# WHAT IS A RECIPROCITY LAW?

B. F. WYMAN, Stanford University

**1. Introduction.** The Law of Quadratic Reciprocity has fascinated mathematicians for over 300 years, and its generalizations and analogues occupy a central place in number theory today. Fermat's glimmerings (1640) and Gauss's proof (1796) have been distilled to an amazing abstract edifice called **class field theory.**

As a graduate student I learned the great cohomological machine and studied **Artin's Reciprocity Law,** one form of which gives an isomorphism between two cohomology groups. A little later I read Shimura's paper [**19**], called "A non-solvable reciprocity law," and couldn't understand the title at all. Where were the cohomology groups? Why was Shimura's theorem a reciprocity law?

It was an embarrassing, but healthy ignorance, because it made me go back and figure out the number theory that lay behind all those cohomology groups. Such a reassessment is especially important nowadays, because it seems more and more certain that the *next* generalization of the Law of Quadratic Reciprocity will require new techniques, and nobody is quite sure which techniques will work.

In this paper I should like to discuss reciprocity laws from a rather general but very concrete point of view. Suppose $f(X)$ is a monic irreducible polynomial with integral coefficients, and suppose $p$ is a prime number. Reducing the coefficients of $f(X)$ modulo $p$ gives a polynomial $f_p(X)$ with coefficients in the field $\mathbf{F}_p$ of $p$ elements. The polynomial $f_p(X)$ may factor (even though the original $f(X)$ was irreducible). If $f_p(X)$ factors over $\mathbf{F}_p$ into a product of distinct linear factors, we say that $f(X)$ **splits completely modulo** $p$, and we define $\mathbf{Spl}(f)$ to be the set of all primes such that $f(X)$ splits completely modulo $p$.

The general **reciprocity problem** we shall be considering is: *Given* $f(X)$ *as above, describe the factorization of* $f_p(X)$ *as a function of the prime* $p$. Sometimes we ask for less: *give a rule to determine which primes belong to* $\mathrm{Spl}(f)$. This vague question is hard to make precise until it is answered. What is a "rule"? What is an acceptable method for describing the factorization of $f_p(X)$? Anyway, a satisfactory answer to this unsatisfactory question will be called a **reciprocity law.**

Quadratic polynomials are easiest to handle, and Section 2 shows how the usual Law of Quadratic Reciprocity gives a reciprocity law. (If it did not, our language would be all wrong.) Section 3 treats cyclotomic polynomials, and Sections 4 and 5 take up general results. It turns out that the reciprocity problem has been solved satisfactorily for polynomials which have an abelian Galois group, but that very little is known about polynomials whose Galois group is not abelian.

---

Bostwick Wyman received his Ph.D. at Berkeley in 1966 under G. Hochschild and A. Ogg. He was an Instructor at Princeton for two years and has been an Assistant Professor at Stanford since then. He spent a year's leave at the University of Oslo. His main research interest is algebraic number theory. *Editor.*

For an arbitrary polynomial $f(X)$ and a specific prime $p$, it only takes a finite number of steps to decide whether $p$ is in $\mathrm{Spl}(f)$. Sections 6 and 7 give a description of an efficient algorithm for doing this calculation and report on results obtained for a family of quintic polynomials. These results probably do *not* constitute a reciprocity law, and the last section tries to answer the main question, "What is a reciprocity law?"

*Prerequisites.* Section 2 assumes only knowledge of the Law of Quadratic Reciprocity. The later sections assume somewhat more: acquaintance with cyclotomic polynomials, Galois groups, and the division algorithm in polynomial rings. Parts of Sections 4 and 5 assume the rudiments of algebraic number theory, but they can be skipped.

*Notation.* We use $\boldsymbol{Z}$, $\boldsymbol{Q}$, and $\boldsymbol{C}$ for the integers, rational numbers, and complex numbers, respectively. If $q$ is a prime or prime power, then $\mathbf{F}_q$ is the field with $q$ elements. If $R$ is a ring, then $R[X]$ is the ring of polynomials with coefficients in $R$; mostly we deal with $\boldsymbol{Z}[X]$ and $\mathbf{F}_p[X]$.

