QUADRATIC RESIDUES

LECTURE NOTES: MATH 422, CSUSM, SPRING 2009. PROF. WAYNE AITKEN

When is an integer a square modulo p? When does a quadratic equation have roots modulo p? These are the questions that will concern us in this handout.

1. The Legendre Symbol

The *Legendre Symbol* is a notation developed by Legendre for indicating whether or not an integer is a square or not. It uses values $0, 1, -1$ to indicate three basic possibilities. Before discussing the Legendre Symbol, we first define some notation for $\mathbb{F}_p$:

Definition 1. Let $b \in \mathbb{F}_p$ where p is a prime. We call b a *square* if there is an element $a \in \mathbb{F}_p$ such that $b = a^2$. Non-zero squares are also called *quadratic residues*.

The set of quadratic residues is written $(\mathbb{F}_p^\times)^2$ or Q_p. We will see later that $(\mathbb{F}_p^\times)^2$ is closed under multiplication (in other words, it is a subgroup of $\mathbb{F}_p^\times$).

We are most interested in the case where $p \neq 2$. When $p = 2$ the situation is very easy: both elements are squares.

Definition 2. If $a \in \mathbb{Z}$ then the class a in $\mathbb{Z}_m$ is called the *image of* a in $\mathbb{Z}_m$. This terminology is based on the function $x \mapsto \overline{x}$ called the *canonical homomorphism* $\mathbb{Z} \to \mathbb{Z}_m$.

Definition 3. Let $a \in \mathbb{Z}$, and let p be an odd prime. Then the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be $0, +1$, or -1.

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 0 if the image of a in $\mathbb{F}_p$ is the zero element. This case occurs if and only if $p \mid a$.

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be $+1$ if the image of a in $\mathbb{F}_p$ is a quadratic residue. In other words, it is $+1$ if and only if $\overline{a} \in (\mathbb{F}_p^\times)^2$.

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be -1 in any other case. In other words, it is -1 whenever the image of a in $\mathbb{F}_p$ is not a square.

Remark. The values $0, +1, -1$ are usually thought of as integers, but they can be thought of as elements of $\mathbb{F}_p$ whenever it is convenient, or even as abstract symbols whose multiplication table is defined in the usual way.

Likewise, the symbol $\left(\frac{a}{p}\right)$ is usually defined for $a \in \mathbb{Z}$, but one can also consider it as defined for $a \in \mathbb{F}_p$.

Exercise 1. Calculate $\left(\frac{a}{11}\right)$ for all $0 \le a < 11$ directly from the definition (without using results developed below).

Date: Spring 2008, Spring 2009. Modified April 9, 2009.

2. Even and Odd Powers of Generators

Given a generator g for $\mathbb{F}_p^\times$, the quadratic residues are simply the even powers of g and the quadratic nonresidues are the odd powers.

Theorem 1. *Suppose p is an odd prime and let g be a generator of $\mathbb{F}_p^\times$. If e is even then g^e is a quadratic residue. If e is odd then g^e is not a square.*

Proof. If e is even, then $e = 2k$ for some k. Thus $g^e = g^{2k} = \left(g^k\right)^2$. Hence g^e is a square. It is not zero, so it is a quadratic residue.

Suppose e is odd. We will show g^e cannot be a square by assuming otherwise, and deriving a contradiction. Suppose that $g^e = b^2$ for some $b \in \mathbb{F}_p$. Since g is a generator and b is nonzero, we have $b = g^k$ for some k. Thus $g^e = g^{2k}$. Since the order of g is $p-1$ this implies that $e \equiv 2k$ modulo $p-1$. Observe that $2 \mid (p-1)$ since p is odd. Thus $e \equiv 2k$ modulo 2. In other words, $e \equiv 0$ modulo 2, contradicting the assumption that e is odd. □

Corollary 2. *Suppose p is an odd prime and let g be a generator of $\mathbb{F}_p^\times$. If a is a quadratic residue then $a = g^e$ for an even e. If a is a quadratic nonresidue then $a = g^e$ for an odd e.*

Proof. Since g is a generator, we can write any nonzero a as g^e for some integer e. If a is a quadratic residue, then e odd contradicts the above theorem, so e is even. If a is a quadratic nonresidue then e even contradicts the above theorem, so e is odd. □

Corollary 3. *Suppose p is an odd prime. Then there are $(p-1)/2$ quadratic residues, and $(p-1)/2$ quadratic nonresidues in $\mathbb{F}_p^\times$.*

Proof. Let g be a generator. Every element of $\mathbb{F}_p^\times$ can be written uniquely as g^e where $0 \le e < p-1$. Half of such e are even and the other half are odd. □

