Quadratic reciprocity

Francisc Bozgan
Los Angeles Math Circle

October 28, 2012

1 Quadratic Reciprocity and Legendre Symbol

In the beginning of this lecture, we recall some basic knowledge about modular arithmetic:

Definition 1. *(Modulo Notation) Let a, b be integer numbers and n a positive integer number, then we say that a is congruent to b modulo n (and we write $a \equiv b \pmod{p}$ if n divides the difference $a - b$.*

Also recall the **Fundamental theorem of arithmetic**: Every integer n can be written uniquely as $n = \pm p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ where r is a positive integer greater than or equal to 1, $p_1, \dots p_r$ distinct prime numbers and $a_1, \dots a_r$ are positive integers.

The last (and non-trivial) result that we have to recall in order to proceed further is **Fermat's Little Theorem** which says that if a is an integer and p is a prime, then $a^p \equiv a \pmod{p}$, or equivalently $a^{p-1} \equiv 1 \pmod{p}$ if $(a, p) = 1$.

Now we can start talking about the quadratic reciprocity method. This method was developed intuitively (not actually on this modern form that you will see here) by some great number theorists of the 17th and 18th century like Fermat, Euler, Lagrange and Legendre. They began by looking at the quadratic polynomials modulo a prime p and trying to solve it in the most general forms. Namely, they did not try to solve

$$ax^2 + bx + c = 0$$

in the real or complex numbers, which was already known, but rather to solve the equation

$$ax^2 + bx + c \equiv 0 (\text{mod } p) \text{ where } p \text{ is a prime number.}$$

in the integer numbers. We will call such an equation **solvable**, if there exists an integer x_0 such that $ax_0^2 + bx_0 + c \equiv 0 \pmod{p}$.

Although with little success, these mathematicians stated some important conjectures in this field that would broadened the field of number theory. A major breakthrough in this direction came when Gauss (in 1798) proved what

is now called the **Quadratic Reciprocity Law** , namely, if p, q are prime numbers and if $q \equiv 1 \pmod 4$, then

$$x^2 - p \equiv 0 \pmod q \text{ is solvable if and only if } x^2 - q \equiv 0 \pmod p \text{ is solvable}$$

and if $q \equiv 1 \pmod 3$, then

$$x^2 - p \equiv 0 \pmod q \text{ is solvable if and only if } x^2 + q \equiv 0 \pmod p \text{ is solvable.}$$

We will learn this theorem later, but in a more modern formulation. Now let's discuss about the essential results of this topic.

Definition 2. *Let m, n and a be integers, $m \geq 1$, $n \geq 1$ and $(a, m) = 1$. We say that a is a residue of n-th degree modulo m if congruence $x^n \equiv a \pmod m$ has an integer solution; else a is a nonresidue of n-th degree. In particular, if $n = 2$, we will call **quadratic residue** or **quadratic nonresidue**.*

Now we state our first theorem:

Theorem 3. *Given a prime p and an integer a, the equation $x^2 \equiv a$ has zero, one, or two solutions modulo p.*

Proof. Suppose that the considered congruence has a solution x_1. Then so clearly is $x_2 = x_1$. There are no other solutions modulo p, because $x^2 \equiv a \equiv x_1^2 \pmod p$ implies $x \equiv \pm x_1$. □

As an immediate corollary of the above thereom, we have that for every odd prime p, among the numbers $1, 2, \ldots, p-1$ there are exactly $\frac{p-1}{2}$ quadratic residues (and as many quadratic nonresidues).

Now we are ready to define the **Legendre's symbol**:

Definition 4. *Given a prime number p and an integer a, Legendres symbol $\left(\frac{a}{p}\right)$ is defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue (mod } p); \\ -1, & \text{if } p \nmid a \text{ and } a \text{ is a quadratic nonresidue (mod } p); \\ 0, & \text{if } p \mid a. \end{cases}$$

As a first result about the Legendre's symbol, we see that $\left(\frac{x^2}{p}\right) = 1$ for each prime p and integer x, $p \nmid x$. From now on, unless noted otherwise, p is always an odd prime and a an integer.

Clearly, a is a quadratic residue modulo p if and only if so is $a + kp$ for some integer k. Thus we may regard Legendre's symbol as a function from the residue classes modulo p to the set $\{-1, 0, 1\}$.

Fermats theorem asserts that if $(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod p$, which implies $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. More precisely:

Theorem 5. *(Euler's Criterion) If a is an integer and p a prime, then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.*

Proof. The statement is trivial for p divides a. From now on we assume that $p \nmid a$.

Let g be a primitive root modulo p. Then the numbers g^i, $i = 0, 1, \ldots, p-2$ form a reduced system of residues modulo p. We observe that $(g^i)^{\frac{p-1}{2}} = g^{i\frac{p-1}{2}} \equiv 1 (\text{mod } p)$ if and only if $p-1$ divides $i\frac{p-1}{2}$, or equivalently, 2 divides i.

