# QUADRATIC RECIPROCITY I

PETE L. CLARK

We now come to the most important result in our course: the law of quadratic reciprocity, or, as Gauss called it, the **aureum theorema** ("golden theorem").

Many beginning students of number theory have a hard time appreciating this golden theorem. I find this quite understandable, as many first courses do not properly prepare for the result by discussing enough of the earlier work which makes quadratic reciprocity an inevitable discovery and its proof a cause for celebration. Happily, our study of quadratic rings and the quadratic form $x^2 - Dy^2$ has provided excellent motivation. There are also other motivations, involving (what we call here) the direct and inverse problems regarding the Legendre symbol.

A faithful historical description of the QR law is especially complicated and will not be attempted here; we confine ourselves to the following remarks. The first traces of QR can be found in Fermat's Lemma that $-1$ is a square modulo an odd prime $p$ iff $p \equiv 1 \pmod 4$, so date back to the mid 1600's. Euler was the first to make conjectures equivalent to the QR law, in 1744. He was unable to prove most of his conjectures despite a steady effort over a period of about 40 years. Adrien-Marie Legendre was the first to make a serious attempt at a proof of the QR law, in the late 1700's. His proofs are incomplete but contain much valuable mathematics. He also introduced the Legendre symbol in 1798, which as we will see, is a magical piece of notation with advantages akin to Leibniz's $dx$ in the study of differential calculus and its generalizations. Karl Friedrich Gauss gave the first complete proof of the QR law in 1797, at the age of 19(!). His argument used mathematical induction(!!). The proof appears in his groundbreaking work *Disquisitiones Arithmeticae* which was written in 1798 and first published in 1801.

The circle of ideas surrounding quadratic reciprocity is so rich that I have found it difficult to "linearize" it into one written presentation. (In any classroom presentation I have found it useful to begin each class on the subject with an inscription of the QR Law on a side board.) In the present notes, the ordering is as follows. In §1 we give a statement of the quadratic reciprocity law and its two supplements in elementary language. Then in §2 we discuss the Legendre symbol, restate QR in terms of it, and discuss (with proof) some algebraic properties of the Legendre symbol which are so important that they should be considered part of the quadratic reciprocity package. In §3 we return to our "unfinished theorems" about representation of primes by $|x^2 - Dy^2|$ when $\mathbb{Z}[\sqrt{D}]$ is a PID: using quadratic reciprocity, we can state and prove three **bonus theorems** which complement Fermat's Two Squares Theorem. In §4 we define and discuss the "direct and inverse problems" for the Legendre symbol and show how quadratic reciprocity is useful for both of these, in particular for rapid computation of Legendre symbols. More precisely, the computation would be rapid if we could somehow avoid having to factor numbers

Thanks to Laura Nunley for pointing out a typo.

quickly, and §5 explains how we can indeed avoid this by using an extension of the Legendre symbol due to Jacobi.

## 1. Statement of Quadratic Reciprocity

Notational comment: when we write something like $p \equiv a, b, c \pmod{n}$, what we mean is that $p \equiv a \pmod{n}$ or $p \equiv b \pmod{n}$ or $p \equiv c \pmod{n}$. (I don't see any other vaguely plausible interpretation, but it doesn't hurt to be careful.)

**Theorem 1.** *(Quadratic Reciprocity Law) Let $p \neq q$ be odd primes. Then:*
*(i) If $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, $p$ is a square mod $q$ iff $q$ is a square mod $p$.*
*(ii) If $p \equiv q \equiv 3 \pmod{4}$, $p$ is a square mod $q$ iff $q$* ***is not*** *a square mod $p$.*

**Theorem 2.** *(First Supplement to the Quadratic Reciprocity Law) If $p$ is an odd prime, then $-1$ is a square modulo $p$ iff $p \equiv 1 \pmod{4}$.*

**Theorem 3.** *(Second Supplement to the Quadratic Reciprocity Law) If $p$ is an odd prime, then $2$ is a square modulo $p$ iff $p \equiv 1, 7 \pmod{8}$.*

## 2. The Legendre Symbol

### 2.1. Defining the Legendre Symbol.

We now define a piece of notation introduced by Adrien-Marie Legendre in 1798. There is no new idea here; it is "merely notation", but is an example of how incredibly useful well-chosen notation can be.

For $n$ an integer and $p$ an odd prime, we define the **Legendre symbol**

$$\left(\frac{n}{p}\right) := \begin{cases} 0, & \text{if } n \equiv 0 \pmod{p} \\ 1, & \text{if } n \bmod p \text{ is a nonzero square} \\ -1, & \text{if } n \bmod p \text{ is nonzero and not a square} \end{cases}$$

We must of course distinguish the Legendre symbol $\left(\frac{n}{p}\right)$ from the rational number $\frac{n}{p}$. To help with this, I recommend that $(\frac{n}{p})$ be read "$n$ on $p$".[1]

Example 1: To compute $(\frac{12}{5})$, we must first observe that 5 does not divide 12 and then determine whether 12 is a nonzero square modulo 5. Since $12 \equiv 2 \pmod{5}$ and the squares modulo 5 are $1, 4$, the answer to the question "Is 12 a nonzero square modulo 5?" is negative, so $(\frac{12}{5}) = -1$.

