}$ solves

By Lagrange, a quadratic congruence modulo p has $\leqslant 2$ incongruent solutions.

In this case, those solutions evidently are: $x \equiv$

□

We apply **Euler's criterion**, which said $a \perp p$ is a quadratic residue of p iff

We apply the criterion to the two cases given in the lemma.

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

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

□

A. **Legendre Symbol.** We introduce a symbol for identifying quadratic residues.

Let p be:

and a be an integer such that:

Then the **Legendre symbol** is defined by

$(a/p) =$

This is read "a over p".

By Euler's criterion, and the subsequent example, if p is an odd prime then

$(a/p) \equiv$

For example we compute

$(1/7) =$

$(2/7) =$

$(3/7) =$

$(4/7) =$

$(5/7) =$

$(6/7) =$

Let us establish some useful properties.

Let p be prime. Then

$(-1/p) \equiv$

Proof. We actually proved this, eons ago. □

Let p be prime and a and b be relatively prime to p.

Then the Legendre symbol $(ab/p) =$

Proof. If $p = 2$ this is obvious. If p is an odd prime we compute

$(ab/p) \equiv$

□

Example 2. Calculate the Legendre symbol $(-133/137)$.

Solution. 137 is indeed prime, which we could confirm if needed.

Now we apply rules of Legendre symbols.

$(133/137) =$

Example 3. Prove there are infintely many primes of the form $4k + 1$.

Solution. Suppose towards a contradiction there are finitely many such primes

and consider the integer

$N =$

Let p be a prime divisor of N.

We will show that

whence we will obtain the contradiction

Let's prove that p has the desired form. Because $p \mid N$ it follows

Thus $(-1/p) =$

Based on the last page, either

which means p is in the list $2, p_1, \ldots, p_r$. $\square$

B. **Legendre and Primitive Roots.** We relate Legendre symbols to primitve roots.

Let p be an odd prime and select a

Then in the list

the quadratic residues are exactly those

As r is a primitive root the given list is congruent mod p after reordering to

and thus as a consequence among the integers $[1 \ldots p-1]$ exactly

Proof. First observe that, because r is a primitive root

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

Thus r is **not** a quadratic residue, so

$(r/p) =$

Now let integer k from $[1 \ldots p-1]$ be given. Then

$(r^k/p) =$

This is 1 if and only if:

□