A FEW RESULTS OF QUADRATIC RECIPROCITY

EKAM KAUR

Abstract. In this paper, we present a few proofs of the Quadratic Reciprocity Law that are not particularly well known. We also use Quadratic Reciprocity to see which primes can be written in the form x^2+ny^2. We introduce the Jacobi Symbol and Quadratic Reciprocity Law for Jacobi Symbol (or simply "Jacobi Reciprocity Law"). We also explore other related ideas such as Modular Functions and Hensel's Lemma.

1. Introduction

Quadratic Reciprocity is one of the most important and powerful theorems in elementary number theory. The law was first formulated, but not proved by Euler. In 1785, Legendre discovered it independently of Euler and partially proved it. The first complete proof was given by Gauss in 1796 in *Disquisitiones Arithmeticae*, a book that laid foundations of modern number theory. Later in life, Gauss discovered 7 other proofs.

2. Quadratic Residues

In this section we introduce the basic definitions and theorems which we will use throughout the rest of the paper.

Definition 2.1. For $a \in \mathbb{Z}$, we say a is a *quadratic residue* $\pmod p$ is there exists some x such that $x^2 \equiv a \pmod p$. Otherwise we say a is a *quadratic non-residue* $\pmod p$.

Fact 2.2. *Exactly half of the linear nonzero residues* $\pmod p$ *are quadratic residues.*

Now we state the following lemma:

Lemma 2.3. *Let p, be an odd prime, then $p \mid x^2 + y^2$ with x and y relatively prime if and only if (-1) is a quadratic residue* $\pmod p$.

Proof. Since x and y are relatively prime, y has a multiplicative inverse modulo p. So $x^2 + y^2 \equiv 0 \pmod p$ if and only if $(xy^{-1})^2 \equiv -1 \pmod p$. ∎

Definition 2.4. We define the Legendre Symbol as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \text{ is a quadratic residue } \pmod p \text{ and } p \nmid a \\ -1 & \text{if } p \text{ is a non-quadratic residue } \pmod p \text{ and } p \nmid a \end{cases}$$

Now we present a useful theorem as follows:

Theorem 2.5 (Euler's Criterion)**.** *Let p be an odd prime and a be any integer. Then we have the following:*

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

Date: July 2020.

Proof. We first recall Fact 2.2.
By Fermat's Little Theorem, we have

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

If a is a quadratic residue modulo p, then $x^2 \equiv a \pmod{p}$ for some integer x. Then we have

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Thus it suffices to prove that for non-quadratic residues, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Now let's consider the equation $x^{\frac{p-1}{2}} = 1$ in $\mathbb{Z}_p$. It has at most $\frac{p-1}{2}$ roots by the Fundamental Theorem of Algebra. But we already know that the quadratic residues modulo p are roots of this equation. So there is no other root, meaning that for any quadratic non-residue a, $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Thus we must have $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. ■

Corollary 2.6. *For an odd prime p, we have*

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

Corollary 2.7. *For an odd prime p and $a, b \in \mathbb{Z}$,*

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

Theorem 2.8 (Gauss Lemma for Quadratic Reciprocity)**.** *Take an $a \in \mathbb{Z}$ not divisible by an odd prime p. Let $S = \{1a, 2a, \ldots, \frac{p-1}{2}a\}$ and reduce the elements of $S \pmod{p}$. If k denotes the number of elements of S whose residue is at least $\frac{p+1}{2}$, then*

$$\left(\frac{a}{p}\right) = (-1)^k.$$

Proof. Let $a_1, \ldots, a_j$ be the residue of set S less than $\frac{p}{2}$ and $b_1, \ldots, b_k$ be the residue of set S more than $\frac{p}{2}$. Thus $j + k = \frac{p-1}{2}$.
Now we prove the following claim:

Claim 2.9. $\left\{1, 2, \ldots, \frac{p-1}{2}\right\} = \{p - b_1, \ldots, p - b_k, a_1, \ldots, a_j\}$.

We prove the claim as follows:
The a_i's are contained in $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ since the a_i's are less than $\frac{p}{2}$. What about the $p - b_i$'s?
We have that $b_i > \frac{p}{2} \implies p - b_i < \frac{p}{2}$. So we have $p - b_i \leq \frac{p-1}{2}$. This shows that the $p - b_i$'s are contained in $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ as well.
Since there are $\frac{p-1}{2}$ elements in $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ and $j + k = \frac{p-1}{2}$, it suffices to prove that the a_i's and $p - b_i$'s are distinct.
Each a_i can be written in the form ra where $1 \leq r \leq \frac{p-1}{2}$. So if $ra \equiv sa \pmod{p}$, then $p \mid (r - s)a$ which is impossible when r, s are distinct.
A similar argument shows that the b_i's are distinct, and hence the $p - bi$'s are too.
Could $a_i = p - b_j$? If this is possible, then $p - ra \equiv sa \pmod{p} \implies p \mid (r + s)a$ which is impossible since $2 \leq r + s \leq p - 1$. This completes the proof that $\left\{1, 2, \ldots, \frac{p-1}{2}\right\} =$

$\{p-b_1,\ldots,p-b_k,a_1,\ldots,a_j\}$. Since the two sets are the same, the product must be the same as well:

$$\prod_{i=1}^{k} p-b_i \prod_{i=1}^{j} a_i \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Since $p-b_i \equiv -b_i \pmod{p}$, we get

$$(-1)^k \prod_{i=1}^{k} b_i \prod_{i=1}^{j} a_i \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

But notice that the a_i's and b_i's are the the residues of the numbers $a, 2a, \ldots, \frac{p-1}{2}$, so we get the following:

$$(-1)^k a \cdot 2a \cdot 3a \cdots \frac{p-1}{2}a \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

$$\implies (-1)^k a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Since p and $\frac{p-1}{2}$ are relatively prime,

$$(-1)^k a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

$$\implies (-1)^k \left(\frac{a}{p}\right) \equiv 1 \pmod{p}$$

$$\implies \left(\frac{a}{p}\right) \equiv (-1)^k$$

■

Proposition 2.10. *For an odd prime p,*

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

Proof. We apply Gauss Lemma (Theorem 2.7) to the set $S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Then

$$\{2s : s \in S\} = \{2, 4, \ldots, p-1\}$$

and

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

where k denotes the number of residue of the set $\{2, 4, \ldots, p-1\}$ at least $\frac{p+1}{2}$. Now $p = 8x+y$ for some x and $y \in \{1, 3, 5, 7\}$. Considering each case, we see that the number of residues in $\{2, 4, \ldots, p-1\}$ more than $\frac{p}{2}$ is even when $p \equiv 1, 7 \pmod{8}$ and odd when $p \equiv 3, 5 \pmod{8}$. Note that $\frac{p^2-1}{8}$ is even when $p \equiv \pm 1 \pmod{8}$ and odd otherwise. So thus