Example 2: To compute $(\frac{101}{97})$ – note that 97 is prime! – we observe that 97 does not divide 101. Since $101 \equiv 4 \equiv 2^2 \pmod{97}$, the answer to the question "Is 101 a nonzero square modulo 97?" is positive, so $(\frac{101}{97}) = 1$.

Example 3: To compute $(\frac{97}{101})$ – note that 101 is prime! – we observe that 101 certainly does not divide 97. However, at the moment we do not have a very efficient way to determine whether 97 is a square modulo 101: our only method is to compute all of the squares modulo 101. Some calculation reveals that $400 = 20^2 = 3 \cdot 101 + 7$, so $20^2 \equiv 97 \pmod{101}$. Thus 97 is indeed a square modulo 101, so $(\frac{97}{101}) = 1$.

[1] There is in fact some relationship with "$n$ divided by $p$", since if we divide $n$ by $p$ with remainder, getting $n = qp + r$ with $0 \leq r < p$, then the Legendre symbols $(\frac{n}{p})$ and $(\frac{r}{p})$ are equal.

### 2.2. Restatement of Quadratic Reciprocity Using the Legendre Symbol.

**Theorem 4.** *(Quadratic Reciprocity Restated) Let $p$ and $q$ be distinct odd primes.*
*a)* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.
*b)* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
*c)* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

### 2.3. Some elementary group theory related to the Legendre symbol.

Let $p$ be an odd prime, and consider the group $U(p) = (\mathbb{Z}/p\mathbb{Z})^\times$; since $p$ is prime, this is precisely the multiplicative group of nonzero elements of $\mathbb{Z}/p\mathbb{Z}$ under multiplication: in particular, it is a finite commutative group of even order $p-1$.

In fact $U(p)$ is a cyclic group: there exists some element $g \in U(p)$ such that every element $x \in U(p)$ is of the form $g^i$ for a unique $0 \leq i < p$. In classical number-theoretic language the element $g$ (often viewed as an integer, $0 < g < p$) is a **primitive root modulo p**. This is nontrivial to prove. We do in fact give the proof elsewhere in these notes, but in at least one version of the course, we are covering quadratic reciprocity before the material on the Euler $\varphi$ function which we use in our proof of this fact. So we would like to give a more elementary discussion of some weaker properties of $U(p)$ that suffice for our needs here.

Let $(G, \cdot)$ be a commutative group, and let $n$ be a positive integer. The map

$$[n] : G \to G, \ x \mapsto x^n$$

which sends each element to its $n$th power, is a homomorphism. We denote the kernel of the map by $G[n]$; this is the subgroup of all elements of order dividing $n$, often called the **n-torsion subgroup** of $G$. We put $G^n = [n](G)$, the image of the homomorphism, which is the subgroup of elements of $G$ which are $n$th powers. There is thus a canonical isomorphism

$$[n] : G/G[n] \xrightarrow{\sim} G^n.$$

Now further suppose that $G$ is finite. Then

$$\#G^n = \frac{\#G}{\#G[n]}.$$

Consider for a moment the case $\gcd(n, \#G) = 1$. Suppose $g \in G[n]$. Then the order of $g$ divides $n$, whereas by Lagrange's theorem, the order of $g$ divides $\#G$, so the order of $G$ divides $\gcd(n, \#G) = 1$: so $g = 1$ and $G[n] = \{1\}$. Thus $\#G^n = \#G$ so $G^n = G$. So in this case every element of $G$ is an $n$th power.

We remark in passing that the converse is also true: if $\gcd(n, \#G) > 1$, then $G[n]$ is nontrivial, so the subgroup $G^n$ of $n$th powers is proper in $G$. We do not need this general result, so we do not prove it here, but mention only that it can be deduce from the classification theorem for finite commutative groups.

