# CLASS 24, GIVEN ON 11/15/2010, FOR MATH 25

## 1. Quadratic congruences: Introduction

We conclude this class by considering the analogue of a classical problem from secondary school. Consider a quadratic polynomial in a single variable; say $f(x) = ax^2 + bx + c$. A typical and important question is to determine the roots of this polynomial; ie, the values of $x$ for which $f(x) = 0$. When we think of $x$ as being a real or complex variable, the answer is given by the quadratic equation:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Since this is a number theory class, we might be interested in the same equation, except now we think of $x$ being an element of the integers mod $n$. Instead of starting from scratch, we might ask whether the quadratic equation works when we think of $x$ as a variable in $\mathbb{Z}/n\mathbb{Z}$. Addition, subtraction, and multiplication are all defined for $\mathbb{Z}/n\mathbb{Z}$. Division is defined if we are dividing by a unit of $\mathbb{Z}/n\mathbb{Z}$, so we might run into difficulties if 2 or $a$ are not units mod $n$. But the biggest problem is figuring out what to make of the $\sqrt{b^2 - 4ac}$ term.

When we think of $x$ as a real or complex variable, then we simply accept the fact that square roots of real or complex numbers exist, as complex numbers. But what if we are in $\mathbb{Z}/n\mathbb{Z}$? Then it is not so clear that square roots exist, and even if they do, we want an effective way to calculate them. After all, a square root in $\mathbb{Z}/n\mathbb{Z}$ will be represented by a congruence class of $\mathbb{Z}/n\mathbb{Z}$ so we should have a way to determine what that congruence class actually is. In other words, given an integer $a$, we want to know when $x^2 \equiv a \mod n$ has a solution, and if it does, how to find all solutions.

Of course, since this is a finite problem we can use the naive method and just use trial and error. But this takes a long time and is not particularly efficient. Furthermore, a trial and error method does not provide any enlightening theoretical information about the numbers in $\mathbb{Z}/n\mathbb{Z}$ which are square roots and the numbers which are not square roots. For instance, if $a$ is a real number, then we know $\sqrt{a}$ is real exactly when $a \geq 0$. We want some sort of similar, (relatively) easy to state condition for determining when $x^2 \equiv a \mod n$ has a solution. The theory is simplest when we restrict ourselves to elements in $U_n$; in practice this is not too harmful because we will mostly be interested in the case when $n$ is prime.

**Definition 1.** *An element of $U_n$ is called a* quadratic residue *mod $n$ if the congruence equation $x^2 \equiv a \mod n$ has a solution in $U_n$. The set of quadratic residues in $U_n$ is frequently denoted $Q_n$. An element of $U_n$ which is not a quadratic residue is called a* quadratic non-residue.

**Examples.**

- Let $n = 5$. The set of quadratic residues is $1, 4 \mod 5$, because $1^2 \equiv 1 \mod 5, 2^2 \equiv 4 \mod 5, 3^2 \equiv 4 \mod 5, 4^2 \equiv 1 \mod 5$. So one way to compute $Q_n$ is to simply square every element of $U_n$ and look at the results. Notice that we already see that not all elements of $U_n$ have to be quadratic residues.
- Let $n = 8$. The set of quadratic residues is then just $1 \mod 8$, because $1^2, 3^2, 5^2, 7^2 \equiv 1 \mod 8$.

The following proposition is of fundamental importance. We will shortly see a stronger version of this proposition which holds when $n$ is prime.

**Proposition 1** (Lemma 7.2)**.** *$Q_n$ is a subgroup of $U_n$.*

*Proof.* Let $a, b \in Q_n$, and let $x_a, x_b$ be two elements of $U_n$ which square to $a, b$. Then $x_a x_b \in U_n$, and its square is $(x_a x_b)^2 = x_a^2 x_b^2 = ab$, so $ab$ is also in $Q_n$. Clearly the identity element 1 is in $Q_n$, since $1^2 = 1$, and finally, if $x_a^2 = a$, then $(x_a^{-1})^2 = a^{-1}$, and since $x_a^{-1} \in U_n$, $a^{-1} \in Q_n$. These three properties confirm the fact that $Q_n$ is a subgroup of $U_n$. □

## 2. When $n = p$: introduction and notation

A common theme in this class is that when asking questions about integers mod $n$, it is frequently best to start with the case $n = p$, and then work our way to prime powers, and then to general $n$. So we will consider quadratic residues mod primes $p$. We first define a convenient notation for indicating when a number is a quadratic residue mod $p$. From now on, we will let $p$ be an odd prime; when $p = 2$ we already know that 1 is a quadratic residue mod 2.