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

and we are done. ■

Theorem 2.11 (Eisenstein's Lemma)**.** *Let p an odd prime and $q \in \mathbb{Z}$ such that q is coprime to p. Consider the residue classes $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ of the set*

$$\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}.$$

Then

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

Proof. Consider the list of numbers $(-1)^{r_1}r_1, (-1)^{r_2}r_2, \ldots, (-1)^{r_{\frac{p-1}{2}}}r_{\frac{p-1}{2}}$. We claim that this list coincides with the set $\{2, 4, \ldots, p-1\}$. First, let us observe that each such residue class is represented by an even number. Indeed, if r_i is even, then $(-1)^{r_i}r_i$ is also even. If r_i is odd, then $(-1)^{r_i}r_i$ is a negative and since p is odd, it is also represented by an even residue class.
Second, let us observe that the $(-1)^{r_i}r_i$ are all distinct. To prove this, suppose for the sake of contradiction,

$$(-1)^{r_i}r_i = (-1)^{r_j}r_j$$

for some distinct integers i and j. Equivalently

$$qa \equiv \pm qa' \pmod{p}$$

where a and a' are elements of the set $\{2, 4, \ldots, p-1\}$. Since q is relatively prime to p, we conclude that

$$a \equiv a' \pmod{p},$$

or equivalently $a \pm a' \equiv 0 \pmod{p}$. Since a and a' are both distinct even numbers less than $p-1$, the sum and difference are both even numbers strictly less than $2p$. Thus it follows that $a \neq a'$.
Now by the definition of r_i, we see that

$$q^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} 2i \equiv r_i \prod_{i=1}^{\frac{p-1}{2}} \pmod{p}.$$

On the other hand,

$$\prod_{i=1}^{\frac{p-1}{2}} 2i \equiv \prod_{i=1}^{\frac{p-1}{2}} (-1)^{r_i} r_i \equiv (-1)^{\sum_{r=1}^{\frac{p-1}{2}} r_i} \prod_{i=1}^{\frac{p-1}{2}} r_i \pmod{p}.$$

Plugging in, we get

$$q^{\frac{p-1}{2}} \equiv (-1)^{\sum_{r=1}^{\frac{p-1}{2}} r_i} \pmod{p}.$$

Now Euler's Criterion tells us that

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

So we conclude

$$\left(\frac{q}{p}\right) \equiv (-1)^{\sum_{r=1}^{\frac{p-1}{2}} r_i} \pmod{p}.$$

■

We can extend Theorem 2.10 further and prove that

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{r=1}^{\frac{p-1}{2}} \lfloor \frac{2iq}{p} \rfloor}.$$

as follows:

By the division algorithm we can write $2iq = m_i p + r_i$ for suitable integers m_i. Therefore,

$$\sum_{i=1}^{\frac{p-1}{2}} 2iq = \sum_{i=1}^{\frac{p-1}{2}} m_i p + r_i = p\left(\sum_{i=1}^{\frac{p-1}{2}} m_i\right) + r_i$$

In fact, m_i is precisely $\left[\frac{2iq}{p}\right]$, where the square brackets denotes the greatest integer function. Since we are interested in the sign $(-1)^{\sum_{i=1}^{2-1} r_i}$, we only care about the parity of the expression in the exponent. since the integers qa are all even, it follows that

$$(-1)^{\sum_{i=1}^{p-1} r_i} = (-1)^{\sum_{i=1}^{p-1} \left[\frac{2iq}{p}\right]}$$

and we may conclude that

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^{p-1} \left[\frac{2iq}{p}\right]}.$$

3. Quadratic Reciprocity

Here, we introduce and prove the main theorem of the paper.

Theorem 3.1 (Law of Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

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

We present four proofs as follows:

First Proof. Consider now the box in the $x-y$ -plane with vertices $A = (0,0), (0,q), (p,0)$ and $B = (q,p)$ Look at the lattice points inside If we draw the line through (0,0) and (q,p), it has slope $\frac{q}{p}$. Since p and q are relatively prime, this line does not pass through any points with integer coordinates. Moreover, the box has $(p-1)\times(q-1)$ points on the interior with integer coordinates. since p and q are both odd, that means there are an even number of lattice points in the interior of the box. since we are interested in the sign $(-1)^{\sum_{i=1}^{p-1} \left[\frac{2iq}{p}\right]}$, it suffices for us to understand the parity of the expression $\sum_{i=1}^{p-1} \left[\frac{2iq}{p}\right]$. The expression $\left[\frac{2iq}{p}\right]$ is precisely the number of lattice points below the line with slope $\frac{q}{p}$ with even integer x -coordinate $2i$ (these are called abscissas). Now, we make various observations about this number of lattice points. 1. The number of lattice points inside the box above the line AB is equal to the number of lattice points below the line. 2. since $q-1$ is even, the number of lattice points on each vertical line on the interior of the box is even, and thus the parity of the number of points with a given x -coordinate above AB is equal to the parity of the number of points AB. 3. Given an even x -coordinate $a > \frac{p}{2}$. The number of lattice points with x -coordinate a above the line AB coincides with the number of lattice points with x -coordinate $p-a$ below the line AB. Putting these three things together, observe that the parity of the number of lattice points with even x -coordinate below the line AB is therefore

the same as the parity of the number of points lying on the interior of the triangle with coordinates $A, C = \left(\frac{p}{2}, 0\right)$ and $D = \left(\frac{p}{2}, \frac{q}{2}\right)$. In a formula,

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{2iq}{p}\right] \equiv \mu \pmod 2$$

where μ is the number of lattice points inside the triangle ACD. Reversing the roles of p and q, one similarly concludes that

$$\sum_{i=1}^{\frac{q-1}{2}} \left[\frac{2ip}{q}\right] \equiv \nu \pmod 2$$

where ν is the number of lattice points inside the triangle AED where $E = \left(0, \frac{q}{2}\right)$ The result of the previous section implies that:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{i=1}^{p-1}\left[\frac{2iq}{p}\right]}(-1)^{\sum_{i=1}^{q-1}\left[\frac{2ip}{q}\right]}$$

The arguments above show that the sign on the right is equivalent to

$$(-1)^{\mu+\nu}$$

However, the total number of lattice points in the rectangle $AECD$ is precisely $\frac{p-1}{2}\frac{q-1}{2}$, and therefore,

$$(-1)^{\mu+\nu} = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

So we get

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

as desired. ■

Second Proof. 1. Assume that p and q have their usual meaning and let G denote the series

$$G = x - x^g + x^{g^2} \mp \ldots - x^{g^{p-2}} \tag{3.1}$$

where g is a primitive root modulo p. Then it follows from properties of binomial coefficients that $G^q - \left(x - x^g + x^{g^2} \mp \ldots - x^{g^{p-2}}\right)^q \equiv 0 \bmod q$, or, since q is odd that

$$G^q - G_q \equiv 0 \pmod q, \quad \text{where} \quad G_q = x^q - x^{qg} + x^{qg^2} \pm \ldots - x^{qg^{p-2}} \tag{3.2}$$

If moreover $q \equiv g^\mu \pmod p$, then the system of equations

$$q = g^\mu + f_1 p, \quad qg = g^{\mu+1} + f_2 p, \quad \ldots, \quad qg^{p-2} = g^{\mu+p-2} + f_3 p$$

implies

$$x^{qg^\lambda} - x^{qg^{\mu+\lambda}} = (1 - x^p)\, f(x) \tag{3.3}$$

where $f(x)$ is a polynomial in x. Thus we find

$$G_q - \left\{x^{g^\mu} - x^{g^{\mu+1}} \pm \ldots \pm x^{g^{\mu+p-2}}\right\} = (1 - x^p)\, W \tag{3.4}$$

where W is also a polynomial in x. The exponents of the $p-1$ terms inside the brackets are just the integers $1, 2, \ldots, p-1$ since g is a primitive root modulo p. since the signs alternate, we see that $x^{g^\mu} - x^{g^{\mu+1}} \pm \ldots = \pm G$. The sign of G is that of $-(-1)^{p-\mu}x$, and since p is odd

we conclude that $\pm G = (-1)^{\mu} G$ From $q \equiv g^{\mu} \pmod{p}$ we then find $q^{\frac{p-1}{2}} \equiv \left(g^{\frac{p-1}{2}}\right)^{\mu} \equiv \left(\frac{q}{p}\right) \pmod{p}$, and since $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, this implies