Now we specialize to the case $G = U(p) = (\mathbb{Z}/p\mathbb{Z})^\times$ and $n = 2$. Then

$$G[2] = \{x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \mid x^2 = 1\}.$$

We claim that $G[2] = \{\pm 1\}$. First, note that since $p$ is odd, $1 \not\equiv -1 \pmod{p}$, i.e., $+1$ and $-1$ are distinct elements in $\mathbb{Z}/p\mathbb{Z}$, and they clearly both square to 1, so that $G[2]$ contains at least the two element subgroup $\{\pm 1\}$. Conversely, as above every element of $G[2]$ is a root of the quadratic polynomial $t^2 - 1$ in the field $\mathbb{Z}/p\mathbb{Z}$. But a polynomial of degree $d$ over any field (or integral domain) can have at most $d$ distinct roots: whenever $p(a) = 0$, applying the division algorithm to $p(t)$ and $t - a$ gives $p(t) = q(t)(t-a) + c$, where $c$ is a constant, and plugging in $t = a$ gives $c = 0$. Thus we can factor out $t - a$ and the degree decreases by 1. Therefore $\#G[2] \leq 2$, and since we have already found two elements, we must have $G[2] = \{\pm 1\}$.

So $G^2$ is an index two subgroup of $G$ and the quotient $G/G^2$ has order two. Like any group of order 2, it is uniquely isomorphic to the group $\{\pm 1\}$ under multiplication. Thus we have defined a surjective group homomorphism

$$L : U(p) \to \{\pm 1\},$$

namely we take $x \in U(p)$ to the coset $xU(p)^2$. So, $L(x) = 1$ if $x$ is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$ and $L(x) = -1$ otherwise. But this means that for all $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, $L(x) = (\frac{x}{p})$. Thus we have recovered the Legendre symbol in terms of purely algebraic considerations and also shown that

$$\forall x, y \in U(p), \left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right).$$

In fact we can give a (useful!) second description of the Legendre symbol using power maps. To see this, consier the map

$$[\frac{p-1}{2}] : U(p) \to U(p).$$

We claim that the kernel of this map is again the subgroup $U(p)^2$ of squares, of order $\frac{p-1}{2}$. On the one hand, observe that $U(p)^2 \subset U(p)[\frac{p-1}{2}]$: indeed $(x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$ by Lagrange's Theorem. Conversely, the elements of $U(p)[\frac{p-1}{2}]$ are roots of the polynomial $t^{\frac{p-1}{2}} - 1$ in the field $\mathbb{Z}/p\mathbb{Z}$, so there are at most $\frac{p-1}{2}$ of them. Thus $U(p)^2 = U(p)[\frac{p-1}{2}]$. By similar reasoning we have $U(p)^{\frac{p-1}{2}} \subset \{\pm 1\}$, hence we can view $[\frac{p-1}{2}]$ as a homomorphism

$$L' = [\frac{p-1}{2}] : U(p) \to \{\pm 1\}.$$

Since the kernel of $L'$ is precisely the subgroup $U(p)^2$ and there are only two possible values, it must be the case that $L'(x) = -1$ for all $x \in U(p) \setminus U(p)^2$. In other words, we have $L'(x) = (\frac{x}{p})$.

The following result is essentially a summary of the above work. We strongly recommend that the reader take time out to convince herself of this.

**Proposition 5.** *The following hold for any $a, b \in \mathbb{Z}$ and any odd prime $p$.*
*a)* $\left(\frac{a}{p}\right)$ *depends only on the residue class of $a$ modulo $p$.*
*b) (Euler)* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
*c)* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Note that by taking $a = -1$ in Proposition 5b), we get

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

This is precisely the First Supplement to the quadratic reciprocity law, which we have now proved twice (in the handout on Pythagorean triples we called it **Fermat's Lemma** and proved it using Wilson's theorem).

### 2.4. A faster proof using the cyclicity of $U(p)$.

If we happen to know that the unit group $U(p) = (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, we can give a much more streamlined proof of Proposition 5. First note that part a) is obvious from the definition. Moreover, if we assume part b), part c) follows immediately:

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

So it remains to prove part b). But now suppose that $g$ is a generator for the group $U(p)$, so that we can write $a = g^i$. Then $a^{\frac{p-1}{2}} = g^{\frac{i(p-1)}{2}}$.
Case i: $i$ is even. Then on the one hand $a = (g^{\frac{i}{2}})^2$ is a square in $U(p)$. On the other hand $p-1 \mid i\frac{p-1}{2}$, so that $g^{\frac{i(p-1)}{2}} = 1$ by Lagrange's theorem.
Case 2: $i$ is odd. Then on the on the one hand $a = g^i$ is not a square in $U(p)$: for instance, we know that the subgroup of squares has exactly $\frac{p-1}{2}$ elements, and we found $\frac{p-1}{2}$ distinct elements in Case 1 above: $\{g^{2k} \mid 0 \leq k < \frac{p-1}{2}\}$. On the other hand, since $i$ is odd, $p-1 \nmid i\frac{p-1}{2}$, so that $a^{\frac{p-1}{2}} = g^{\frac{i(p-1)}{2}} \neq 1$. Since its square is 1, it must therefore be equal to $-1$.

