Number Theory Homework.

We have proven the following in class.

Theorem 1. *If p is an odd prime, and $p \nmid a$ then the congruence*

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

has a solution if and only if the ***discriminant***

$$D = b^2 - 4ac$$

is a perfect square modulo p. $\square$

Proposition 2. *If the discriminant, D, of $ax^2 + bx + c$ is zero, then for some integer r*

$$ax^2 + bx + c \equiv a(x - r)^2 \mod p$$

Problem 1. Prove this. *Hint:* Complete the square. See class notes. $\square$

Definition 3. If p is an odd prime and $\gcd(a, p) = 1$, then a is a ***quadratic residue*** modulo p iff $x^2 \equiv a \mod p$ has a solution. Otherwise a is a ***quadratic non-residue***. $\square$

Definition 4. If p is an odd prime and a is an integer, then the ***Legendre symbol*** is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p \mid a; \\ +1, & a \text{ is a quadratic residue modulo } p; \\ -1, & a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

To be a little more explict about the if $p \nmid a$, then $\left(\frac{a}{p}\right) = 1$ means that a has a square root modulo p, and $\left(\frac{a}{p}\right) = -1$ means that a does not have a square modulo p. We start with some results that follow directly from the definition.

Proposition 5. *If p is a odd prime, then*

$$a \equiv b \mod p \qquad \Longrightarrow \qquad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Problem 2. Prove this. $\square$

Proposition 6. *If p is an odd prime and $p \nmid a$, then*

$$\left(\frac{a^2}{p}\right) = 1$$

Problem 3. Prove this. $\square$

The following gives a direct method for determining if a is a quadratic residue modulo p.

Theorem 7 (Euler's Criterion). *If p is an odd prime and $p \nmid a$, then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$

We give some applications before giving the proof.

Proposition 8. *Let p be an odd prime.*

(a) If $p \equiv 1 \mod 4$, then -1 is a quadratic residue of p.
(b) If $p \equiv 3 \mod 4$, then -1 is a quadratic non-residue of p.

In terms of the Legendre symbol

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, & p \equiv 1 \mod p \\ -1, & p \equiv 3 \mod p. \end{cases}$$

Problem 4. Prove this. *Hint:* If $p = 4k+1$, then $(p-1)/2 = 2k$ and therefore $(-1)^{(p-1)/2} = (-1)^{2k} = 1$. If $p = 4k+3$, then $(p-1)/2 = 2k+1$ so that $(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$ and use Theorem 7. □

As anther application

Proposition 9. *If p is an odd prime then for any integers, the Legendre symbol satisfies*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Problem 5. Prove this. *Hint:* If either a or b is divisible by p then both sides of the the equation are zero. If p does not divide either a or b then $(ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2}$ and we can again use Theorem 7. □

We now use Gauss' Theorem on the existence on primitive roots to prove Euler's Criterion. Let p be an odd prime. Recall that g is a ***primitive element*** modulo p is $\operatorname{ord}_p(g) = \phi(p)$ where $\operatorname{ord}_p(a)$ is the smallest positive k such that $g^k \equiv 1 \mod p$. As $\phi(p) = p-1$ we can summarize that g is a primitive element modulo p if and only if $g^{p-1} \equiv 1 \mod p$, and if k is any positive integer with $g^k \equiv \mod p$, then $(p-1) \le k$. We have also shown that if $g^m \equiv 1 \mod p$, then $(p-1) \mid m$.

Proposition 10. *Let p be an odd prime and g a primitive element modulo p. Then if $p \nmid a$, there is a $j \ge 0$ such that $a \equiv g^j \mod p$. That is every nonzero element of $\mathbb{Z}_p$ is a power of g in $\mathbb{Z}_p$.*

Proof. No two of the elements of $1 = g^0, g, g^2, g^3, \ldots, g^{p-2}$ are congruent modulo (for it $g^i \equiv g^j \mod p$ with $0 \le i < j \le (p-2)$ then we can cancel to get $1 \equiv g^{j-i} \mod p$ which would contradict that $g^k \not\equiv 1 \mod p$ when $1 < k < (p-1)$). Thus the set $\{g^0, g, g^2, g^3, \ldots, g^{p-2}\}$ is a complete set of nonzero residues modulo p. As $a \not\equiv 0 \mod p$ this implies is congruent to one of the elements of $\{g^0, g, g^2, g^3, \ldots, g^{p-2}\}$ as required. □