On the other hand, g^i is a quadratic residue modulo p if and only if there exists $j \in \{0, 1, , p-2\}$ such that $(g^j)^2 \equiv g^i \pmod{p}$, which is equivalent to $2j \equiv i \pmod{p-1}$. The last congruence is solvable if and only if 2 divides i, that is, exactly when $(g^i)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. □

Now, by Euler's Criterion we have that

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

for all integers a, b and prime numbers p, therefore we proved that the Legendre's symbol is multiplicative.

Theorem 6. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *for all integers* a, b *and prime number* $p \geq 2$.

From Euler's Criterion, we also get what is called the

Theorem 7. ***First Supplement of the Quadratic Reciprocity Law***
For every prime number $p \geq 3$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Now we return to our initial problem, the one that started all this theory about quadratic residues:

Theorem 8. *Let* x, y *be coprime integers and* a, b, c *be arbitrary integers. If* p *is an odd prime divisor of number* $ax^2 + bxy + cy^2$ *which doesn't divide* abc*, then* $D = b^2 - 4ac$ *is a quadratic residue modulo* p.

In particular, if p *divides* $x^2 - Dy^2$ *and* $(x, y) = 1$*, then* D *is a quadratic residue modulo* p.

Proof. Denote $N = ax^2 + bxy + cy^2$. Since $4aN = (2ax + by)^2 - Dy^2$, we have

$$(2ax + by)^2 \equiv Dy^2 \pmod{p}.$$

Furthermore, y is not divisible by p; otherwise so would be $2ax+by$ and therefore x itself, contradicting the assumption. There is an integer y_1 such that $yy_1 \equiv 1 (\text{mod } p)$. Multiplying the above congruence by y_1^2 gives us $(2axy_1 + byy_1)^2 \equiv D(yy_1)^2 \equiv D(\text{mod } p)$, implying the statement. □

Let us get closer to the main theorem of this introduction to quadratic reciprocity, but first we have to state another intermediate theorem:

Theorem 9. ***Second Supplement of the Quadratic Reciprocity Law***
We have $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. *In other words, 2 is a quadratic residue modulo a prime* $p \geq 3$ *if and only if* $p \equiv \pm 1$ *(mod* 8*).*

The proof is pretty complicated and uses the Gauss Lemma, a very beautiful and helpful trick.

With all this being said, we conclude with the most important theorem of this part, the **Gauss' Law of Quadratic Reciprocity**:

Theorem 10. *For any different odd primes p and q,*

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

The proof of this fact is also pretty tricky, and it will be ommitted. Nevertheless, this won't stop us to use it frequently in deducing other properties about Legendre's symbol. You may ask why Gauss did not state his theorem in this more elegant form. Well, you should know that Legendre invented his symbol long after Gauss proved the quadratic reciprocity law, similarly as Gauss invented the modulo sign long after Fermat, Euler and Lagrange proved their theorems.

Exercises

1. What is $\left(\frac{1}{p}\right)$ if p is a prime number of the form $19k+3$? Is 25 a quadratic residue modulo 79? Is 26 a quadratic residue modulo 79? Is 11718 a quadratic 11719 (trust me, this number is indeed prime)?

2. Compute the following Legendre symbols: $\left(\frac{2}{17}\right)$, $\left(\frac{13}{59}\right)$, $\left(\frac{2012}{103}\right)$,

$$\left(\frac{2^{2012}\cdot 3^{2013}\cdot 5^{2014}\cdot 7^{2015}}{19}\right).$$

3. In fact, what Gauss proved was $\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$. Prove that

$$(-1)^{\left(\frac{p^2-1}{8}\right)} \equiv \left[\frac{p+1}{4}\right] \pmod 2$$

for any odd prime number p, so indeed Theorem 9 is exactly what Gauss proved. (Note that $[x]$ is the greatest integer smaller or equal to x)

4. Is 23 a square mod 41? Is 15 a square mod 41? (CHMMC, Winter 2010)

5. Compute the number of primes p less than 100 such that p divides n^2+n+1 for some integer n. (CHMMC, Winter 2010)

6. Find all the primes p with the property that $7p+3^p-4$ is a perfect square. (Junior Balkan MO 2007)(Hint: Use Fermat's Little Theorem)

7.

(a) -2 is a quadratic residue modulo p if and only if $p \equiv 1$ or $p \equiv 3 \pmod 8$;

(b) -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 6$;

(c) 3 is quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{12}$;

(d) 5 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{10}$.

8. Show that there exist infinitely many prime numbers of the form $10k+9$.

9.Prove that for $n \in \mathbb{N}$ every prime divisor p of number $n^4 - n^2 + 1$ is of the form $12k+1$.