## 3. Motivating Quadratic Reciprocity I: Bonus Theorems

### 3.1. Some unfinished theorems.

An excellent motivation for the quadratic reciprocity law is provided by our previous study of the equation $x^2 - Dy^2 = p$. Recall we have proved:

**Theorem 6.** *Let $D$ be squarefree integer different from $0$ and $1$. Assume that the ring $\mathbb{Z}[\sqrt{D}]$ is a UFD. Then, for a prime number $p$, TFAE:*
*(i) There exist $x, y \in \mathbb{Z}$ such that $p = |x^2 - Dy^2|$.*
*(ii) There exists $x \in \mathbb{Z}$ such that $D \equiv x^2 \pmod{p}$.*

Moreover we know that $\mathbb{Z}[\sqrt{D}]$ is a UFD when $D \in \{-1, \pm 2, 3\}$. The case $D = -1$ yielded Fermat's two squares theorem given the additional knowledge that $-1$ is a square modulo an odd prime $p$ iff $p \equiv 1 \pmod{4}$. To complete our "bonus theorems" we need answers to the following questions:

- For which odd primes $p$ is it the case that $-2$ is a square modulo $p$?
- For which odd primes $p$ is it the case that 2 is a square modulo $p$?
- For which odd primes $p$ is it the case that 3 is a square modulo $p$?

Comparing with the answer for $D = -1$, one might hope that the answer is in terms of some congruence condition on $p$. Let's look at some data:

The odd primes $p < 200$ for which $-2$ is a square modulo $p$ are:

$$3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97, 107, 113, 131, 137, 139, 163, 179, 193.$$

Notice that these are precisely the primes $p < 200$ with $p \equiv 1, 3 \pmod 8$.

For $D = 2, 3$ we will give some data and allow you a chance to find the pattern.

The odd primes $p < 200$ for which 2 is a square modulo $p$ are:

$$7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, 127, 137, 151, 167, 191, 193, 199.$$

The odd primes $p < 200$ for which 3 is a square modulo $p$ are:

$$3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109, 131, 157, 167, 179, 181, 191, 193.$$

While we are at it, why not a bit more data?

The odd primes $p < 200$ for which 5 is a square modulo $p$ are:

$$5, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109, 131, 139, 149, 151, 179, 181, 191, 199.$$

The odd primes $p < 200$ for which 7 is a square modulo $p$ are:

$$3, 7, 19, 29, 31, 37, 47, 53, 59, 83, 103, 109, 113, 131, 137, 139, 149, 167, 193, 197, 199.$$

### 3.2. **With the help of quadratic reciprocity.**

We already know that a prime $p$ is of the form $|x^2 - 2y^2|$ iff $(\frac{2}{p}) = 1$, and the second supplement tells us that this latter conditions holds iff $p \equiv 1, 7 \pmod 8$. While we are here, let's deal with the absolute value: it happens that $\mathbb{Z}[\sqrt{2}]$ contains an element of norm $-1$, namely $1 - \sqrt{2}$:

$$N(1 - \sqrt{2}) = (1 - \sqrt{2})(1 + \sqrt{2}) = 1^2 - 2 \cdot 1^2 = -1.$$

From this and the multiplicaitivity of the norm map, it follows that if we can represent any integer $n$ in the form $x^2 - 2y^2$, we can also represent it in the form $-(x^2 - 2y^2)$, and conversely. From this it follows that the absolute value is superfluous and we get the following result.

**Theorem 7.** *(First Bonus Theorem) A prime number $p$ is of the form $x^2 - 2y^2$ iff $p = 2$ of $p \equiv 1, 7 \pmod 8$.*

Now let's look at the case of $D = -2$, i.e., the form $x^2 + 2y^2$. Since $2 = 0^2 + 2 \cdot 1^2$, 2 is of of the form $x^2 + 2y^2$. Now assume that $p$ is odd. We know that an odd prime $p$ is of the form $x^2 + 2y^2$ iff $(\frac{-2}{p}) = 1$. We don't have a single law for this, but the multiplicativity of the Legendre symbol comes to our rescue. Indeed,

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

so

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

Case 1: $(\frac{-1}{p}) = (\frac{2}{p}) = 1$. By the first and second supplements, this occurs iff $p \equiv 1 \pmod 4$ and $p \equiv 1, 7 \pmod 8$, so iff $p \equiv 1 \pmod 8$.

Case 2: $(\frac{-1}{p}) = (\frac{2}{p}) = -1$. By the first and second supplements, this occurs iff $p \equiv 3 \pmod 4$ and $p \equiv 3, 5 \pmod 8$, so iff $p \equiv 3 \pmod 8$. Thus:

**Theorem 8.** *(Second Bonus Theorem) A prime number $p$ is of the form $x^2 + 2y^2$ iff $p = 2$ or $p \equiv 1, 3 \pmod 8$.*

Now let's look at the case of $D = 3$, i.e., the form $|x^2 - 3y^2|$. We know that a prime $p$ is of this form iff $(\frac{3}{p}) = 1$. Now we use QR itself, and there are two cases:
Case 1: If $p \equiv 1 \pmod 4$, then $(\frac{3}{p}) = 1$ iff $p \equiv 1 \pmod 3$.
Case 2: If $p \equiv 3 \pmod 4$, then $(\frac{3}{p}) = 1$ iff $p \equiv -1 \pmod 3$.