**2. Quadratic Polynomials.** Suppose that $f(X)$ is an irreducible quadratic polynomial with integral coefficients. If $p$ is a prime number, let $f_p(X)$ be the corresponding polynomial in $\mathbf{F}_p[X]$ obtained by reducing the coefficients of $f(X)$ modulo $p$. The reduced polynomial $f_p(X)$ can factor in one of three ways:

(0) $f_p(X) = l(X)^2$, where $l(X)$ is linear.

(1) $f_p(X) = l_1(X) \cdot l_2(X)$, where $l_1(X)$ and $l_2(X)$ are two distinct linear polynomials. In this case we say that $f(X)$ **splits** modulo $p$.

(2) $f_p(X)$ is irreducible in $\mathbf{F}_p[X]$.

In this paper we shall stick to polynomials of the form $X^2 - q$, where $q$ is prime. If $f(X) = X^2 - q$, then Case (0) occurs modulo $p$ when $p = q$, and also when $p = 2$. (The prime 2 behaves strangely for quadratic polynomials.) To distinguish Cases (1) and (2) we need to know whether $q$ is a quadratic residue modulo $p$. If $q$ is a quadratic residue, and $q \equiv a^2 \pmod{p}$, we get $X^2 - q \equiv (X + a)(X - a) \pmod{p}$. This puts us in Case (1) if $p \neq 2$. If $q$ is not a quadratic residue, we are in Case (2).

Using the Legendre symbol, and ignoring the prime 2 and the exceptional Case (0) (a widespread practice!), we summarize:

(1) $X^2 - q$ splits modulo $p$ if $(q/p) = +1$.

(2) $X^2 - q$ is irreducible modulo $p$ if $(q/p) = -1$.

Remember that we are trying to describe the set $\mathrm{Spl}(X^2 - q)$ of primes $p$ such that $X^2 - q$ splits modulo $p$, and now we know that $p$ *is in* $\mathrm{Spl}(X^2 - q)$ *if and only if* $(q/p) = +1$.

The reader should still be skeptical, because this translation of the problem does not do much for us. The symbol $(q/p)$ is not easy to evaluate, and besides, if we change $p$ we have to start all over again. Since there are infinitely many primes $p$,

this naive approach requires an infinite amount of work to describe $\mathrm{Spl}(X^2 - q)$. Can we find a better description?

Since $q$ is fixed and $p$ varies, things would be better if we could use the symbol $(p/q)$ instead of $(q/p)$. For fixed $q$, the value of $(p/q)$ depends only on the residue class of $p$ modulo $q$. There are only $q$ residue classes, and therefore only $q$ symbols to evaluate. This suggests looking for a relationship between $(p/q)$ and $(q/p)$ in hopes of using $(p/q)$ to describe $\mathrm{Spl}(X^2 - q)$. Now you can guess where we are; we have sneaked up behind the Law of Quadratic Reciprocity. Legendre's statement goes like this [**10**, p. 455 ff.]:

THEOREM 2–1 (Law of Quadratic Reciprocity): *Let $p$ be an odd prime. Then*

1. $(1/p) = (-1)^P$, *where* $P = \frac{1}{2}(p-1)$.
2. $(2/p) = (-1)^R$, *where* $R = (p^2-1)/8$.
3. *If $q$ is another odd prime, then* $(q/p) = (-1)^{P \cdot Q}(p/q)$, *where* $P = \frac{1}{2}(p-1)$ *and* $Q = \frac{1}{2}(q-1)$.

Gauss gave the first proof of this theorem [**6**, Article 131 ff.], and a modern proof can be found in almost any number theory text, for example, Niven and Zuckerman [**17**, p. 74].

This venerable law is really exactly what we need to compute $\mathrm{Spl}(X^2 - q)$. We start with a less fancy but quite useful form of the theorem.