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

and

$$G_q - \left(\frac{q}{p}\right) G = (1 - x^p)\, W \tag{3.5}$$

2. Now consider the system of identities

$$\begin{gathered} +xG - x^2 + x^{g+1} - x^{g^2+1} + \ldots + x^{g^{p-2}+1} = 0, \\ -x^g G - x^{2g} + x^{g^2+g} - x^{g^3+g} + \ldots + x^{g^{p-1}+g} = \left(x^{g^{p-1}} - 1\right), \end{gathered}$$

$+$

$$\begin{gathered} x^{p-2} G - x^{2g^{p-2}} + x^{g^{p-1}+g^{p-2}} + \ldots + x^{g^{2p-4}+g^{p-2}} = \\ x^{g^{p-2}+1} \left\{ x^{g^{p-1}-1} - 1 - \left(x^{g^p-1} - 1\right) - \ldots \right\}. \end{gathered}$$

Adding these equations gives

$$\Omega = G^2 - f\left(x^{g^0+1}\right) + f\left(x^{g+1}\right) \mp \ldots + f\left(x^{g^{p-2}+1}\right) \tag{3.6}$$

where Ω denotes the sum of the expressions on the right-hand side of the above system of equations and where we have set $f\left(x^{\lambda}\right) = 1 + x^{\lambda} + x^{\lambda g} + \ldots + x^{\lambda g^{p-2}}$. It is easily seen that Ω is divisible by $1 - x^p$, hence by $\frac{1-x^p}{1-x}$; on the other hand $f\left(x^{\lambda}\right)$ is, because g is a primitive root modulo p, divisible by $1 - x^{\lambda p}$, hence by $\frac{1-x^{\lambda p}}{1-x}$. Thus $f\left(x^{\lambda}\right)$ will be divisible by $\frac{1-x^p}{1-x}$ if

$$\frac{1 - x^{\lambda p}}{1 - x} \equiv 0 \pmod{\frac{1 - x^p}{1 - x}}$$

For a proof we have to distinguish two cases. (I) λ and p are coprime. Then $y\lambda = hp + 1$ for integers y and h, hence

$$\frac{1 - x^{\lambda p}}{1 - x} : \frac{1 - x^p}{1 - x} = \frac{1 - x^{\lambda p}}{1 - x} \cdot \frac{1 - x^{y\lambda}}{1 - x^{\lambda}} - x \frac{1 - x^{\lambda p}}{1 - x^{\lambda}} \cdot \frac{1 - x^{hp}}{1 - x^p}$$

and this implies that $f\left(x^{\lambda}\right)$ is divisible by $\frac{1-x^p}{1-x}$. (II) λ and p are not coprime. Then

$$f\left(x^{\lambda}\right) - p = x^{\lambda} \left\{ (x^g - 1) + \left(x^{g^2} - 1\right) + \ldots + \left(x^{g^{p-2}} - 1\right) \right\},$$

and this immediately implies that $f\left(x^{\lambda}\right) - p$ is divisible by $\frac{1-x^p}{1-x}$ Collecting everything and recalling that $g^0 + 1, g + 1, \ldots, g^{p-2} + 1$ represent the numbers $2, 3, \ldots, p$ in some order, we can deduce from (3.6)

$$\Omega = G^2 - (-1)^{\frac{p-1}{2}} f\left(x^{g^{\frac{p-1}{2}}+1}\right) \equiv 0 \pmod{\frac{1 - x^p}{1 - x}} \tag{3.7}$$

or, if Z denotes a polynomial in x,

$$G^2 - (-1)^{\frac{p-1}{2}} p = \frac{1 - x^p}{1 - x} Z \tag{3.8}$$

From (3.8) we immediately deduce

$$G^{q-1} - (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} = \frac{1-x^p}{1-x} Y \tag{3.9}$$

3. Using Eqs. (3.3),(3.4),(3.8) and (3.9), the reciprocity law can be proved easily. First we observe that (3.3) and (3.4) imply

$$qGX = G^{q+1} - G\left\{(1-x^p)\,W + \left(\frac{q}{p}\right) G\right\}$$

where X denotes a polynomial in x defined by (3.2) as

$$G^q - G_q = qX$$

Moreover, from (3.9) we get

$$qGX = \left\{(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} + \frac{1-x^p}{1-x} Y\right\} G^2 - G\,(1-x^p)\,W - \left(\frac{q}{p}\right) G^2$$

or, using (3.8) we get,

$$\begin{aligned} qGX =& (-1)^{\frac{p-1}{2}} p \left\{(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right)\right\} \\ &+ \frac{1-x^p}{1-x}\left\{Z\left((-1)^{\frac{p-1}{2}} q^{\frac{p-1}{2}} - \left(\frac{q}{p}\right)\right) + YG^2 - WG(1-x)\right\} \end{aligned} \tag{3.10}$$

According to (3.1), G has degree $p-1$. If we put $GX = \frac{1-x^p}{1-x} U + T$, where U and T are polynomials in x, then T will be a polynomial of degree less than $p-1$. Plugging the last equation into (3.10) we get

$$\begin{aligned} & qT - (-1)^{\frac{p-1}{2}} p \left\{(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\tfrac{q}{p}\right)\right\} \\ &= \tfrac{1-x^p}{1-x}\left\{Z\left[(-1)^{\frac{p-1}{2}} q^{-1} 2p^{\frac{q-1}{2}} - \left(\tfrac{q}{p}\right)\right]\right. \\ &\qquad \left. + YG^2 - WG(1-x) - qU\right\} \end{aligned} \tag{3.11}$$

where the degree of the left-hand side is less than $p-1$. Now Z, Y, W are polynomials in x, hence the degree of the right-hand side is bigger than $p-1$.
Thus the equation above can hold only if both sides vanish. Thus we find

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

or

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right) \equiv 0 \pmod{q}$$

and this is exactly what we wanted to prove. ■

Third Proof. Let p and $q > p$ be two distinct positive odd primes. For $2n+1 = 1, 3, 5 \ldots 4q-2$, choose m in such a way that

$$(2n+1)p - 2mq = r \tag{3.12}$$

where r is an odd integer between q and $-q$. Let μ denote the number of negative values of r; then clearly $\left(\frac{p}{q}\right) = (-1)^{\mu}$. Among the residues in (3.12), we single out those that lie

between $+p$ and $-p$. As a condition for this he gets the equation $(2n'+1)\,q - 2m'p = r$, or, by adding and subtracting pq in (3.12):

$$(p-2m)q - (q-2m-1)p = r. \tag{3.13}$$

This implies that r is between $+p$ and $-p$ in (3.12) for $p-2m = 1, 3, \ldots, p-2$ that is, for $m = 1, 2, \ldots, \frac{p-1}{2}$ Now replace μ by v and switch the roles of p and q; then $\left(\frac{q}{p}\right) = (-1)^v$ Moreover it is seen that v can be derived from (3.13) in the same way as μ from (3.12).