Corollary 4. *Suppose p is an odd prime and g is a generator of $\mathbb{F}_p^\times$. Then g is not a square.*

Proof. Observe that $g = g^1$ and $e = 1$ is odd. □

3. Euler's Critera and Formula for the Legendre Symbol

We begin with a simple lemma:

Lemma 5. *Suppose p be an odd prime and let g be a generator (primitive root) of $\mathbb{F}_p^\times$. Then*

$$g^{(p-1)/2} = -1.$$

Proof. Recall that g has order $p-1$ since it is a generator. Let $a = g^{(p-1)/2}$. So

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

Since $a^2 = 1$, the element a is a root of the polynomial $x^2 - 1$. Thus a is 1 or -1. However, $a = g^{(p-1)/2}$ is not 1 since the order of g is $p-1$ which is greater than $(p-1)/2$. Therefore, $a = -1$. □

Theorem 6 (Euler's Criterion)**.** *Let p be an odd prime. If $a \in \mathbb{F}_p^\times$ then $a^{(p-1)/2}$ is either* 1 *or* -1*. Furthermore, a is a quadratic residue if and only if $a^{(p-1)/2} = 1$.*

Proof. Let g be a generator of $\mathbb{F}_p^\times$. Write $a = g^e$. Then Lemma 5 gives us that

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

If e is even then a is a quadratic residue, and the above simplifies to 1. If e is odd then a is a quadratic nonresidue and the above simplifies to -1. The result follows easily. □

Theorem 7. *If p is an odd prime and a is an integer, then*

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

Proof. There are three cases to consider.

First suppose that $\left(\frac{a}{p}\right) = 0$. By definition of the Legendre Symbol, $a \equiv 0 \bmod p$. Thus Thus, $a^{(p-1)/2} \equiv 0 \bmod p$. The result follows.

Next suppose that $\left(\frac{a}{p}\right) = +1$. By definition of the Legendre Symbol, the image of a in $\mathbb{F}_p^\times$ is a quadratic residue. The result follows from Theorem 6.

Finally, suppose that $\left(\frac{a}{p}\right) = -1$. By definition of the Legendre Symbol, the image of a in $\mathbb{F}_p^\times$ is a quadratic nonresidue. The result follows from Theorem 6. □

Exercise 2. Calculate $\left(\frac{a}{11}\right)$ for all $0 \le a < 11$ using Theorem 7. Compare your answer to Exercise 1.

4. Basic properties of the Legendre Symbol

Here are some very useful properties to know in order to calculate $\left(\frac{a}{p}\right)$. Throughout this section, let p be an odd prime.

Property 1. *If $a \equiv r \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$. In particular, $\left(\frac{p}{p}\right) = 0$.*

Proof. If $a \equiv r \bmod p$ then a and r have the same image in $\mathbb{F}_p$. Since Definition 3 depends only on the images in $\mathbb{F}_p$ the result follows. □

Property 2. *If $a \not\equiv 0 \bmod p$ then $\left(\frac{a^2}{p}\right) = 1$. In particular, $\left(\frac{1}{p}\right) = 1$.*

Proof. The image of a^2 in $\mathbb{F}_p^\times$ is trivially a square. □

Property 3. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. *In particular:*

$$\text{If } p \equiv 1 \bmod 4, \quad \text{then } \left(\frac{-1}{p}\right) = 1.$$

$$\text{If } p \equiv 3 \bmod 4, \quad \text{then } \left(\frac{-1}{p}\right) = -1.$$

Proof. The first equation follows from Theorem 7.

Now we calculate $(-1)^{(p-1)/2}$ in each case.

if $p \equiv 1 \bmod 4$, then $p-1 = 4k$ for some k. Thus $(p-1)/2 = 2k$. In this case $(-1)^{(p-1)/2} = (-1)^{2k} = 1$.

If $p \equiv 3 \bmod 4$, then $p - 3 = 4k$ for some k. Thus $p - 1 = 4k + 2$, and $(p-1)/2 = 2k + 1$. In this case $(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$. □

Property 4. *For $a, b \in \mathbb{Z}$ we have* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof. This follows from Theorem 7:

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

Since all the numbers on the left and right are ± 1 we can replace congruence with equality (1 and -1 are distinct modulo p since $p > 2$). □

Exercise 3. Use Property 4 to show that the product of two quadratic residues is a quadratic residue. Thus the set $U_p = (\mathbb{F}_p^\times)^2$ of quadratic residues is closed under multiplication. (In fact, it is a subgroup of $\mathbb{F}_p^\times$.)