10. If p is a prime of the form $4k+1$, prove that $x = \left(\frac{p-1}{2}\right)!$ is a solution of the congruence $x^2 + 1 \equiv 0 \pmod p$. (Here $m! = 1 \cdot 2 \cdot \ldots \cdot m$)

11. There exists a natural number $a < \sqrt{p}+1$ that is a quadratic nonresidue modulo p. (Hint: Suppose a is a quadratic nonresidue. What can you say about $\left[\frac{p}{a}\right] + 1$?)

12. (Challenge problem) Prove that an integer a is a quadratic residue modulo every prime number if and only if a is a perfect square.

13. Evaluate

$$\left[\frac{1}{2003}\right] + \left[\frac{2}{2003}\right] + \left[\frac{2^2}{2003}\right] + \cdots + \left[\frac{2^{2001}}{2003}\right].$$

(Note that $[x]$ is the greatest integer smaller or equal to x)

14. Prove Gauss' Lemma: Let p be a prime number and a an integer that is coprime with p. Consider the integers $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ and take their least positive residue modulo p. (These residues are all distinct, so there are $\frac{p-1}{2}$ of them.) Let m be the number of quadratic residues that are greater than $\frac{p}{2}$. Show that $\left(\frac{a}{p}\right) = (-1)^m$.

2 Generalization: The Jacobi Symbol

Definition 11. *Let a be an integer and b an odd number, and let $b = p_1^{\alpha_1} p_2^{\alpha_1} \ldots p_r^{\alpha_r}$ be the factorization of b onto primes. Jacobis symbol $\left(\frac{a}{b}\right)$ is defined as a product of Legendre's symbols, namely*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

We see that if a is a quadratic residue modulo n, then clearly $\left(\frac{a}{n}\right) = 1$. However the converse is not true and we can find a counterexample. For example,

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1,$$

but 2 is not a quadratic residue modulo 15, as 2 is not so modulo 3 and 5. Nevertheless, if a is a quadratic nonresidue modulo n, then we get $\left(\frac{a}{n}\right) = -1$, which implies that there exists a prime number p dividing n such that $\left(\frac{a}{p}\right) = -1$ (by the above definition). All this discussion can be summarrized in the following statement:

Theorem 12. *Let a be an integer and b a positive integer, and let $b = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ be the factorization of b onto primes. Then a is a quadratic residue modulo b if and only if a is a quadratic residue modulo $p_i^{\alpha_i}$ for each $i = 1, 2, \dots, r$.*

We will not see the proof of this theorem here. One direction is trivial, namely if there exists an x such that $x^2 \equiv a \pmod{n}$, then clearly the same x satisfies $x^2 \equiv a \pmod{p_i^{\alpha_i}}$. The other direction should be an easy exercise for those of you who know the Chinese Remainder Theorem.

The most beautiful thing about the Jacobi symbol is that it obeys most of the laws that the Legendre's Symbol is obeying.

Theorem 13. *For all integers a, b and odd numbers c, d the following equalities hold:*

$$\left(\frac{a+bc}{c}\right) = \left(\frac{a}{c}\right) \tag{1}$$

$$\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right) \tag{2}$$

$$\left(\frac{a}{cd}\right) = \left(\frac{a}{c}\right)\left(\frac{a}{d}\right) \tag{3}$$

We also have that the Jacobi symbol obeys the three reciproicity laws, namely

Theorem 14. *For every odd integer a,*

$$\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}, \quad \left(\frac{2}{a}\right) = (-1)^{\left(\frac{a^2-1}{8}\right)}$$

and for any two coprime odd numbers a,b it holds that

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

3 Exercises

1. If $\gcd(ab, nm)$=1, then $\left(\frac{ab^2}{nm^2}\right) = \left(\frac{a}{n}\right)$.

2. Let $F(x) = (x^2 - 17)(x^2 - 19)(x^2 - 323)$. Prove that for each m positive integer, the equation

$$F(x) \equiv 0 \pmod{m}$$

has a solution x in $\mathbb{N}$. But $F(x) = 0$ doesn't have any integer solutions (not even rational solutions).

3. Let $m,\ n \geq 3$ be positive odd integers. Prove that $2^m - 1$ doesn't divide $3^n - 1$.

4. Show that there are no positive integers x, y, z, t such that $x + y + t^2 = 4xyz$. (Hint: Write the equation as $4zt^2 + 1 = (4zy - 1)(4zx - 1)$; now look at the Jacobi symbol $\left(\frac{-z}{4yz-1}\right)$).

5. (Challenge Problem) The number of quadratic residues modulo p^n $(n \geq 1)$ is equal to

$$\left[\frac{2^{n-1} - 1}{3}\right] + 2 \text{ for } p = 2, \quad \text{and} \quad \left[\frac{p^{n+1} - 1}{2(p+1)}\right] + 1 \text{ for } p \geq 3.$$

6. (Challenge Problem) Prove that the equation $x^2 = y^3 - 5$ has no integer solutions (x, y).

7. (Challenge Problem) Prove that $4kxy - 1$ does not divide the number $x^m + y^n$ for any positive integers x, y, k, m, n.