Quadratic Reciprocity

Jacob Zhang, Shend Zhjeqi

April 19, 2020

1 Notes for LA Math Circle

I (Jacob) originally wrote this handout two years ago. It uses a bit more algebra than I plan to use in the class. Still, it was meant to be read on its own, so I highly recommend reading it. The problems for Math Circle are at the end.

2 Background

Arithmetic modulo a prime p forms a field $\mathbf{F}_p$. We denote the multiplicative group of the field U_p. Elements of U_p that are perfect squares are called quadratic residues (QRs). We will use some important basic results about QRs and extensions of F_p, which we state here. In the rest of the paper "prime" should always be taken to mean "odd prime."

Theorem 1 (Primitive Root Theorem)**.** *There exists an element $g \in \mathbf{F}_p$ such that the powers $g^0, \ldots, g^{p-2}$ are all the elements of the multiplicative group U_p, or equivalently, there is an isomorphism $U_p \cong \mathbb{Z}_{p-1}$. This is also true for finite fields $\mathbf{F}_{p^k}$.*

Proof. The central observation in the proof is that for a divisor k of $p-1 = |U_p|$ there are k elements of U_p with order dividing k, corresponding to roots of the polynomial $x^k - 1$ in $\mathbf{F}_p[x]$. There are therefore $\phi(p-1) \geq 1$ elements of order $p-1$ where ϕ is the Euler totient function. See any number theory textbook for details. □

Theorem 2 (Fermat)**.** *-1 is a quadratic residue modulo p iff $p \equiv 1 \mod 4$.*

Proof. Let g be a primitive root in $\mathbf{F}_p$. We observe that g^n is a square if and only if n is even, and that $g^{\frac{p-1}{2}} = -1$, since g has order $p-1$. If $p \equiv 1 \mod 4$, then $\frac{p-1}{2}$ is even and we can write $\left(g^{\frac{p-1}{4}}\right)^2 = -1$. On the other hand if $p \equiv 3 \mod 4$, then $\frac{p-1}{2}$ is odd and so $g^{\frac{p-1}{2}}$ cannot be a square. □

Theorem 3 (Frobenius endomorphism)**.** *For a finite field of characteristic p the mapping $F(x) = x^p$ is an automorphism. If an element $\alpha \in \mathbf{F}_{p^k}$ of a finite field extension of $\mathbf{F}_p$ satisfies $F(\alpha) = \alpha$, then $\alpha \in \mathbf{F}_p$.*

Proof. We check that for $x, y \in \mathbf{F}_{p^k}$, we have $(x+y)^p = x^p + y^p$, $(xy)^p = x^p y^p$, and $x^p = 0 \implies x = 0$. Lastly, we note that every element x of $\mathbf{F}_p$ satisfies $x^p - x = 0$, and since this is a degree p polynomial in $\mathbf{F}_{p^k}[x]$, there can be no more solutions to $x^p = x$. □

To study QRs, we introduce the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ quadratic residue} \\ -1 & \text{nonresidue} \end{cases}$$

The congruence

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

follows from the primitive root theorem: if g is a primitive root modulo p and $a \equiv g^n$, then

$$a^{\frac{p-1}{2}} \equiv g^{n\frac{p-1}{2}} \equiv \begin{cases} 1 & n \text{ even} \\ -1 & n \text{ odd} \end{cases}$$

but since a is a QR if and only if n is even, this is the definition of the Legendre symbol. From this equivalence, we see that the Legendre symbol is multiplicative. It is a simple example of a type of multiplicative function mapping nonzero elements modulo p to roots of unity, called Dirichlet characters.

Euler and Legendre conjectured and Gauss finally proved a connection between whether an odd prime p is a QR modulo an odd prime q and whether q is a QR modulo p. Gauss's Law of Quadratic Reciprocity can be stated using the Legendre symbol as

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

In other words, p is a QR mod q iff q is a QR mod p, unless both p and q are 3 mod 4, in which case exactly one of p and q is a QR mod the other. The rest of the paper is devoted to proving this surprising result.