**Definition 2.** *Let $p$ be an odd prime, and let $a$ be any integer. The* Legendre symbol *of $a$ mod $p$ is defined to be*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in Q_p, \\ -1 & \text{if } p \nmid a, a \notin Q_p, \\ 0 & \text{if } p \mid a. \end{cases}$$

The notation might see a little odd at first, because it looks like the number $a/p$ with parentheses around it. As a matter of fact, this notation is ambiguous, but the context should make it clear whether we mean the number $a/p$ or the Legendre symbol $\left(\frac{a}{p}\right)$.

**Example.** Let $p = 5$. Then

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \equiv 1, 4 \mod 5, \\ -1 & \text{if } a \equiv 2, 3 \mod 5, \\ 0 & \text{if } 5 \mid a. \end{cases}$$

There is a nice interaction between the values of the Legendre symbol and primitive roots mod $p$. This proposition also gives some indication why the values of the Legendre symbol are what they are.

**Proposition 2** (Lemma 7.3, Corollary 7.4)**.** *Let $g$ be a primitive root mod $p$. Then $a \equiv g^i \mod p$ is a quadratic residue if and only if $i$ is even. In particular, there are $(p-1)/2$ quadratic residues mod $p$ and $(p-1)/2$ quadratic non-residues mod $p$, and*

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

*Proof.* We want to know when $x^2 \equiv a \equiv g^i \mod p$ has a solution. This has a solution if and only if there is some integer $k$ such that $g^k = x$ solves the above; in other words, when $g^{2k} \equiv g^i \mod p$ has a solution $k$. This has a solution if and only if $g^{2k-i} \equiv 1 \mod p$ has a solution, which has a solution if and only if $(p-1) \mid (2k - i)$, or $2k \equiv i \mod (p-1)$, has a solution, where $k$ is the variable. And we know this has a solution if and only if $\gcd(2, p-1) = 2$ divides $i$, which is the same as saying that $i$ is even. Notice that the parity of $i$ is independent of the actual choice of $i$, because $p - 1$ is even. (For instance,

even though $3 \equiv 2^3 \equiv 2^{11} \mod 8$, so that we could have chosen $i = 3$ or 11, their parity is identical because 4 is even, and adding an even number to an integer $i$ does not change the parity of $i$.)

For the other parts of the proposition, of the $p-1$ elements $g \mod p, g^2 \mod p, \ldots, g^{p-1} \mod p$, exactly $(p-1)/2$ of them have exponents which are even, and exactly $(p-1)/2$ have exponents which are odd. And $\left(\frac{g^i}{p}\right) = (-1)^i$ is true because $\left(\frac{g^i}{p}\right) = 1$ if and only if $i$ is even, if and only if $(-1)^i = 1$. □

**Example.** Let $p = 7$. A primitive root mod 7 is 3. We have

$$3^1 \equiv 3 \mod 7, 3^2 \equiv 2 \mod 7, 3^3 \equiv 6 \mod 7, 3^4 \equiv 4 \mod 7, 3^5 \equiv 5 \mod 7, 3^6 \equiv 1 \mod 7.$$

By the above proposition, $2, 4, 1 \mod 7$ are the quadratic residues mod 7, and $3, 6, 5 \mod 7$ are the quadratic non-residues mod 7.

From a computational point of view, the previous proposition is not very useful for determining the actual elements in $Q_p$, because it involves finding a primitive root (which is nontrivial). It will no slower to simply square all the elements in $U_p$. However, the value of this proposition is not in its computational use but rather in its theoretical use.