The congruence conditions can be consolidated by going mod 12. We get that $(\frac{3}{p}) = 1$ iff $p \equiv 1, 11 \pmod{12}$. Again we can ask what happens when we try to remove the absolute value. This time things work out somewhat differently.

**Theorem 9.** *(Third Bonus Theorem) For a prime $p$, the equation $x^2 - 3y^2 = p$ has an integral solution iff $p \equiv 1 \pmod{12}$. The equation $3y^2 - x^2 = p$ has an integral solution iff $p = 2$, $p = 3$ or $p \equiv 11 \pmod{12}$.*

*Proof.* First we deal with the two exceptional cases. Suppose $p = 2$: reducing $x^2 - 3y^2 = 2$ modulo 3, we get $x^2 \equiv 2 \pmod 3$, which we know has no solution. Note that on the other hand $3(1)^2 - 1^2 = 2$, so 2 is of the form $3y^2 - x^2$. Now suppose $p = 3$: reducing $x^2 - 3y^2 = 3$ modulo 4, we get $x^2 - 3y^2 \equiv x^2 + y^2 \equiv 3 \pmod 4$, which (as we have seen before) has no integral solution. On the other hand, $3 = 3(1)^2 - 0^2$, so 3 is of the form $3y^2 - x^2$.

Now suppose that $p > 3$. Since $\mathbb{Z}[\sqrt{3}]$ is a PID, we know that $p$ is of the form $p = |x^2 - 3y^2|$ iff 3 is a square modulo $p$, i.e., iff $p = 3$ or $(\frac{3}{p}) = 1$. By quadratic reciprocity, this last condition can be expressed as a congruence modulo $4 \cdot 3 = 12$, specifically $p \equiv \pm 1 \pmod{12}$. So if $p \equiv 1, 11 \pmod{12}$ then at least one of the following holds:

$$p = x^2 - 3y^2 \tag{1}$$

or

$$p = 3y^2 - x^2. \tag{2}$$

It turns out that for any prime $p$, exactly one of the two equations (1), (2) holds, which is extremely convenient: it means that we can always show that one of the equations holds by showing that the other one does not hold!

Indeed, if we reduce the equation $p = x^2 - 3y^2$ modulo 3: we get $p \equiv x^2 \pmod 3$, i.e., $(\frac{p}{3}) = 1$, so $p \equiv 1 \pmod 3$. So if $p \equiv 11 \pmod{12}$ then $p$ is not of the form $x^2 - 3y^2$ so must be of the form $3y^2 - x^2$. Simiarly, if we reduce the equation $p = 3y^2 - x^2$ modulo 3, we get $p \equiv -x^2 \equiv -1 \pmod 3$, so if $p \equiv 1 \pmod 3$ then 2 has no solution, so it must be that $p = x^2 - 3y^2$ does have a solution. □

A very similar argument establishes the following more general result.

**Theorem 10.** *Suppose $q \equiv 3 \pmod 4$ is a prime such that $\mathbb{Z}[\sqrt{q}]$ is a PID. Then the equation $x^2 - qy^2 = p$ has a solution iff $p \equiv 1 \pmod 4$ and $(\frac{p}{q}) = 1$.*

### 3.3. Auxiliary congruences.

The restriction to $q \equiv 3 \pmod 4$ in Theorem 10 may appear artificial. But those who have done their homework know better: in fact if $\mathbb{Z}[\sqrt{q}]$ is a PID, then we must have $q = 2$ (which we have already discussed) or $q \equiv 3 \pmod 4$. (Otherwise $\mathbb{Z}[\sqrt{q}]$ is not integrally closed.) A closer look reveals that the distinction between primes which are $1 \pmod 4$ and primes which are $3 \pmod 4$ is a central, albeit somewhat mysterious part, of the natural behavior of quadratic forms.

One way to see this is in terms of what I shall call **auxiliary congruences**. Namely, in our initial study of the equation $|x^2 - Dy^2| = p$, we did not consider all possible congruence obstructions (as e.g. in Legendre's Theorem) but only condition that we got upon reducing modulo $p$: namely that $D$ is a square modulo $p$. Notice that we could also reduce modulo $D$ to get some further conditions: more on this in a moment. But why didn't we reduce modulo $D$ before? The simple but strange answer is that we simply didn't need to: it happened that when $\mathbb{Z}[\sqrt{D}]$ is a PID, we were able to prove that the necessary condition that $D$ be a square modulo $p$ was also sufficient for $p$ to be of the form $|x^2 - Dy^2| = p$.