3 Motivating examples

Consider the question of whether 3 is a QR modulo a prime number p. The polynomial $x^2 - 3$ seems like the natural one to study, but this doesn't get us any further than where we started. However, if we look at a root ω of the polynomial $x^2 + x + 1$, the quadratic formula gives

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

and so $\sqrt{-3} = 2\omega + 1$ and we can check explicitly that

$$(2\omega + 1)^2 = 4\omega^2 + 4\omega + 1 = 3(\omega^2 + \omega) = -3$$

which holds in any field. So we can learn something about whether -3, and therefore 3, is a QR by studying ω. In particular -3 is a QR mod p iff ω is an element of $\mathbf{F}_p$, and ω, a primitive 3rd root of unity, is an element of $\mathbf{F}_p$ iff $p \equiv 1 \mod 3$. If $p \equiv 1 \mod 3$ then we can construct ω by taking a primitive root g in $\mathbf{F}_p$ (of order $p-1$) and letting $\omega = g^{\frac{p-1}{3}}$. If $p \equiv 2 \mod 3$ then $x^3 \equiv 1$ implies $x \equiv 1$ since if we let $x = g^k$ then $x^3 = g^{3k} = 1$ implies $3k \equiv 0 \mod p-1$ which implies $k \equiv 0 \mod p-1$ since $\gcd(p-1, 3) = 1$. Writing this out using the Legendre symbol, we have

$$\left(\frac{-3}{p}\right)\left(\frac{p}{3}\right) = 1$$

and so

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right)\left(\frac{-3}{p}\right)\left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

a clear special case of quadratic reciprocity.

Naturally the next step is to consider the prime 5 instead of 3. Because 5 is 1 mod 4, we expect it to show slightly different behavior, hopefully in a way that is instructive. Here the well-known trig identity

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5} - 1}{4}$$

means that if we let $\omega = e^{\frac{2\pi i}{5}}$ be a primitive 5th root of unity in $\mathbb{C}$, then

$$\sqrt{5} = 2(\omega + \omega^{-1}) + 1 = 2\omega + 2\omega^4 + 1$$

Since the polynomial relation $(2\omega+2\omega^4+1)^2 = 5$ has integer coefficients, we expect that it holds in in a finite field extension of $\mathbf{F}_p$ containing a primitive 5th root of unity ω. In this case the relation $\sqrt{5} = 2\omega + 2\omega^4 + 1$ is not linear, so 5 may be a QR mod p without ω being an element of $\mathbf{F}_p$. Now we use the Frobenius automorphism $F(x) = x^p$ to check whether $\sqrt{5}$ is in $\mathbf{F}_p$. We see that

$$F(\sqrt{5}) = \sqrt{5}^p = 2\omega^p + 2\omega^{4p} + 1$$

and so $\sqrt{5}$ is preserved if multiplication by p maps the set $\{1, 4\}$ to itself. We recognize this as the set of QRs modulo 5, and so $\sqrt{5}$ maps to itself if p is a QR, and to $-\sqrt{5}$ otherwise! We can write this as

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = 1$$

3.1 Sidenote: When is 2 a QR mod p?

We can make a similar argument by letting ω be an 8th root of unity in an extension of $\mathbf{F}_p$. Then

$$(\omega + \omega^7)^2 = \omega^2 + 2\omega^8 + \omega^{14} = 2$$

On the other hand, if we let $S = \omega + \omega^7$, then

$$S^p = (\omega + \omega^7)^p = \omega^p + \omega^{7p}$$

is equal to S if $p \equiv 1, 7 \mod 8$, and equal to $-S$ otherwise. Therefore 2 is a QR modulo p iff $p \equiv 1, 7 \mod 8$, which can be written elegantly as

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

In this case 8 takes the place of 2 as the degree of the root of unity we use, and the set $\{1, 7\}$ is not the quadratic residues modulo 8, though it is still a subgroup of index 2 in U_8, which is really the property of quadratic residues that we are using. We observe a difference between 8 and the odd primes 3,5 because the Primitive Root theorem fails mod 8 - U_8 is not cyclic.