Thus $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ will have the same or the opposite sign according as the number of residues r between $-p$ and $-q$ is even or odd. For such residues $-q < (2n+1)p - 2mq < -p$ we get by putting $m = n-k$ and $p = q-2a$:

$$2m+1 < \frac{k+1}{\alpha}q < 2n+2. \tag{3.14}$$

Thus the number of these negative residues r is equal to the number of fractions $\frac{q}{\alpha}\ \frac{2q}{\alpha}, \ldots, \frac{\alpha-1}{\alpha}\cdot q$ for which the greatest integer contained in them is odd. Now the sum of the fractions with equal distance to the beginning and the end is q, and in particular odd. Thus the sum of the greatest integers belonging to these fractions is even, thus they are either both odd or both even.

1. If $\alpha \equiv 1 \pmod 2$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
2. If $\alpha \equiv 0 \bmod 2$, then we have to take the middle term in the series of fractions into account.

- For $q = 4n+1$ we find $\lfloor(\frac{q}{1}\rfloor) = n$, hence $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
- For $q = 4n+3$, on the other hand, we get $\lfloor(\frac{q}{2}\rfloor) = 2n+1$, hence $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Collecting these two cases we see that

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

Now $p = q - 2\alpha$ shows

$$\begin{aligned}(\alpha-1)\frac{q-1}{2} &= \frac{q-1}{2}\left(\frac{p-1}{2} - \frac{q-1}{2} - 1\right) = \frac{q-1}{2}\frac{q-1}{2} - \frac{q-1}{2}\cdot\frac{q-3}{2} \\ &\equiv \frac{q-1}{2}\frac{q-1}{2} \pmod 2\end{aligned}$$

which is what we wanted to prove. ■

Fourth Proof. Let p be a positive odd prime and ρ a primitive root of $x^p = 1$. Then

$$\frac{x^p-1}{x-1} = \left(x-\rho^2\right)\left(x-\rho^4\right)\cdots\left(x-\rho^{2(p-1)}\right) = 1 + x + x^2 + \ldots + x^{p-1} \tag{3.15}$$

and plugging in $x = 1$ yields

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

Raising this equation to the $\frac{q-1}{2}^{th}$ power we get

$$p^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\prod_{\alpha=1}^{(p-1)/2}\frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}} \equiv \left(\frac{p}{q}\right) \pmod q \tag{3.16}$$

where q denotes a positive odd prime distinct from p. The individual factors of $\prod_{\alpha=1}^{(p-1)/2} \frac{\rho^{\alpha q}-\rho^{-\alpha q}}{\rho^{\alpha}-\rho^{-\alpha}}$ are positive or negative according as αq is congruent to a positive or negative minimal residue modulo p. Applying Gauss's Lemma to (3.16) then gives

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

as desired. ■

4. Primes as a Sum of Squares

Our main goal in this section is to answer the following question:

Which primes can be written in the form $x^2 + ny^2$ where $x, y \in \mathbb{Z}$ and $n = 1, 2, 3$?

In particular, we want to prove the following theorems of Fermat for odd primes p:

$$\begin{aligned} p = x^2 + y^2, &\quad x, y \in \mathbb{Z} \;\Leftrightarrow\; p \equiv 1 \pmod 4 \\ p = x^2 + 2y^2, &\quad x, y \in \mathbb{Z} \;\Leftrightarrow\; p \equiv 1, 3 \pmod 8 \\ p = x^2 + 3y^2, &\quad x, y \in \mathbb{Z} \;\Leftrightarrow\; p = 3 \text{ or } p \equiv 1 \pmod 3. \end{aligned}$$

Lemma 4.1. *Let p be a prime and n be an integer not dividing n. Then there are relatively prime integers x and y such that $p \mid x^2 + ny^2$ if and only if $\left(\frac{-n}{p}\right) = 1$.*

Proof. Suppose that p divides such a number x^2+ny^2. Then $x^2 \equiv -ny^2 \pmod p$ since x and y are relatively prime, it follows that $p \nmid y$. The integers modulo p form a field, so that $yb \equiv 1 \pmod p$ for some b. Multiplying our congruence by b^2, we see that $(xb)^2 \equiv -n \pmod p$, which implies that $\left(\frac{-n}{p}\right) = 1$. The other direction is trivial, and the lemma is proved. ■

Thus we want to find the congruence conditions on p that imply that $\left(\frac{-n}{p}\right) = 1$. We see that the way to unify the congruence conditions is to work modulo $4n$ and look at primes in certain ranges. Working with $n = 1, 2, 3$, we get the following:

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4$$

$$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1, 3 \pmod 8$$

$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \pmod 3.$$

The key problem here is to find the $\pm$'s. For example, $11 \equiv -9 \pmod{20}$ and $-3 \equiv 25 \pmod{28}$. So for $n = -3, -5, -7$, we get the following:

$$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{12}$$

$$\left(\frac{5}{p}\right) = 1 \iff p \equiv \pm 1, \pm 9 \pmod{20}$$

$$\left(\frac{7}{p}\right) = 1 \iff p \equiv \pm 1, \pm 9, \pm 25 \pmod{28}.$$

Notice that all these numbers are perfect squares! But before we get too excited, let's try another case:

$$\left(\frac{6}{p}\right) = 1 \iff p \equiv \pm 1, \pm 5 \pmod{24}.$$

Similarly, 10 and 14 don't work either. So why does it work for $3, 5, 7$ but not $6, 10, 14$. The obvious difference is that the former are prime. From this we get the following conjecture:

Conjecture 4.2. *If p and q are distinct odd primes, then*

$$\left(\frac{q}{p}\right) = 1 \iff p \equiv \pm\beta^2 \text{for some odd } \beta.$$

Theorem 4.3. *Conjecture 4.2 is equivalent to the Law of Quadratic Reciprocity.*

Proof. Let p and q be distinct odd primes, and set $p^* = (-1)^{(p-1)/2}p$. We have that quadratic reciprocity is equivalent to

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

since each side equals ± 1, it follows that quadratic reciprocity can be written as the equivalence

$$\left(\frac{q}{p}\right) = 1 \Leftrightarrow \left(\frac{p^*}{q}\right) = 1$$

and comparing this to Conjecture 4.2, it thus suffices to show

$$p \equiv \pm\beta^2 \pmod 4 q \Leftrightarrow \left(\frac{p^*}{q}\right) = 1. \tag{4.1}$$

Note that $\beta^2 \equiv 1 \pmod 4$ since β is odd. Thus the $\pm$ sign in (4.1) must be $(-1)^{(p-1)/2}$, and we then have

$$\begin{aligned} p \equiv \pm\beta^2 \pmod 4 q &\Leftrightarrow p \equiv (-1)^{(p-1)/2}\beta^2 \pmod 4 q \\ &\Leftrightarrow p^* \equiv \beta^2 \pmod 4 q. \end{aligned}$$

Now, to prove (4.1), suppose that $p^* \equiv \beta^2 \pmod 4 q$. This implies $p^* \equiv \beta^2 \pmod q$ so that $(p^*/q) = 1$ follows immediately. Conversely, if $(p^*/q) = 1$, then $p^* \equiv \alpha^2 \pmod q$ for some α. Letting $\beta = \alpha$ or $\alpha + q$, depending on whether α is odd or even, we obtain $p^* \equiv \beta^2 \pmod 4 q$, and the theorem is proved. ∎

We state the general case for $x^2 + ny^2$ where $n = 1, 2, 3$ as the following theorem.