But this is rather surprising. Let's look closer, and to fix ideas let us take $p$ and $q$ distinct odd primes, and look at the equation

$$x^2 + qy^2 = p.$$

Then reducing modulo $p$ gives $(\frac{-q}{p}) = 1$, whereas reducing modulo $q$ gives $(\frac{p}{q}) = 1$. How do these two conditions interact with each other? Let's examine the cases:

Case 1: $p \equiv 1 \pmod 4$. Then $(\frac{-q}{p}) = (\frac{-1}{p})(\frac{q}{p}) = (\frac{q}{p}) = (\frac{p}{q})$. So the conditions are **redundant**.

Example: Take $q = 5$. Then the congruence conditions tell us that if $p \equiv 1 \pmod 4$ is of the form $x^2 + 5y^2$, we must have $(\frac{p}{5}) = 1$, i.e., $p \equiv 1, 4 \pmod 5$. Thus, every prime $p \equiv 1 \pmod 4$ which is represented by $x^2 + 5y^2$ lies in one of the two congruence classes $p \equiv 1, 9 \pmod 2 0$. As we know, $\mathbb{Z}[\sqrt{-5}]$ is *not* a PID, so nothing we have proved tells us anything about the converse, but the examples in section $\S X.X$ above show that for all $p < 200$, $p \equiv 1, 9 \pmod{20} \implies p = x^2 + 5y^2$. It is easy to extend the compuations to check this for all primes up to say $10^6$. In fact it is true, although we do not have the right techniques to prove it.

Example: Take $q = 3$. Then the congruence conditions tell us that if $p \equiv 1 \pmod 4$ is of the form $x^2 + 3y^2$, then $p \equiv 1 \pmod 3$. Again computations support that every prime $p \equiv 1 \pmod 1 2$ is of the form $x^2 + 3y^2$.

Case 2: $p \equiv 3 \pmod 4$. Then $(\frac{-q}{p}) = (\frac{-1}{p})(\frac{q}{p}) = -(\frac{q}{p})$. To compare this to the condition $(\frac{p}{q}) = 1$, we need to consider further cases.

Case 2a) Suppose also $q \equiv 1 \pmod 4$. Then $1 = (\frac{-q}{p}) = -(\frac{q}{p}) = -(\frac{p}{q})$, i.e., $(\frac{p}{q}) = -1$. This is **inconsistent** with $(\frac{p}{q}) = 1$, so we deduce that when $q \equiv 1 \pmod 4$, $p = x^2 + qy^2 \implies p \equiv 1 \pmod 4$.

This is a new phenomenon for us. Note that when $q = 5$, in conjunction with the above (unproved) result, we get the following

**Theorem 11.** *An odd prime $p$ is of the form $x^2 + 5y^2$ iff $p \equiv 1, 9 \pmod 2$0.*

Case 2b): Suppose also $q \equiv 3 \pmod 4$. Then $1 = (\frac{-q}{p}) = -(\frac{q}{p}) = (\frac{p}{q})$. Thus the two congruence conditions are **consistent** in this case.

Example: Let's reconsider $q = 3$. Nothing in our analysis ruled out a prime $p \equiv 3 \pmod 4$ (except $p = 3$) being of the form $x^2 + 3y^2$: the only congruence condition we found is the main one $1 = (\frac{-3}{p}) = \frac{p}{3}$, i.e., $p \equiv 1 \pmod 3$. In this case computations suggest that an odd prime $p$ is of the form $x^2 + 3y^2$ iff $p \equiv 1 \pmod 3$. Note that this is exactly the result that we would have gotten if $\mathbb{Z}[\sqrt{3}]$ were a UFD except that then 2 would also be of the form $x^2 + 3y^2$, which was exactly what we used to see that $\mathbb{Z}[\sqrt{3}]$ isn't a UFD! It turns out that we *can* prove this result with the techniques we have: an argument is sketched in the exercises.

These considerations have turned up more questions than answers. Our point is that the distinction between primes $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$ is something that is embedded quite deeply into the behavior of quadratic rings and quadratic equations. A proper understanding of this phenomenon goes under the heading **genus theory**, which was treated by Gauss in his *Disquisitiones Arithmeticae* and is intimately related to contemporary issues in number theory.

## 4. Motivating Quadratic Reciprocity II: Direct and Inverse Problems

### 4.1. **The direct and inverse problems.**

We wish to discuss "reciprocal" problems concerning quadratic residues, which can be phrased in terms of whether we regard the Legendre symbol $\left(\frac{n}{p}\right)$ as a function of its numerator or as a function of its denominator.