Exercise 4. Use Property 4 to show that if $a, b \in \mathbb{F}_p^\times$ are units such that one of them is a quadratic residue but the other is not, then ab is *not* a quadratic residue.

Exercise 5. Use Property 4 to show that if $a, b \in \mathbb{F}_p^\times$ are units that are both non-quadratic residues, then ab is a quadratic residue.

Remark. If you know abstract algebra, you will observe that Property 4 tells us that the map $\overline{a} \mapsto \left(\frac{a}{p}\right)$ is a group homomorphism $\mathbb{F}_p^\times \to \{\pm 1\}$. The kernel of this homomorphism is the subgroup $(\mathbb{F}_p^\times)^2$ of quadratic residues. The quadratic residues form a subgroup, but the non-quadratic residues only form a coset.

Exercise 6. Give a multiplication table for the group $Q_{11} = (\mathbb{F}_{11}^\times)^2$. Hint: it should have 5 rows and columns.

5. Advanced properties of the Legendre Symbol

The properties of this section will be stated without proof.

Property 5. *Let p be an odd prime, then $\left(\frac{2}{p}\right)$ is determined by what p is modulo 8.*

$$\text{If } p \equiv 1 \text{ or } p \equiv 7 \mod 8, \quad \text{then } \left(\frac{2}{p}\right) = 1.$$

$$\text{If } p \equiv 3 \text{ or } p \equiv 5 \mod 8, \quad \text{then } \left(\frac{2}{p}\right) = -1.$$

The following is a celebrated theorem of Gauss.

Property 6 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Remark. As we discussed above, $\frac{p-1}{2}$ is even if $p \equiv 1 \bmod 4$, but is odd if $p \equiv 3 \bmod 4$. Similarly, for q. So $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even if either p or q is congruent to 1 modulo 4, but is odd if both are congruent to 3. So

$$\text{If } p \equiv 1 \text{ or } q \equiv 1 \bmod 4, \text{ then } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

$$\text{If } p \equiv 3 \text{ and } q \equiv 3 \bmod 4, \text{ then } \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Remark. Sometimes quadratic reciprocity is written as follows:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

6. Square roots

If $b^2 = a$ in a field F then b is called a *square root* of a. In this section we discuss a few basic results concerning square roots in $\mathbb{F}_p$ and other fields.

Recall that every field F has a multiplicative identity 1. The element $2 \in F$ is defined to be $1+1$. In some fields $2 = 0$, for example in $F = \mathbb{F}_2$. In other fields $2 \neq 0$. For example, if $F = \mathbb{R}$ or if $F = \mathbb{F}_p$ with p an odd prime then $2 \neq 0$. In this handout we focus mainly on fields where $2 \neq 0$.

Lemma 8. *Let F be a field where $2 \neq 0$. In such a field, $b \neq 0$ implies $b \neq -b$.*

Proof. Suppose otherwise that, $b = -b$. Add b to both side giving $b + b = 0$. This implies $2b = 0$. But 2 is a unit, so $2^{-1}2b = 2^{-1}0$. We conclude $b = 0$, a contradition. □

Proposition 9. *Let F be a field where $2 \neq 0$. If $a \in F$ has a square root b then $-b$ is also a square root. Furthermore, $\pm b$ are the only square roots of a.*

Proof. Observe that $(-b)^2 = b^2 = a$. So the first statement follows.

Now we must show that $\pm b$ are the only square roots of a. First assume $b \neq 0$. Then by Lemma 8, b and $-b$ are two distinct solutions to $x^2 = a$. However, the polynomial $x^2 - a$ has at most two roots since its degree is two. So b and $-b$ are the only square roots.

Finally, consider the case where $b = 0$. So $-b = 0$ and $a = 0$ as well. Now suppose c is a non-zero square root of $a = 0$. Then c is a unit. Thus c^2 is a unit since units are closed under multiplication. This is a contradiction since $c^2 = a = 0$. So $b = 0$ is the only square root of a. □

Corollary 10. *Let F be a field where $2 \neq 0$. If $a, b \in F$ are such that $a^2 = b^2$ then $a = \pm b$.*

Proof. Let $c = a^2$. Then a and b are both square root of c. The result follows from the previous proposition. □

Proposition 11. *Let p be an odd prime. Then the number of square roots of a in $\mathbb{F}_p$ is given by the formula $(\frac{a}{p}) + 1$.*

Proof. There are three cases.

Case $(\frac{a}{p}) = 0$. By definition, $a = 0$, which has 0 for a square root. By Proposition 9 the square roots are ± 0. So 0 is the unique square root: there is exactly one square root. Observe that $(\frac{a}{p}) + 1 = 0 + 1 = 1$ gives the correct answer in this case.