Theorem 4.4. *Let p be an odd prime $a^2 + nb^2$ where $n = 1, 2, 3$ and a, b are relatively prime integers. Then p can be written in the form $x^2 + ny^2$.*

Proof. We first state the following crucial lemma:

Lemma 4.5. *Let $q = x^2 + ny^2$ where n a positive integer, and suppose that q divides a number $N = a^2 + nb^2$, where a and b are relatively prime. If either q is prime, or $q = 4$ and $n = 3$, then $N/q = c^2 + nd^2$, where c and d are relatively prime.*

Proof. Let us first consider the case where q is prime. Since q divides both $x^2N = x^2\left(a^2 + nb^2\right)$ and $a^2q = a^2\left(x^2 + ny^2\right)$, it divides their difference

$$x^2\left(a^2 + nb^2\right) - a^2\left(x^2 + ny^2\right) = n\left(x^2b^2 - a^2y^2\right) = n(xb - ay)(xb + ay).$$

Since q is prime, it must divide one of these factors.

If $q \mid n$, then $q = n$ since $q = x^2 + ny^2$. Hence $n \mid N = a^2 + nb^2$, so that $n \mid a$, i.e. $a = nd$. Then $N = n^2d^2 + nb^2$, which implies $N/q = b^2 + nd^2$, as desired.

If $q \mid xb-$ ay or $q \mid xb+ay$, we can assume that the former holds by changing the sign of y. Then $xb - ay = dq = d\left(x^2 + ny^2\right)$. This implies that

$$xb - dx^2 = ay + dny^2 = y(a + ndy) \tag{4.2}$$

from which we conclude that $x \mid y(a+ndy)$. Since x and y are relatively prime (q is prime), we must have $x \mid a + ndy$, i.e.,

$$a + ndy = cx \tag{4.3}$$

so that $a = cx - ndy$. Substituting (4.3) into (4.2), we obtain

$$x(b - dx) = y(cx).$$

which implies that $b = dx + cy$.

However, we also have the famous identity

$$\left(c^2 + nb^2\right)\left(x^2 + ny^2\right) = (cx - ndy)^2 + n(dx + cy)^2.$$

Using the above formulas for a and b, this becomes

$$\left(c^2 + nd^2\right) q = a^2 + nb^2 = N,$$

and we get $\frac{N}{q} = c^2 + nd^2$ as desired.

Since a and b are relatively prime, we get that c and d are also relatively prime.

It remains to consider the case $n = 3$ and $q = 4$. Here, we have $4 \mid a^2 + 3b^2$, so that a and b have the same parity. since a and b are relatively prime, they must be odd. since $4 = 1^2 + 3 \cdot 1^2$, the argument for the prime case (with $x = y = 1$) would work, provided that $4 \mid b - a$ or $4 \mid b + a$. But the latter holds for any pair of odd numbers, which proves the lemma in this case. ■

To complete the proof of Theorem 2.1, consider an odd prime p dividing $a^2 + nb^2$ where a and b are relatively prime. Assume that p itself is not of this form. We will show that there is an odd prime $q < p$ with exactly the same properties. We would then be done by Fermat's principle of infinite descent: applying the same argument to q would give us $q' < q$, and continuing we would get an infinite decreasing sequence $p > q > q' > \cdots$ of positive integers, which contradicts the well-ordering property.

To produce q, we work with $a^2 + nb^2$. It is divisible by p, and remains so if we replace a and b by $a - kp$ and $b - \ell p$ respectively. Furthermore, we may choose k and ℓ so that $|a - kp| < \frac{p}{2}$ and $|b - \ell p| < \frac{p}{2}$ because p is odd. Thus we may assume that $p \mid a^2 + nb^2$ where $|a| < \frac{p}{2}$ and $|b| < \frac{p}{2}$. Since $n \leq 3$, it follows that $a^2 + nb^2 < (\frac{p}{2})^2 + 3(\frac{p}{2})^2 = p^2$. Thus $a^2 + nb^2$ can be written as

$$a^2 + nb^2 = pq_1 \cdots q_r \tag{4.4}$$

where the primes q_i all satisfy $q_i < p$. We claim that one of these q_i's is odd and not of the form $x^2 + ny^2$.

To prove this, assume not for the sake of contradiction. Then all of the odd q_i 's can be written as $x^2 + ny^2$, so that by repeatedly applying Lemma 4.5 we can eliminate all of the odd q_i's from (4.4). This leaves us with

$$a^2 + nb^2 = 2^a p$$

If $n = 1$ or 2, we can also apply Lemma 4.5 to $2 = 1^2 + 1^2 = 0^2 + 2 \cdot 1^2$ to eliminate factors of 2, showing that $p = a^2 + nb^2$, a contradiction. If $n = 3$, the case $q = 4$ of Lemma 4.5 shows that we can reduce to either $p = a^2 + 3b^2$ or $2p = a^2 + 3b^2$. It remains to show that the latter

case cannot occur. But $p \mid a^2 + 3b^2$ implies $\left(\frac{-3}{p}\right) = 1$, which by quadratic reciprocity means $p \equiv 1 \bmod 3$, so that $2p \equiv 2 \pmod 3$. Yet $2p = a^2 + 3b^2$ implies $2p \equiv a^2 \equiv 1 \pmod 3$, and thus we have a contradiction.

This completes the proof of Theorem 4.4. ■

This finishes our proof of the Fermat's three theorems.

5. Modular Divisor Functions

Definition 5.1. We define $\tau(a, p)$ the number of ordered pairs of integers (x, y) such that

$$0 < x < \frac{1}{2}p, \qquad 0 < y < \frac{1}{2}p, \qquad xy \equiv a \pmod p.$$

Proposition 5.2. *If p is an odd prime and a is an integer not divisible by p, then a is a quadratic residue* (mod p) *if and only if $\tau(a, p)$ is odd.*

Proof. If (x, y) is a pair counting towards $\tau(a, p)$, then (y, x) is also a pair counting towards $\tau(a, p)$. It follows that there is an even number of pairs (x, y) with $x \neq y$ counting towards $\tau(a, p)$. If a is a quadratic residue modulo p, so that $a \equiv x_0^2 \bmod p$ for some integer x_0, then

$$x^2 \equiv a \bmod p \iff x \equiv \pm x_0 \bmod p$$

so there is a unique integer x with $0 < x < \frac{1}{2}p$ such that $x^2 \equiv a \bmod p$, and it follows that $\tau(a, p)$ is odd. If a is not a quadratic residue modulo p then there are no integers x such that $x^2 \equiv a \bmod p$, and it follows that $\tau(a, p)$ is even. This completes the proof. ■

Lemma 5.3. *Let p and q be distinct odd primes and*

$$\tilde{p} = \frac{p-1}{2}, \qquad \tilde{q} = \frac{q-1}{2}.$$

Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if and only if $\overline{pq}$ is even.