THEOREM 2–2. *Let $p$ and $q$ be distinct odd primes.*

1. *If* $q \equiv 1 \pmod 4$, *then* $(q/p) = (p/q)$.
2. *If* $q \equiv 3 \pmod 4$, *then* $(q/p) = \begin{cases} (p/q) \text{ if } p \equiv 1 \pmod 4 \\ -(p/q) \text{ if } p \equiv 3 \pmod 4. \end{cases}$

The derivation of Theorem 2–2 from Theorem 2–1 is an easy exercise.

Now we are ready to give a prescription for computing $(q/p)$ for fixed $q$ and variable $p$: First, compute $(b/q)$ for all integers $b$ such that $1 \leqq b \leqq q-1$. Second, given $p$, find the $b$ such that $1 \leqq b \leqq q-1$ and $b \equiv p \pmod q$. We have therefore $(b/q) = (p/q)$. Third, use the tables in Theorem 2 to convert knowledge of $(p/q)$ into knowledge of $(q/p)$.

*Example* 1. $q = 17$. The squares modulo 17 are 1, 2, 4, 8, 9, 13, 15, and 16, so that we have $(b/17) = +1$ for $b$ equal one of these, and $(b/17) = -1$ for $b = 3, 5, 6, 7, 10, 11, 12$, or 14. That is (second step), $(p/17) = +1$ if and only if $p \equiv 1, 2, 4, 8, 9, 13, 15$, or 16 (mod 17). Finally, (third step), $17 \equiv 1 \pmod 4$ so that $(17/p) = (p/17)$. If we return to the language of polynomials splitting modulo a prime, we can say that

$$p \in \mathrm{Spl}(X^2 - 17) \text{ if and only if}$$

$$p \equiv 1, 2, 4, 8, 9, 13, 15, \text{ or } 16 \pmod{17}.$$

That is, the set $\mathrm{Spl}(X^2 - 17)$ can be defined by "congruence conditions modulo 17."

*Example* 2. $q = 11$. By finding the quadratic residues modulo 11, we conclude that $(p/11) = +1$ if and only if $p \equiv 1, 3, 4, 5$, or 9 (mod 11). In this case $11 \equiv 3$ (mod 4) so $(11/p) = \pm(p/11)$ with a sign that depends on the residue of $p$ modulo 4. For example, $23 \equiv 1$ (mod 11), and $23 \equiv 3$ (mod 4), so that $(11/23) = -(23/11) = -(1/11) = -1$. On the other hand, $89 \equiv 1$ (mod 11) but $89 \equiv 1$ (mod 4) and $(11/89) = +(89/11) = +(1/11) = +1$. Using the Chinese Remainder Theorem, we see that the value of $(11/p)$ depends on the residue class of $p$ modulo 44, and after some calculation we get:

$$p \in \mathrm{Spl}(X^2 - 11) \text{ if and only if}$$

$$p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, \text{ or } 43 \pmod{44}.$$

In this case the set $\mathrm{Spl}(X^2 - 11)$ can be described by congruence conditions modulo 44.

The results of the last two examples are actually quite general.

THEOREM 2–3. *Suppose that $q$ is an odd prime. Then the set* $\mathrm{Spl}(X^2 - q)$ *can be defined by congruence conditions modulo $q$ if $q \equiv 1$* (mod 4) *and modulo $4q$ if $q \equiv 3$* (mod 4). *Furthermore,* $\mathrm{Spl}(X^2 - 2)$ *can be described by congruence conditions modulo* 8.

In this theorem the phrase "congruence conditions" is interpreted as in the examples. The first part follows from Theorem 2–2, and the second part from Theorem 2–1, part 2. Details are left as an exercise for the reader.

Theorem 2–3 shows that the Law of Quadratic Reciprocity gives a "reciprocity law" in the sense of Section 1. That is, it yields a nice description of sets $\mathrm{Spl}(f)$ for quadratic polynomials. In the next section we shall try to find such a reciprocity law for certain special polynomials (the *cyclotomic* ones) of higher degree.