Case $(\frac{a}{p}) = 1$. By definition, a is a non-zero square, so it has a square root b in $\mathbb{F}_p$. Clearly b is non-zero (otherwise a would be 0^2, but a is non-zero). By Proposition 9 and Lemma 8 there is exactly one other square root, namely $-b$. So there are two square roots. Observe that $(\frac{a}{p}) + 1 = 1 + 1 = 2$ gives the correct answer in this case.

Case $(\frac{a}{p}) = -1$. By definition, a is not a square in $\mathbb{F}_p$. So there are no roots. Observe that $(\frac{a}{p}) + 1 = -1 + 1 = 0$ gives the correct answer in this case. □

Exercise 7. Find all the square roots of all the elements of $\mathbb{F}_{11}$. For more practice try $\mathbb{F}_7$ or $\mathbb{F}_5$.

Exercise 8. For which primes p is it true that -1 has a square root? Find the first eight primes with this property. For a few of these, find square roots of -1.

7. Quadratic Equations in General

In this section we will consider quadratic equations in a field F with $2 \neq 0$. Define 4 to be 2^2. Since 2 is a unit, then 4 is also a unit in F. Thus 2^{-1} and 4^{-1} exist in F. We use fractional notation for units. For example, let $b/2$ denote $2^{-1}b$.

Lemma 12 (Completing the square: part 1)**.** *Suppose $b \in F$. Then*

$$x^2 + bx \;=\; (x + b/2)^2 - b^2/4.$$

Proof. Use the distributive law to simplify the right-hand side. ☐

Lemma 13 (Completing the square: part 2)**.** *Suppose $b, c \in F$. Then*

$$x^2 + bx + c \;=\; (x + b/2)^2 - (b^2 - 4c)/4.$$

Proof. Observe that

$$\begin{aligned} x^2 + bx + c &= \big((x + b/2)^2 - b^2/4\big) + c && \text{(Lemma 12)} \\ &= (x + b/2)^2 - \big(b^2/4 - 4c/4\big) \\ &= (x + b/2)^2 - (b^2 - 4c)/4. \end{aligned}$$

☐

Lemma 14 (Completing the square: part 3)**.** *Suppose $a, b, c \in F$ where $a \neq 0$. Then*

$$ax^2 + bx + c \;=\; a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a}.$$

Proof. First divide the given polynomial by a. In other words, let $b' = b/a$ and $c' = c/a$ and consider $x^2 + b'x + c'$. By Lemma 13,

$$x^2 + b'x + c' = (x + b'/2)^2 - (b'^2 - 4c')/4 = (x + b/(2a))^2 - (b^2/a^2 - 4c/a)/4.$$

Now multiply both sides by a and simplify. ☐

Remark. We call $b^2 - 4ac$ the *discriminant* of $ax^2 + bx + c$.

Theorem 15. *Suppose F is a field with $2 \neq 0$. Consider a quadratic polynomial $ax^2 + bx + c$ where $a, b, c \in F$ with $a \neq 0$. If $ax^2 + bx + c$ has a root in F then $b^2 - 4ac$ is a square in F. In this case, the roots are*

$$\frac{-b \pm d}{2a}$$

where d is a square root of $b^2 - 4ac$.

Conversely, if $b^2 - 4ac$ is a square in F then $ax^2 + bx + c$ has roots in F. If $b^2 - 4ac$ is a non-zero square, then there are two roots. If $b^2 - 4ac = 0$ there is a unique root.

Proof. Suppose that $x = x_0$ is a root of $ax^2 + bx + c$. By Lemma 14,

$$a\left(x_0 + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a} = 0$$

Thus

$$b^2 - 4ac = \left(x_0 + \frac{b}{2a}\right)^2 4a^2 = \left(\left(x_0 + \frac{b}{2a}\right)2a\right)^2.$$

This shows that $b^2 - 4ac$ is a square. Let d be a square root. So

$$d^2 = b^2 - 4ac = \left(\left(x_0 + \frac{b}{2a}\right)2a\right)^2 = (2ax_0 + b)^2.$$

By Corollary 10, $2ax_0 + b = \pm d$. Thus $x_0 = (-b \pm d)/2a$.

Conversely, suppose that $b^2 - 4ac$ is a square in F. Let d be a square root. Then $(-b \pm d)/2a$ are clearly roots of

$$a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a}.$$

By Lemma 14, these give roots of $ax^2 + bx + c$.