Proof. Given an integer n with $|n| < \frac{1}{2}pq$, we define a pair of integers $(\rho(n), \rho'(n))$ as follows: if n is divisible by p then $\rho(n) = 0$; if n is not divisible by p then $\rho(n)$ is the unique integer such that

$$0 < |\rho(n)| < \frac{1}{2}p, \quad n\rho(n) \equiv q \bmod p$$

if n is divisible by q then $\rho'(n) = 0$; if n is not divisible by q then $\rho'(n)$ is the unique integer such that

$$0 < |\rho'(n)| < \frac{1}{2}q, \quad n\rho'(n) \equiv p \bmod q.$$

For distinct integers n_1 and n_2 in the interval $\left(-\frac{1}{2}pq, \frac{1}{2}pq\right)$ we have $n_1 \equiv n_2 \bmod p$ or $n_1 \equiv n_2 \bmod q$, from which it follows that $\rho(n_1) \neq \rho(n_2)$ or $\rho'(n_1) \neq \rho'(n_2)$. The pairs $(\rho(n), \rho'(n))$ therefore take distinct values, so they take each of the pq possible values exactly once. In particular, let S be the set of integers n with $|n| < \frac{1}{2}pq$ such that $\rho(n)\rho'(n) < 0$; then S has $2\tilde{p}\tilde{q}$ members. Clearly $n \in S$ if and only if $-n \in S$, so half of the members of S are positive; thus there are $\tilde{p}\tilde{q}$ integers n with $0 < n < \frac{1}{2}pq$ such that $\rho(n)\rho'(n) < 0$ Now let T be the set of integers n with $0 < n < \frac{1}{2}pq$ such that $\rho(n) > 0$. Let u be the number of integers n in T such that $\rho'(n) = 0$, let v be the number such that $\rho'(n) > 0$, and let w be the number such that $\rho'(n) < 0$, so that T has $u + v + w$ members all together. We will show that the value of $u + v + w$ determines the value of $\left(\frac{q}{p}\right)$. Indeed the members n of T which are less than

$\frac{1}{2}p$ correspond to the pairs (x, y) which count towards $\tau(q, p)$(take $x = n$ and $y = \rho(n)$), so T has $\tau(q, p)$ members less than $\frac{1}{2}p$. On the other hand, the interval $\left(\frac{1}{2}p, \frac{1}{2}pq\right)$ has length $p\tilde{q}$, so the equation $\rho(n) = i$ has $\tilde{q}$ solutions with $\frac{1}{2}p < n < \frac{1}{2}pq$ for each given integer i with $1 \leq i \leq \tilde{p}$, and it follows that T has $\tilde{p}\tilde{q}$ members greater than $\frac{1}{2}p$. since T has $u + v + w$ members all together, this gives us

$$\tau(q, p) + \tilde{p}\tilde{q} = u + v + w.$$

From Proposition 1 we see that $\left(\frac{q}{p}\right) = 1$ if and only if $u + v + w - \tilde{p}\tilde{q}$ is odd Next we show that u is odd. Indeed, u is the number of multiples n of q with $0 < n < \frac{1}{2}pq$ such that $\rho(n) > 0$. These multiples correspond to the pairs (x, y) which count towards $\tau(1, p)$ (take $x = n/q$ and $y = \rho(n)$), so $u = \tau(1, p)$. since 1 is a quadratic residue modulo p, it follows from Proposition 1 that u is odd. Therefore $\left(\frac{q}{p}\right) = 1$ if and only if $v + w - \tilde{p}\tilde{q}$ is even.

Analogously, let w' be the number of integers n with $0 < n < \frac{1}{2}pq$ such that $\rho(n) < 0$ and $\rho'(n) > 0$; then $\left(\frac{p}{q}\right) = 1$ if and only if $v + w' - \tilde{p}\tilde{q}$ is even, and it follows that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ if and only if $w + w'$ is even. But $w + w'$ is the number of integers n with $0 < n < \frac{1}{2}pq$ such that $\rho(n)\rho'(n) < 0$, so $w + w' = \tilde{p}\tilde{q}$ as already observed. Therefore $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ if and only if $\tilde{p}\tilde{q}$ is even. This completes the proof. ■

Remark 5.4. Note that $\left(\frac{a}{p}\right) = (-1)^{\tau(a,p)-1}$.

We define U_p as the set of nonzero integers such that $|n| < \frac{1}{2}p$ and ρ_p^a as the permutation of U_p given by

$$i\rho_p^a(i) \equiv a \pmod{p}.$$

Proposition 5.5. *Let a be an integer, and p be a prime. Then we have*

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

where sgn(σ) denotes the sign of permutation σ.

Proof. We see that U_p has $\tau(a, p)$ positive members with positive images under ρ_p^a, so U_p has $\frac{1}{2}(p-1)-\tau(a, p)$ positive members with negative images under ρ_p^a. Clearly $\rho_p^a(-i) = -\rho_p^a(i)$ for all i in U_p, so the sign of ρ_p^a is $(-1)^{[(p-1)/2]-\tau(a,p)}$. Writing sgn σ for the sign of a permutation σ, we see that

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

as desired. ■

Let π_p^a be the permutation of U_p given by

$$\pi_p^a(i) \equiv ai \pmod{p}.$$

Proposition 5.6 (Zolotarev's Lemma)**.** *Let a be an integer and p be a prime. Then we have*

$$\left(\frac{a}{p}\right) = sgn\pi_p^a$$

Proof. Note that we have $\pi_p^a = \rho_p^1 \cdot \rho_p^a$ which implies $\operatorname{sgn} \pi_p^a = \operatorname{sgn} \rho_p^1 \cdot \operatorname{sgn} \rho_p^a$. We also have $\operatorname{sgn} \rho_p^1 = (-1)^{(p-3)/2}$ because 1 is a quadratic residue modulo p. So we get

$$\left(\frac{a}{p}\right) = \operatorname{sgn} \pi_p^a$$

as desired. ■

Note that both Propositions 5.5 and 5.6. give the same information in different ways.

6. Composite Moduli

Our goal in this section is to generalize the Legendre Symbol and allowing composite moduli.

We first state the Chinese Remainder Theorem.

Theorem 6.1 (Chinese Remainder Theorem)**.** *Let $m_1, m_2, \ldots, m_k$ be pairwise coprime integers and $a_1, a_2, \ldots, a_k$ be arbitrary integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo M where $M = m_1 m_2 \cdots m_k$.

Let m and a be relatively prime integers where m is odd. We will prove a is a quadratic residue modulo m if and only if a is a quadratic residue modulo p for every prime dividing m. By Theorem 6.1, it suffices to to consider congruences modulo prime powers.

Theorem 6.2. *Let R be a ring and $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial with coefficients in R. Then*

$$f(x+h) = f(x) + f'(x)h + r(x,h)h^2$$

where r(x,h) is a polynomial in two variables x and h with coefficients in R.

