SQUARES MODULO p, II

KEITH CONRAD

For a whole year this theorem tormented me and absorbed my greatest efforts until at last I obtained a proof. Gauss

1. Introduction

For a prime p in $\mathbf{Z}^+$ and an integer a, the Legendre symbol $(\frac{a}{p})$ is

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \equiv \Box \bmod p, a \not\equiv 0 \bmod p, \\ -1, & \text{if } a \not\equiv \Box \bmod p, \\ 0, & \text{if } a \equiv 0 \bmod p. \end{cases}$$

Since the Legendre symbol is multiplicative in a (that is, $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$), its evaluation is reduced to the case when $a = -1$ or a is a prime number. In part I we computed $(\frac{-1}{p})$ and $(\frac{2}{p})$. Here we will prove the main law of quadratic reciprocity: $(\frac{q}{p}) = (-1)^{(p-1)/2\cdot(q-1)/2}(\frac{p}{q})$ for distinct odd primes p and q.

2. Background to Proving the Main Law: Counting Solutions

Our proof of the main law is due to V. A. Lebesgue (1838). Lebesgue's proof of the main law is based on counting the number of points on the "mod p unit hypersphere"

$$x_1^2 + x_2^2 + \cdots + x_n^2 \equiv 1 \bmod p \tag{2.1}$$

in $(\mathbf{Z}/(p))^n$. (Actually, only odd n and $n = 2$ will be important for us; we used $n = 2$ in part I to compute $(\frac{2}{p})$.) It will be convenient to work with equations in $\mathbf{Z}/(p)$ rather than congruences in $\mathbf{Z}$, principally because we will be introducing changes of variables that are simpler to describe within $\mathbf{Z}/(p)$. Thus we will view (2.1) as the equation

$$x_1^2 + x_2^2 + \cdots + x_n^2 = 1$$

directly in $\mathbf{Z}/(p)$.

Since $x^2 = 1$ has two solutions in $\mathbf{Z}/(p)$, the number of solutions when $n = 1$ is 2. The next result, concerning $n = 2$, was proved in part I.

Lemma 2.1. *For $a \in \mathbf{Z}/(p)$,*

$$\#\{(x, y) : x, y \in \mathbf{Z}/(p), x^2 + y^2 = a\} = \begin{cases} p - (\frac{-1}{p}), & \text{if } a \neq 0, \\ p + (\frac{-1}{p})(p-1), & \text{if } a = 0. \end{cases}$$

Definition 2.2. For an odd prime p, let

$$\mathrm{N}_{n,p} = \#\{(x_1, \ldots, x_n) \in (\mathbf{Z}/(p))^n : x_1^2 + \cdots + x_n^2 = 1\}.$$

We have found $\mathrm{N}_{1,p}$ and $\mathrm{N}_{2,p}$. For $n \geq 3$, we will find a recursion connecting $\mathrm{N}_{n,p}$ to $\mathrm{N}_{n-2,p}$.

When trying to solve the equation

$$x_1^2 + x_2^2 + \cdots + x_{n-1}^2 + x_n^2 = 1$$

with $x_i \in \mathbf{Z}/(p)$, let $x_1, \ldots, x_{n-2}$ be chosen arbitrarily. There are p^{n-2} such choices that can be made. To solve for x_{n-1} and x_n amounts to writing $1 - x_1^2 - \cdots - x_{n-2}^2$ as a sum of two squares, and Lemma 2.1 tells us the number of ways to write an element of $\mathbf{Z}/(p)$ as a sum of two squares depends only on whether or not the element is 0. Taking into account the formula in Lemma 2.1,

$$\begin{aligned}
\mathrm{N}_{n,p} &= \sum_{x_1,\ldots,x_{n-2} \in \mathbf{Z}/(p)} \#\{(x,y) \in (\mathbf{Z}/(p))^2 : x^2 + y^2 = 1 - x_1^2 - \cdots - x_{n-2}^2\} \\
&= \sum_{x_1^2+\cdots+x_{n-2}^2 \neq 1} \left(p - \left(\frac{-1}{p}\right)\right) + \sum_{x_1^2+\cdots+x_{n-2}^2 = 1} \left(p + \left(\frac{-1}{p}\right)(p-1)\right).
\end{aligned}$$

Both summation terms contain $p - (\frac{-1}{p})$ and the second summation term contains an additional $(\frac{-1}{p})p$. Thus for any integer $n \geq 3$,

$$\begin{aligned}
\mathrm{N}_{n,p} &= \sum_{x_1,\ldots,x_{n-2}} \left(p - \left(\frac{-1}{p}\right)\right) + \sum_{x_1^2+\cdots+x_{n-2}^2 = 1} \left(\frac{-1}{p}\right) p \\
&= p^{n-2}\left(p - \left(\frac{-1}{p}\right)\right) + \left(\frac{-1}{p}\right) p\, \mathrm{N}_{n-2,p} \\
&= p^{n-1} + \left(\frac{-1}{p}\right)\left(p\, \mathrm{N}_{n-2,p} - p^{n-2}\right). \qquad (2.2)
\end{aligned}$$

Equation (2.2) is a crucial formula. It provides a recursion for the sequence $\mathrm{N}_{n,p}$ linking any members that are two terms apart. We will focus on $\mathrm{N}_{n,p}$ for odd n.