We still must show that the roots are distinct if $b^2 - 4a$ is a non-zero square. In this case $d \neq 0$ (otherwise $d^2 = b^2 - 4ac$ would be zero). By Lemma 8 $d \neq -d$. Now suppose the roots are not distinct: $(-b + d)/2a = (-b - d)/2a$. Then $b + d = -b - d$. This implies $d = -d$, a contradiction. Thus we have two distinct roots. If $b^2 - 4ac = 0$ then $d = 0$ (otherwise $d^2 \neq 0$, a contradiction). So $(-b + d)/2a = (-b - d)/2a$. Hence there is exactly one root. □

Now we focus on the case where $F = \mathbb{F}_p$ where p is an odd prime.

Corollary 16. *Let p be an odd prime, and consider the polynomial $ax^2 + bx + c$ where $a \neq 0$ and where $a, b, c \in \mathbb{F}_p$. Then the number of roots in $\mathbb{F}_p$ is given by the following (Legendre Symbol based) formula:*

$$\left(\frac{b^2 - 4ac}{p}\right) + 1.$$

8. Additional Practice Problems

Exercise 9. Compute $\left(\frac{5}{71}\right)$ using the above properties. Likewise, compute $\left(\frac{3}{71}\right)$.

Exercise 10. Use the Legendre symbol to decide if 14 is a square in $\mathbb{F}_{101}$.

Exercise 11. How many roots does $2x^2 + 3x + 4$ have in $\mathbb{F}_{239}$?

Exercise 12. When is 5 a square modulo p where p is an odd prime? List the first eight primes where this happens. Check a few of these to see if you can find square roots of 5. (Hint: the answer depends on what p is modulo 5.)

Exercise 13. When is 7 a square modulo p where p is an odd prime? List the first eight primes where this happens. Check a few of these to see if you can find square roots of 7. (Hint: the answer depends on what p is modulo 28. Divide into two cases: $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$. Use the Chinese Remainder Theorem.)

Exercise 14. Show that $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$ for all odd primes p. (Hint: divide into three cases. (i) $p = 3$, (ii) $p \equiv 1 \bmod 4$, and (iii) $p \equiv 3 \bmod 4$ with $p \neq 3$.)

Exercise 15. For what odd primes p are there elements a and $a+1$ in $\mathbb{F}_p$ that are multiplicative inverses to each other? List the first eight primes where this happens. Check a few of these to see if you can find a. (Hint: show this happens if and only if $x^2 + x - 1 = 0$ has roots.)

Exercise 16. For what odd primes p are there elements a and b in $\mathbb{F}_p$ that are both additive and multiplicative inverses to each other? List the first eight primes where this happens. Check a few of these to see if you can find a and b. (Hint: show this happens if and only if $x^2 + 1$ has roots.)

Exercise 17. For what odd primes p are there elements a and b in $\mathbb{F}_p$ that add to 3 but multiply to 2? Give examples.

Exercise 18. For what odd primes p are there elements a and b in $\mathbb{F}_p$ that add to 2 but multiply to 3? List the first eight primes where this happens. Check a few of these to see if you can find a and b. (Hint: the answer depends on whether -2 is a square modulo p. Compute the Legendre symbol for each possible value of p modulo 8. Observe that knowing p modulo 8 gives you knowledge of p modulo 4.)

Exercise 19. For what odd primes p is there a non-zero element in $\mathbb{F}_p$ whose cube is equal to 3 times itself? List the first eight primes where this happens. Check a few of these primes to see if you can find the desired element in $\mathbb{F}_p$. (Hint: show this happens if and only if $x^2 = 3$ has a solution. Split into three cases: $p = 3$ and $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$.)

Exercise 20. Which odd primes can divide integers of the form $N^2 + 1$? Give a list of seven such primes. Give and justify a general answer.
Answer: primes such that $p \equiv 1 \bmod 4$.

Exercise 21. Which odd primes can divide integers of the form $N^2 - 5$? Give a list of seven such primes. Give and justify a general answer.
Answer: $p = 5$ and other primes such that $p \equiv 1 \bmod 5$ or $p \equiv 4 \bmod 5$.

Exercise 22. Which odd primes can divide integers of the form $N^2 + 5$? Give a list of seven such primes. Give and justify a general answer.
Answer: $p = 5$ and other primes such that $p \equiv 1, 3, 7, 9 \bmod 20$.

Exercise 23. Which odd primes can divide integers of the form $N^2 + N + 1$? Give a list of seven such primes. Give and justify a general answer.
Answer: $p = 3$ and other primes such that $p \equiv 1 \bmod 3$.

Exercise 24. Which odd primes can divide integers of the form $2N^2 + 5N + 1$? Give a list of seven such primes. Give and justify a general answer. Hint: it depends on what p is modulo 17.