Direct problems: Fix an odd prime $p$.
direct problem A: Determine all integers which are squares modulo $p$.
direct problm B: Determine whether a given integer $n$ is a square modulo $p$.

By Proposition 5a), the answer only depends upon $n$ modulo $p$, so for fixed $p$ it is a finite problem: we know that exactly half of the elements of $\mathbb{F}_p^\times$ are squares, so for instance to compute all of them we could simply calculate $1^2, 2^2, \ldots, (p-1)^2$ modulo $p$.[2] However if $p$ is large this will take a long time, and it is natural to wonder whether there is a faster way of computing $\left(\frac{n}{p}\right)$ for some specific $n$.

inverse problem: Fix $n \in \mathbb{Z}$. For which odd primes $p$ is $\left(\frac{n}{p}\right) = 1$?

Example: The case $n = -1$ was needed to prove the two squares theorem. We found that $(\frac{-1}{p}) = 1$ iff $p \equiv 1 \pmod 4$. Note that, although our original proof was

[2] In fact this gives every square twice; we will get every square once by computing the squares up to $(\frac{p-1}{2})^2$, as we saw in the Handout on Sums of Two Squares.

more elementary, this follows immediately from Proposition 5b): $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

In contrast to the direct problems, the inverse problem is apparently an *infinite* problem. Moreover, the inverse problem comes up naturally in applications: indeed solving the inverse problem for $n = \pm 2, 3$ was exactly what we did in the last section in order to complete our study of the forms $x^2 - ny^2$.

### 4.2. With the help of quadratic reciprocity.

We now make two key observations. First: The Quadratic Reciprocity Law allows us to reduce the inverse problem to the direct problem A.

Example: Take $n = 5$. For which odd primes $p$ is 5 a square modulo $p$?

Answer: Since 5 is 1 (mod 4), $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, and we know what the squares are mod 5: $\pm 1$. Thus the answer is that 5 is a square modulo $p$ iff $p \equiv \pm 1 \pmod 5$.

Example: Take $n = 7$. For which odd primes $p$ is 7 a square modulo $p$?

Answer: Since 7 is 3 (mod 4), we need to distinguish two cases: $p \equiv 1 \pmod 4$ and $p \equiv -1 \pmod 4$. If $p \equiv 1 \pmod 4$, then $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$, so we just want $p$ to be a square modulo 7. The squares mod 7 are $1^2 \equiv 1, 2^2 \equiv 4$ and $3^2 \equiv 2$. We now have both a congruence condition mod 7 and a congruence condition mod 4: by the Chinese Remainder theorem, these conditions can be expressed by congruence conditions mod 28: namely we want $p \equiv 1, 9, 25 \pmod{28}$.

Next we consider the case $p \equiv -1 \pmod 4$. This time since $p$ and 7 are both $-1$ mod 4, QR tells us that $\left(\frac{7}{p}\right) = -1\left(\frac{p}{7}\right)$, so we want the nonsquares modulo 7, or $3, 5, 6$. Again we may combine these with the congruence $p \equiv -1 \pmod 4$ by going mod 28, to get $p \equiv 3, 19, 27$. So 7 is a square modulo $p$ iff

$$p \equiv 1,\ 3,\ 9,\ 19,\ 25,\ \text{or } 27 \pmod{28}.$$

The QR law leads to the following general solution of the inverse problem:

**Corollary 12.** *Let $q$ be any odd prime.*
*a) If $q \equiv 1 \pmod 4$, then $\left(\frac{q}{p}\right) = 1$ iff $p$ is congruent to a square modulo $q$ (so lies in one of $\frac{q-1}{2}$ residue classes modulo $q$).*
*b) If $q \equiv -1 \pmod 4$, then $\left(\frac{q}{p}\right) = 1$ iff $p \equiv \pm x^2 \pmod{4q}$ (so lies in one of $q-1$ out of the $2(q-1)$ reduced residue classes modulo $4q$).*

Corollary 12 was first conjectured by Euler and is in fact equivalent to the QR law. As we will not be using Corollary 12 in the sequel, we leave the proof as an exercise.

So much for the first observation. Here is the second:

The QR law yields an efficient algorithm for Direct Problem B.

This is best explained by way of examples.

Example: Suppose we want to compute $\left(\frac{7}{19}\right)$. Using QR we can "invert" the Legendre symbol, tacking on an extra factor of $-1$ because $7 \equiv 19 \equiv -1 \pmod 4$:

$$\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right).$$

We have reduced to a problem we know: 2 is not a square mod 5, so the final answer is $\left(\frac{7}{19}\right) = -(-1) = 1$.