Proof. This is just a standard calculation. Expanding $f(x+h)$ by the binomial theorem, we obtain

$$\begin{aligned} f(x+h) &= \sum_{i=0}^{n} a_i (x+h)^i \\ &= \sum_{i=0}^{n} a_i \sum_{j=0}^{i} \binom{i}{j} x^{i-j} h^j \\ &= \sum_{j=0}^{n} \sum_{i=j}^{n} \binom{i}{j} a_i x^{i-j} h^j \\ &= \sum_{i=0}^{n} a_i x^i + \sum_{i=1}^{n} i a_i x^{i-1} h + \sum_{j=2}^{n} \sum_{i=j}^{n} \binom{i}{j} a_i x^{i-j} h^j \\ &= f(x) + f'(x)h + r(x,h)h^2 \end{aligned}$$

where

$$r(x,h)=\sum_{j=2}^{n}\sum_{i=j}^{n}\left(\begin{array}{c} i \\ j \end{array}\right)a_i x^{i-j}h^{j-2}$$

is a polynomial in x and h with coefficients in R. ■

Theorem 6.3 (Hensel's Lemma)**.** *Let p be a prime and $f(x)$ be a polynomial of degree n and leading coefficient not divisible by p. If there exists an a such that*

$$f(x_1)\equiv 0 \pmod{p}$$

and

$$f'(x_1)\not\equiv 0 \pmod{p},$$

then for every $k\geq 2$, there exists an x_k such that

$$f(x_k)\equiv 0 \pmod{p^k}$$

and

$$x_k\equiv x_{k-1} \pmod{p^{k-1}}.$$

Proof. The proof is by induction on k. We begin by constructing x_2 There exist integers u_1 and v_1 such that $f(x_1)=u_1p$ and $f'(x_1)=v_1\neq 0\ (\mathrm{mod}p)$. We shall prove that there exists an integer y_1 such that $f(x_1+\ y_1p)\equiv 0 \pmod{p^2}$ By Theorem 6.2, there exists a polynomial $r(x,h)$ with integer coefficients such that

$$\begin{aligned} f(x_1+y_1p) &= f(x_1)+f'(x_1)\,y_1p+r(x_1,y_1p)\,p^2 \\ &= u_1p+v_1y_1p+r(x_1,y_1p)\,p^2 \\ &\equiv u_1p+v_1y_1p \quad \left(\mathrm{mod}p^2\right) \end{aligned}$$

Therefore, there exists an integer y_1 such that

$$f(x_1+y_1p)\equiv 0 \quad \left(\mathrm{mod}p^2\right)$$

if and only if the linear congruence

$$v_1y\equiv -u_1 \pmod{p}$$

is solvable. We see that this congruence does have a solution y_1 because $(v_1,p)=1$. Let

$$x_2=x_1+y_1p$$

Then

$$f(x_2)\equiv 0 \pmod{p} \quad \text{and} \quad x_2\equiv x_1 \pmod{p}$$

Let $k\geq 3$, and assume that we have constructed integers $x_2,\ldots,x_{k-1}$ such that

$$f(x_i)\equiv 0 \quad \left(\mathrm{mod}p^i\right) \quad \text{and} \quad x_i\equiv x_{i-1} \quad \left(\mathrm{mod}p^{i-1}\right)$$

for $i=2,\ldots,k-1$. There exists an integer u_{k-1} such that

$$f(x_{k-1})=u_{k-1}p^{k-1}$$

Let $f'(x_{k-1})=v_{k-1}$. since $x_{k-1}\equiv x_1 \pmod{p}$, it follows that

$$v_{k-1}=f'(x_{k-1})\equiv f'(x_1)\not\equiv 0 \pmod{p}$$

Applying Theorem 6.2 with $t = x_{k-1}$ and $h = y_{k-1}p^{k-1}$, we obtain

$$\begin{aligned} &f\left(x_{k-1} + y_{k-1}p^{k-1}\right) \\ &= f\left(x_{k-1}\right) + f'\left(x_{k-1}\right) y_{k-1}p^{k-1} + r\left(x_{k-1}, y_{k-1}p^{k-1}\right) y_{k-1}^2 p^{2k-2} \\ &\equiv u_{k-1}p^{k-1} + v_{k-1}y_{k-1}p^{k-1} \pmod{p^k} \end{aligned}$$

It follows that

$$f\left(x_{k-1} + y_{k-1}p^{k-1}\right) \equiv 0 \pmod{p^k}$$

if and only if there exists an integer y_{k-1} such that

$$v_{k-1}y_{k-1} \equiv -u_{k-1} \pmod{p}$$

This last congruence is solvable, since $(v_{k-1}, p) = 1$. ■

Theorem 6.4. *Let p be an odd prime and a be an integer not divisible by p. If $\left(\frac{a}{p}\right) = 1$, then $\left(\frac{a}{p^k}\right) = 1$ for every $k \geq 1$.*

Proof. Consider the polynomial $f(x) = x^2 - a$ and its derivative $f'(x) = 2x$. If a is a quadratic residue modulo p, then there exists an integer x_1 such that $x_1 \neq 0 \pmod{p}$ and $x_1^2 \equiv a \pmod{p}$. Then $f\left(x_1\right) \equiv 0 \pmod{p}$ and $f'\left(x_1\right) \neq 0 \pmod{p}$. By Hensel's lemma, the polynomial congruence $f(x) \equiv 0 \pmod{p^k}$ is solvable for every $k \geq 1$, and so a is a quadratic residue modulo p^k for every $k \geq 1$. ■

7. Quadratic Reciprocity Law for Jacobi Symbol

The Jacobi Symbol is a natural generalization of the Legendre Symbol where modulus is composite (briefly explored in the last section).

Let n be an odd integer and k be relatively prime to n. We define

$$\left(\frac{k}{n}\right) = \prod_{i=1}^{t} \left(\frac{k}{p_i}\right)^{e_i}$$

where $n = \prod_{i=1}^{t} p_i^{e_i}$. However, note that $\left(\frac{a}{n}\right) = 1$ does not imply that a is a quadratic residue modulo n.

Theorem 7.1. *Let n be an odd positive integer and $a \in \mathbb{Z}$ be relatively prime to n. Then if a is a quadratic residue modulo n, then $\left(\frac{a}{n}\right) = 1$. The converse does not hold if n is not prime.*

Proof. Suppose that a is a quadratic residue modulo n, i.e. the equation $x^2 \equiv a(\mathrm{mod}\, n)$ has a solution. Let $n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_t^{et}$ be the prime factorization of n. Let $m_i = p_i^{e_i}$ for each i. By the Chinese remainder theorem, the equation $x^2 \equiv a \left(\mathrm{mod} m_i\right)$ has a solution for each $i = 1, 2, \cdots, t$. it then follows that the equation $x^2 \equiv a \left(\mathrm{mod} p_i\right)$ has a solution too for each $i = 1, 2, \cdots, t$. Hence the Legendre symbol $\left(\frac{a}{p_i}\right) = 1$ for each i. It follows that the Jacobi symbol $\left(\frac{a}{n}\right) = 1$. ■

Lemma 7.2. *Let a and b be odd positive integers. Then following two conditions hold*

$$\tfrac{a-1}{2} \times \tfrac{b-1}{2} \equiv \tfrac{ab-1}{2} (\mathrm{mod} 2)$$

$$\tfrac{a^2-1}{8} \times \tfrac{b^2-1}{8} \equiv \tfrac{(ab)^2-1}{8} (\mathrm{mod} 2)$$