4 Proof in the general case

In the examples above, a pattern emerges: for a prime q, we make ζ a primitive qth root of unity in a finite extension of $\mathbf{F}_p$ and consider the sum

$$S_q = \sum_{k=0}^{q-1} \zeta^{k^2}$$

The usefulness of this sum (called a Gaussian period) is that

$$S_q^p = \sum_{k=0}^{q-1} \zeta^{pk^2} = \begin{cases} S_q & p \text{ quadratic residue} \mod q \\ -S_q & p \text{ nonresidue} \mod q \end{cases}$$

This means that S_q is a square root of some sort, since its only potential conjugate is its negative, and whether it is in $\mathbf{F}_p$ depends on whether p is a QR mod q. From the examples, a reasonable guess is that

$$S_q^2 = \begin{cases} q & q \equiv 1 \mod 4 \\ -q & q \equiv 3 \mod 4 \end{cases}$$

which if proven would imply

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & q \equiv 1 \mod 4 \\ 1 & q \equiv 3 \text{ and } p \equiv 1 \\ -1 & q \equiv 3 \text{ and } p \equiv 3 \end{cases} = (-1)^{\frac{(p-1)(q-1)}{4}}$$

by the same logic used in the examples. We now prove this guess by considering the two cases separately.

4.1 $q \equiv 1 \mod 4$ case

In this case we have that $i = \sqrt{-1} \in \mathbf{F}_q$, and so we can manipulate S_q^2 as follows:

$$S_q^2 = \sum_{(a,b)\in\mathbf{F}_q^2} \zeta^{a^2+b^2} = \sum_{(a,b)\in\mathbf{F}_q^2} \zeta^{(a+bi)(a-bi)}$$

At this point if we substitute $u = a + bi$, $v = a - bi$, we find that the pairs (u, v) also range over $\mathbf{F}_q^2$, since this is an invertible linear transformation. Therefore

$$S_q^2 = \sum_{(u,v)\in\mathbf{F}_q^2} \zeta^{uv} = \sum_{u=0}^{q-1}\sum_{v=0}^{q-1} (\zeta^u)^v$$

and since the inner sum is 0 unless $u = 0$, in which case it is equal to q, we have that $S_q^2 = q$ as desired.

4.2 $q \equiv 3 \mod 4$ case

In this case we have that $i = \sqrt{-1}$ is not an element of $\mathbf{F}_q$, and so we can form the field extension $\mathbf{F}_q(i)$. This time we manipulate

$$S_q^2 = \sum_{(a,b)\in\mathbf{F}_q^2} \zeta^{a^2+b^2} = \sum_{w\in\mathbf{F}_q(i)} \zeta^{|w|^2}$$

The mapping $w \mapsto |w|^2$ is a homomorphism from the multiplicative group of $\mathbf{F}_q(i)$ to the multiplicative group of $\mathbf{F}_q$ and so its range must be a subgroup of that group; but since the range includes more than half the elements of $\mathbf{F}_q$, it must be the entire group. Therefore every nonzero element of $\mathbf{F}_q$ can be written as $|w|^2$ for exactly $\frac{q^2-1}{q-1} = q + 1$ values of w, and there is only one way to write 0, as $0^2 + 0^2$. So

$$S_q^2 = \sum_{w\in\mathbf{F}_q(i)} \zeta^{|w|^2} = 1 + \sum_{k=1}^{q-1} (q+1)\zeta^k = 1 + (q+1)(-1) = -q$$

as desired.

5 Problems

1. Prove that there are at least $p - 3$ ordered pairs (a, b) of residues modulo p satisfying $a^2 + b^2 \equiv 1$, or equivalently, that there are at least $\frac{p-3}{2}$ residues a such that $1 - a^2$ is a quadratic residue modulo p.

2. Prove that there are at least $\frac{p-5}{4}$ residues a modulo p such that $1 + a$ and $1 - a$ are both not quadratic residues.

3. Using quadratic reciprocity, decide whether 210 is a quadratic residue modulo the prime number 1009 (hint: factor 210). How could you have done this without quadratic reciprocity? Which method is faster?