Example:

$$\left(\frac{41}{103}\right) = \left(\frac{103}{41}\right) = \left(\frac{21}{41}\right) = \left(\frac{3}{41}\right)\left(\frac{7}{41}\right) = \left(\frac{41}{3}\right)\left(\frac{41}{7}\right)$$
$$= \left(\frac{-1}{3}\right)\left(\frac{-1}{7}\right) = -1 \cdot -1 = 1.$$

Example:

$$\left(\frac{79}{101}\right) = \left(\frac{101}{79}\right) = \left(\frac{22}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{11}{79}\right) =$$
$$1 \cdot \left(\frac{11}{79}\right) = -\left(\frac{79}{11}\right) = -\left(\frac{2}{11}\right) = -(-1) = 1.$$

Let us now stop and make an important observation: the quadratic reciprocity law along with its first and second supplements, together with parts a) and c) of Proposition 5, allows for a computation of the Legendre symbol $\left(\frac{n}{p}\right)$ in all cases. Indeed, it is multiplicative in the numerator, so we may factor $n$ as follows:

$$n = (-1)^{\epsilon} 2^a p^b p_1 \cdots p_r \cdot m^2,$$

where $\epsilon = \pm 1$, the primes $p_1, \ldots, p_r$ are distinct and prime to $p$, and $m$ is prime to $p$. If $b > 0$ then the symbol evaluates to 0. Otherwise we have

$$\left(\frac{n}{p}\right) = \left(\frac{-1}{p}\right)^{\epsilon} \left(\frac{2}{p}\right)^{a} \prod_i \left(\frac{p_i}{p}\right).$$

## 5. The Jacobi symbol

Computing Legendre symbols via the method of the previous section is, for moderately small values of $n$ and $p$, much faster and more pleasant to do by hand than computing the list of all $\frac{p-1}{2}$ quadratic residues mod $p$. However, when the numbers get larger a "hidden cost" of the previous calculation becomes important: the calculation requires us to do several factorizations, and factorization is the *ne plus ultra* of time-consuming number-theoretic calculations.

In fact it is not necessary to do any factorization at all, except to factor out the largest power of 2, which is computationally trivial (especially if the number is stored in binary form!). One can use a generalization of the Legendre symbol introduced in 1837 by Carl Gustav Jacob Jacobi (1804-1851).

For $a$ an integer and $b$ an odd positive integer, we define the **Jacobi symbol**

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right),$$

where $b = p_1 \cdots p_r$ is the factorization of $b$ into (not necessarily distinct!) primes.

**Warning**: If $a$ is a square modulo $b$, then $\left(\frac{a}{b}\right) = 1$, but the converse does not hold (you are asked to supply a counterexample in the homework). The Jacobi symbol is instead a "formal" generalization of the Legendre symbol, as is summarized by the following two results:

**Proposition 13.** *Let $a$, $a_1, a_2$ be integers and $b$, $b_1$, $b_2$ be odd positive integers.*
*a)* $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$ *if* $a_1 \equiv a_2 \pmod{b}$.
*b)* $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$.
*c)* $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.

**Theorem 14.** *(QR Law for the Jacobi Symbol) Let $a$ be an integer and $b$ an odd positive integer.*
*a)* $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.
*b)* $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.
*c) If $a$ is also odd and positive then*

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

The point is that the Jacobi symbol equals the Legendre symbol when the denominator is a prime, and is moreover completely determined by Proposition 13a) and Theorem 14. Therefore one can compute Legendre symbols by a process of repeated inversion and reduction of the numerator modulo the denominator, without worrying about whether the numerator or denominator is prime.

If $a$ and $b$ each have no more than $k$ digits, then computing the Jacobi symbol $\left(\frac{a}{b}\right)$ using the QR law requires no more than a constant times $k^2$ steps, or more succinctly, can be done in time $O(k^2)$.[3] In particular, when $b = p$ is prime, the algorithm takes $O(\log^2 p)$ steps so is **polynomial time** (in the number of digits of $p$), whereas computing all $\frac{p-1}{2}$ quadratic residues takes time $O(p)$.

Using the Euler relation $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ to compute $\left(\frac{a}{p}\right)$ is also rather efficient, as one can takie advantage of a **powering algorithm** to rapidly compute exponents modulo $p$ (the basic idea being simply to not compute the integer $a^{\frac{p-1}{2}}$ at all but rather to alternate raising $a$ to successively larger powers and reducing the result modulo $p$): this can be done in time $O(\log^3 p)$. For more information on this and many other topics related to number-theoretic algorithms, we recommend Henri Cohen's *A Course in Computational Algebraic Number Theory.*

## 6. A Reminder

Remember that we have not yet proved the Quadratic Reciprocity Law, nor the Second Supplement which computes $\left(\frac{2}{p}\right)$. We are, however, heavily invested in it, which makes us eager to see a proof, even if it will not be easy.

[3] The notation $O(f(x))$ is used in algorithmic complexity theory and also in analytic number theory to indicate a quantity which is bounded above by a constant times $f(x)$.