Lemma 11. *If g is a primitive element modulo p where p is an odd prime, then if $g^i \equiv g^j \mod p$, then i and j are either both even or both odd. (Or what is the same thing $i \equiv j \mod 2$.)*

Problem 6. Prove this. *Hint:* If $i = j$ there is nothing to prove, so assume that $i < j$. Then $g^i \equiv g^j \mod p$ implies $g^{j-i} \equiv 1 \mod p$. This implies $(p-1) \mid (j-i)$. But p is odd, so that $(p-1)$ is even. Thus $(p-1) \mid (j-i)$ implies $2 \mid (j-i)$. $\square$

Proposition 12. *Let g be a primitive element for the odd prime p. Then the element g^j is a quadratic residue if and only if j is even. In terms of the Legendre symbol this can be stated as*

$$\left(\frac{g^j}{p}\right) = (-1)^j.$$

Proof. If j is even, say $j = 2k$, then $g^j = g^{2k} = (g^k)^2$ and so g^k is a square root of g^j modulo p and therefore g^j is a quadratic residue modulo p.

Conversely if g^j is a quadratic residue modulo p, then $g^j \equiv a^2$ for some integer a. By Proposition 10 $a \equiv g^i$ for some integer i. Therefore

$$g^j \equiv a^2 \equiv (g^i)^2 \equiv g^{2i} \mod p.$$

As $2i$ is even, Lemma 11 implies j is even. $\square$

Lemma 13. *If g is a primitive root for the odd prime p, then*

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

Problem 7. Prove this. *Hint:* Let $b = g^{(p-1)/2}$. Then

$$b^2 \equiv \left(g^{(p-1)/2}\right)^2 \equiv g^{(p-1)} \equiv 1 \mod p.$$

Thus b is a solution to the congruence $x^2 \equiv 1 \mod p$. But we have seen this only has the two solutions $x \equiv 1 \mod p$ and $x \equiv -1 \mod p$. So to complete the proof, it is enough to show $b = g^{(p-1)/2} \not\equiv 1 \mod p$, which follows from the definition of g being a primitive root. $\square$

Problem 8 (Proof of Euler's Criterion.). Prove Theorem 7. *Hint:* Let p be an odd prime and $p \nmid a$. By Gauss' theorem on the existence of primitive roots we know there is a primitive root g for p. By Proposition 10 we have that $a \equiv g^j \mod p$ for some j.

(a) Show

$$\left(\frac{a}{p}\right) = \left(\frac{g^j}{p}\right) = (-1)^j.$$

Hint: Propositions 5 and 12.

(b) Show

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

Hint:

$$a^{(p-1)/2} = \left(g^j\right)^{(p-1)/2} = \left(g^{(p-1)/2}\right)^j$$

and by Proposition 13 $g^{(p-1)/2} \equiv -1 \mod p$.

(c) Combine the last two steps to conclude

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

which is the statement of Euler's Criterion. □

We now give two more basic results about quadratic residues which we will not prove.

Theorem 14 (Euler)**.** *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p = 8k \pm 1, \\ -1, & p = 8k \pm 3. \end{cases}$$

That is if $p \equiv \pm 1 \mod 8$, then 2 is a quadratic residue of p and if $p \equiv \pm 2 \mod 8$, then 2 a not a quadratic residue of p. Sometimes this is written

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1 \mod 8, \text{ or } p \equiv 7 \mod 8; \\ -1, & p \equiv 3 \mod 8, \text{ or } p \equiv 5 \mod 8. \end{cases}$$

Finally here is the deepest result we have seen in this course. It is due to Gauss.

Theorem 15 (Quadratic Reciprocity)**.** *Let p and q be odd primes. Then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

unless p and q are both of the form $4k+3$ in which case

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

With the rules above we can compute Legendre symbol without two much trouble, as we have seen in class.