Another reason for defining the values of the Legendre symbol to be $0, \pm 1$ is because of the following corollary, which is a stronger version of the fact that $U_p$ is a subgroup:

**Corollary 1** (Theorem 7.5)**.** *Let $a, b$ be any integers. Then*

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

*Proof.* First, suppose that either $p \mid a$ or $p \mid b$. Then one of the terms on the left hand side is equal to 0, and as $p \mid ab$, the right hand side equals 0, so the corollary is true in this case. Now suppose $p \nmid a, b$. Then using the previous proposition, if we let $g$ be a primitive root mod $p$ and $a \equiv g^i \mod p, b \equiv g^j \mod p$ for two integers $i, j$, then

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)^i(-1)^j = (-1)^{i+j} = \left(\frac{ab}{p}\right),$$

where in the last equality we used the fact that $ab \equiv g^{i+j} \mod p$. □

This result can be rephrased in various ways. For instance, this result tells us that the product of two QRs (quadratic residues) is still a QR, because $1 \cdot 1 = 1$, which we already knew since $Q_p$ is a subgroup. But it also tells us that the product of two non-QRs (quadratic non-residues) is a quadratic residue, since $-1 \cdot -1 = 1$, and it also tells us that a product of a QR with a non-QR is a non-QR.

There is also an interpretation of this result in terms of algebra. Recall that an isomorphism is a function $f : G \to G'$ such that $f$ is a bijection, and $f(g_1 g_2) = f(g_1)f(g_2)$. While it is not true that the Legendre symbol, which gives a map

$$\left(\frac{\cdot}{p}\right) : U_p \to \{\pm 1\},$$

is an isomorphism (simply because it is not a bijection), it does have the property that $f(g_1 g_2) = f(g_1)f(g_2)$. This map is called a *homomorphism* of $G$ to $G'$, so in this terminology the Legendre symbol is a homomorphism from $U_p$ to $\pm 1$.

**Example.** This corollary allows us to reduce the computation of a Legendre symbol $\left(\frac{a}{p}\right)$ by factoring $a$. For instance, suppose we want to calculate $\left(\frac{12}{13}\right)$. Since $12 = 2^2 \cdot 3$, we have

$$\left(\frac{12}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{3}{13}\right),$$

where in the last equality we use the fact that $\left(\frac{2}{13}\right)^2 = 1$, since $(\pm 1)^2 = 1$. Since $4^2 \equiv 3 \mod 13$, $\left(\frac{12}{13}\right) = \left(\frac{3}{13}\right) = 1$.

This example makes it clear that one possible approach to computing $\left(\frac{a}{p}\right)$ is to figure out how to compute $\left(\frac{a}{p}\right)$ when $a$ itself is either an odd prime, 2, or $-1$. Before we investigate this problem, we will prove another proposition which provides another way of computing the Legendre symbol, which will be useful for theoretical purposes.

**Proposition 3** (Theorem 7.6)**.** *Let $a$ be any integer. Then*

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

*Proof.* If $p \mid a$, then $a^{(p-1)/2} \equiv 0 \mod p$, and also $\left(\frac{a}{p}\right) \equiv 0 \mod p$, so the proposition is clear in this case. So suppose $p \nmid a$.

Since $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1 \mod p$, we know that $a^{(p-1)/2} \equiv \pm 1 \mod p$. Let $g$ be any primitive root mod $p$. Recall that we know $a$ is a quadratic residue mod $p$ if and only if $a \equiv g^i \mod p$ for an even integer $i$. Plugging in $a \equiv g^i$ into $a^{(p-1)/2}$, we get

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

This is equal to $1 \mod p$ exactly when $(p-1) \mid i(p-1)/2$. Clearly this is the case if and only if $i$ is even. Therefore, assuming $p \nmid a$, $a^{(p-1)}/2 \equiv 1 \mod p$ if and only if $a$ is a quadratic residue mod $p$, as desired. □

**Example.** Let $p = 7$. Then $(p-1)/2 = 3$, so to determine whether $a \mod p$ is a quadratic residue mod 7, we can calculate $a^3 \mod p$. For example, $2^3 \equiv 1 \mod 7, 3^3 \equiv -1 \mod p$, so $2 \in Q_p$ while $3 \notin Q_p$.

In practice, calculating $a^{(p-1)/2} \mod p$ might be slightly faster than the brute force method of listing all the squares mod $p$ by calculating $1^2, 2^2, \ldots \mod p$, but it can still take a while, if $p$ is reasonably large. For instance, it would be hard to calculate $a^{(p-1)/2}$ mod $p$ by hand if $p$ were a three digit number.

These general properties of the Legendre symbol and quadratic residues will be used in the next class, when we start looking for ways to rapidly compute the Legendre symbol. We will start with the symbols $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, and then think about the more general symbol $\left(\frac{q}{p}\right)$, where $q$ is an odd prime.