Proof. The lemma is established by the following derivation:

$$\frac{ab-1}{2} - \left[\frac{a-1}{2} + \frac{b-1}{2}\right] = \frac{ab-a-b+1}{2} = \frac{(a-1)(b-1)}{2}$$

$$\frac{(ab)^2-1}{8} - \left[\frac{a^2-1}{8} + \frac{b^2-1}{8}\right] = \frac{(ab)^2-a^2-b^2+1}{8} = \frac{\left(a^2-1\right)\left(b^2-1\right)}{8}$$

Because both a and b are odd integers, the right-hand-side of both equations are even integers and thus $\equiv 0 \pmod 2$. ■

Proposition 7.3. *The Jacobi Symbol is multiplicative when the bottom argument is fixed, namely,*

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

Proof. This follows from the definition of the Jacobi Symbol and corresponding properties of the Legendre Symbol. ■

Proposition 7.4. *The Jacobi Symbol is multiplicative when the upper argument is fixed, namely,*

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

Proof. This follows from the definition of the Jacobi Symbol and corresponding properties of the Legendre Symbol. ■

The Jacobi Reciprocity Law is a three-part statement:

Theorem 7.5 (Jacobi Reciprocity Law)**.**

(1) 1.*If a and b are odd relatively prime integers, then* $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$.
(2) 2.$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
(3) 3.$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

Proof. For the first part,

let $a = p_1 \times p_2 \times \cdots \times p_w$ and $b = q_1 \times q_2 \times \cdots \times q_t$ be their prime factorizations. Note that the primes p_i are not necessarily distinct and the primes q_i are not necessarily distinct. However, $p_i \neq q_j$ since a and b are relatively prime. Consider the following derivation of the

product $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)$

$$\begin{aligned}
\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_{i=1}^{t}\left(\frac{a}{q_i}\right)\prod_{j=1}^{w}\left(\frac{b}{p_j}\right) \\
&= \prod_{i=1}^{t}\prod_{j=1}^{w}\left(\frac{p_j}{q_i}\right)\prod_{j=1}^{w}\prod_{i=1}^{t}\left(\frac{q_i}{p_j}\right) \\
&= \prod_{i=1}^{t}\prod_{j=1}^{w}\left(\frac{p_j}{q_i}\right)\prod_{i=1}^{t}\prod_{j=1}^{w}\left(\frac{q_i}{p_j}\right) \\
&= \prod_{i=1}^{t}\prod_{j=1}^{w}\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right) \\
&= \prod_{i=1}^{t}\prod_{j=1}^{w}(-1)^{\frac{p_j-1}{2}\cdot\frac{q_j-1}{2}} \\
&= (-1)^{E}
\end{aligned}$$

where

$$E = \sum_{i,j}\left[\frac{p_j-1}{2}\times\frac{q_i-1}{2}\right].$$

Theorem 7.5 is established after the quantity E is simplified as follows:

$$\begin{aligned}
\sum_{i,j}\left[\frac{p_j-1}{2}\times\frac{q_i-1}{2}\right] &= \sum_{j}\left[\sum_{i}\frac{q_i-1}{2}\right]\frac{p_j-1}{2} \\
&\equiv \sum_{j}\left[\frac{b-1}{2}\right]\frac{p_j-1}{2} \text{ Use Lemma 7.2} \\
&\equiv \frac{b-1}{2}\sum_{j}\frac{p_j-1}{2} \\
&\equiv \frac{b-1}{2}\frac{a-1}{2} \pmod 2 \quad \text{Use Lemma 7.2}
\end{aligned}$$

as desired.

For the second part, the proof is by induction on the number of prime factors of n. If n is a prime, then it is done. So we assume $n = p_1 \times p_2$ (not necessarily distinct). Consider the following derivation:

$$\begin{aligned}
\left(\frac{-1}{n}\right) &= \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right) \\
&= (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}} \\
&= (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}} \\
&\equiv (-1)^{\frac{p_1p_2-1}{2}} \text{ Use Lemma 7.2} \\
&\equiv (-1)^{(n-1)/2} \pmod 2
\end{aligned}$$

It is a straightforward argument that whenever the property is true for n being a product of k primes, the property is true for n being a product of $k+1$ primes. Thus we are done.

For the third part, the proof is by induction on the number of prime factors of n. The most important case is the one consisting of two prime factors.

$$\begin{aligned}\left(\frac{2}{n}\right) &= \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\\ &= (-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}\\ &= (-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}}\\ &\equiv (-1)^{\frac{(p_1p_2)^2-1}{8}} \text{ Use Lemma 7.2}\\ &\equiv (-1)^{\frac{n^2-1}{8}} (\text{mod} 2)\end{aligned}$$

With the 2-case established, it is straightforward to carry out the remainder of the induction proof of this part.

■

References

[1] Li, Chao. *Quadratic Reciprocity* July 2012. Columbia University, http://www.math.columbia.edu/~chaoli/tutorial2012/Lecture2.pdf.

[2] Goldmakher, Leo. *Quadratic Reciprocity* Department of Mathematics, University of Toronto, https://web.williams.edu/Mathematics/lg5/C15W13/QR.pdf

[3] Lynn, Ben. *Number Theory* Stanford University, https://crypto.stanford.edu/pbc/notes/numbertheory/.

[4] Baumgart, Oswald. *The Quadratic Reciprocity Law* 2015, https://www.springer.com/gp/book/9783319162829.

[5] Steiner, Richard. *Modular Divisor Functions and Quadratic Reciprocity* Dec 2017. The American Mathematical Monthly, https://www.tandfonline.com/doi/abs/10.4169/000298910X485978.

[6] Nathanson, Melvyn B. *Elementary Methods in Number Theory* 2017. Graduate Texts in Mathematics, https://www.springer.com/gp/book/9780387989129.

[7] Tangedal, Brett A. *Eisenstein's Lemma and Quadratic Reciprocity for Jacobi Symbols* Apr 2018. Mathematics Magazine, https://www.tandfonline.com/doi/abs/10.1080/0025570X.2000.11996820.

[8] Sun, Zhi-Hong. *Congruences for $q^{[p/8]}$ (mod p) under the condition $4n^2p = x^2 + qy^2$* 2015. International Journal of Number TheoryVol. 11, No. 04, pp. 1301-1312 (2015), https://worldscientific.com/doi/10.1142/S1793042115500700

[9] Daileda, R. C. *The Law of Quadratic Reciprocity* Trinity University, Number Theory, http://ramanujan.math.trinity.edu/rdaileda/teach/s18/m3341/lectures/quadratic_reciprocity.pdf

[10] Stephen, Humble. *A Proof of the Law of Reciprocity for Jacobi Symbols* May 1965. The Mathematical Gazette Vol. 49, No. 368 (May, 1965), pp. 169-170, https://www.jstor.org/stable/3612310?seq=1

[11] Cox, David A. *Quadratic Reciprocity: Its Conjecture and Application* May 1988. The American Mathematical Monthly Vol. 95, No. 5 (May, 1988), pp. 442-448, https://www.jstor.org/stable/2322482?seq=1

[12] *Lecture 34: Quadratic reciprocity* Lecture Notes https://dornsife.usc.edu/assets/sites/1176/docs/PDF/430F19/430_Lecture_34.pdf

[13] Aigner, Martin, Ziegler, Günter M. *Proofs from THE BOOK* 2018 https://www-springer-com.stanford.idm.oclc.org/gp/book/9783662572641