Since $\mathrm{N}_{1,p} = 2$, by (2.2)

$$\begin{aligned}
\mathrm{N}_{3,p} &= p^2 + \left(\frac{-1}{p}\right)(p \cdot 2 - p) \\
&= p^2 + \left(\frac{-1}{p}\right) p
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{N}_{5,p} &= p^4 + \left(\frac{-1}{p}\right)\left(p\, \mathrm{N}_{3,p} - p^3\right) \\
&= p^4 + \left(\frac{-1}{p}\right)\left(p^3 + \left(\frac{-1}{p}\right) p^2 - p^3\right) \\
&= p^4 + p^2.
\end{aligned}$$

Doing this one more time,

$$\begin{aligned}\mathrm{N}_{7,p} &= p^6 + \left(\frac{-1}{p}\right)(p\,\mathrm{N}_{5,p} - p^5)\\ &= p^6 + \left(\frac{-1}{p}\right)(p^5 + p^3 - p^5)\\ &= p^6 + \left(\frac{-1}{p}\right)p^3.\end{aligned}$$

We collect all these formulas for $\mathrm{N}_{n,p}$ in Table 1.

n	$\mathrm{N}_{n,p}$
1	2
3	$p^2 + (\frac{-1}{p})p$
5	$p^4 + p^2$
7	$p^6 + (\frac{-1}{p})p^3$

Table 1

Using the data in Table 1, it is not hard to conjecture the next result.

Theorem 2.3. *For odd $n \geq 1$,*

$$\mathrm{N}_{n,p} = p^{n-1} + \left(\frac{-1}{p}\right)^{\frac{n-1}{2}} p^{\frac{n-1}{2}}.$$

Proof. Use (2.2) and induction (the inductive step goes from n to $n+2$). □

The reader is invited to use (2.2) to get a formula for $\mathrm{N}_{n,p}$ when n is even following the same methods as we used when n is odd, but the case of even $n > 2$ will turn out not to be necessary to prove the main law of quadratic reciprocity, so we omit it.

Remark 2.4. There is a geometric interpretation for part of Theorem 2.3. The number $\mathrm{N}_{n,p}$ counts the solutions to a single equation in n-dimensional space over $\mathbf{Z}/(p)$ and the dominant term in its formula (for p fixed and n large) is p^{n-1}. A single equation in n variables is one constraint, so intuitively its solution space has "dimension" $n-1$. (Compare with Euclidean space, where the solution set of $x^2+y^2+z^2 = 1$ in $\mathbf{R}^3$ is a sphere, which is a surface and thus locally looks 2-dimensional: $2 = 3-1$.) The standard $(n-1)$-dimensional space $(\mathbf{Z}/(p))^{n-1}$ has size p^{n-1}, and $\pm p^{(n-1)/2}$ in Theorem 2.3 is much smaller than p^{n-1} for large n, so to a *first approximation* the "$(n-1)$-dimensional hypersurface"

$$x_1^2 + \cdots + x_n^2 = 1$$

in $(\mathbf{Z}/(p))^n$ has about as many points as the standard $(n-1)$-dimensional space $(\mathbf{Z}/(p))^{n-1}$.

3. Proof of the main law

We will use Theorem 2.3 to prove the main law of quadratic reciprocity. In Theorem 2.3, let $n = q$ be an odd prime number $\neq p$. That is, we look at

$$\mathrm{N}_{q,p} = \#\{(x_1, \ldots, x_q) \in (\mathbf{Z}/(p))^q : x_1^2 + \cdots + x_q^2 = 1\}.$$

By Theorem 2.3,

$$\begin{aligned}\mathrm{N}_{q,p} &= p^{q-1}+\left(\frac{-1}{p}\right)^{\frac{q-1}{2}}p^{\frac{q-1}{2}}\\ &= p^{q-1}+(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}p^{\frac{q-1}{2}}.\end{aligned}$$

This is an exact formula for the number of solutions to $x_1^2+\cdots+x_q^2=1$ in $\mathbf{Z}/(p)$. Reducing the formula for $\mathrm{N}_{q,p}$ modulo q, p^{q-1} becomes 1 and $p^{\frac{q-1}{2}}$ becomes $(\frac{p}{q})$:

$$\mathrm{N}_{q,p}\equiv 1+(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)\bmod q. \tag{3.1}$$

Now we will compute $\mathrm{N}_{q,p} \bmod q$ by a wholly different method and compare to (3.1). The number $\mathrm{N}_{q,p}$ counts solutions over $\mathbf{Z}/(p)$ to the polynomial equation $x_1^2+\cdots+x_q^2=1$ in q variables. The polynomial $x_1^2+\cdots+x_q^2$ is symmetric in its q variables. Therefore the solution set counted by $\mathrm{N}_{q,p}$ is closed under *cyclic shifts*. Solutions have q coordinates, and q is prime, so either a solution has no cyclic shifts besides itself (all x_i are equal) or it has q cyclic shifts. Solutions where the coordinates are not all equal come in collections of size q (all disjoint). By counting $\mathrm{N}_{q,p} \bmod q$, only the solutions with all coordinates equal matter in the counting, so

$$\mathrm{N}_{q,p}\equiv\#\{x\in\mathbf{Z}/(p): qx^2=1\}\bmod q.$$

How many solutions x are there to $qx^2=1$ in $\mathbf{Z}/(p)$? If q is a square in $\mathbf{Z}/(p)$ then there are two solutions. If q is a nonsquare then there are no solutions. In both cases, the number of solutions is $1+(\frac{q}{p})$. Comparing this to (3.1), we obtain

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

Subtracting 1 from both sides,

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

Both sides of this congruence are ±1, so being congruent modulo $q>2$ implies they are equal integers:

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

This is the main law of quadratic reciprocity!

Remark 3.1. We used $\mathrm{N}_{q,p}$ for prime q in the proof of the main law of quadratic reciprocity. But the proof of the formula for $\mathrm{N}_{n,p}$ (odd n) in Theorem 2.3 used induction on n and therefore would not have worked if at that point we only let n be prime.