**3. Cyclotomic polynomials.** Suppose $\zeta$ is a primitive $n$th root of unity; for instance, $\zeta = e^{2\pi i/n}$ is one choice. Then the minimal polynomial of $\zeta$ over $\boldsymbol{Q}$ is written $\Phi_n(X)$ and is called the ***n*-th cyclotomic polynomial**. One knows that $\Phi_n(X)$ has coefficients in $\boldsymbol{Z}$ and has degree $\phi(n)$, where $\phi$ is the Euler phi-function. It can be computed conveniently from the formula

$$X^n - 1 = \prod_{d|n} \Phi_d(X),$$

where the product runs are all divisors of $n$, including 1 and $n$ itself. For example, $\Phi_1(X) = X - 1$, and if $p$ is a prime, then $X^p - 1 = (X - 1) \cdot \Phi_p(X)$ and

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Proofs of these facts and more information about $\Phi_n(X)$ can be found in Lang [**14**, p. 206], van der Waerden [**20**, Sec. 53] and in many other algebra textbooks.

The goal of this section is a "reciprocity law" for these cyclotomic polynomials. We want a description of the set $\mathrm{Spl}(\Phi_n(X))$, and, just as in the quadratic case, the description will be given in terms of congruence conditions with respect to a modulus which depends on the polynomial. The theorem follows.

THEOREM (Cyclotomic Reciprocity Law). *The cyclotomic polynomial* $\Phi_n(X)$ *factors into distinct linear factors modulo* $p$ *if and only if* $p \equiv 1 \pmod{n}$.

First we give a lemma about finite fields, and then use the lemma to prove the theorem. To avoid excessive notation we also use the symbol $\Phi_n(X)$ to denote the cyclotomic polynomial with coefficients reduced modulo a prime $p$.

LEMMA. *Suppose* $p$ *is a prime number, and* $a$ *is an element of* $\mathbf{F}_p$ *with* $a^n = 1$. *If* $a^d \neq 1$ *for all proper divisors* $d$ *of* $n$, *then* $X - a$ *divides* $\Phi_n(X)$ *in* $\mathbf{F}_p[X]$.

*Proof.* The relation $X^n - 1 = \prod_{d|n}\Phi_d(X)$ holds in $\mathbf{F}_p$, so that $a^n - 1 = 0 = \prod_{d|n}\Phi_d(a)$. Since $\mathbf{F}_p$ is a field, it follows that $\Phi_m(a) = 0$ for some divisor $m$ of $n$, and that $a^m - 1 = \prod_{d|n}\Phi_d(a) = 0$. This gives $a^m = 1$ which can only happen if $m = n$. Therefore, $\Phi_n(a) = 0$, and $X - a$ divides $\Phi_n(X)$.

*Proof of theorem.* Recall that the multiplicative group $\mathbf{F}_p^*$ of non-zero elements of $\mathbf{F}_p$ is cyclic of order $p - 1$. Therefore, $\mathbf{F}_p^*$ has a cyclic subgroup of order $n$ if and only if $n$ divides $p - 1$. Such a subgroup has $\phi(n)$ generators, so that $\mathbf{F}_p^*$ contains $\phi(n)$ distinct primitive $n$th roots of 1 (these generators!) if and only if it contains one, and this happens exactly when $p \equiv 1 \pmod{n}$.

Now assume $p \equiv 1 \pmod{n}$, so that $\mathbf{F}_p$ contains $\phi(n)$ distinct primitive roots of 1. These must be roots of $\Phi_n(X)$, by the lemma, so that $\Phi_n(X)$ splits into a product of distinct linear factors.

Conversely, assume that $\Phi_n(X)$ splits into linear factors modulo $p$. If these factors are distinct, then $p$ cannot divide $n$ (exercise: start from Lang [**14**, p. 206]), and it follows easily that $X^n - 1$ also has distinct roots modulo $p$. Let $a$ be a root of $\Phi_n(X)$ in $\mathbf{F}_p$, so that $a^n = 1$. If $d$ is the smallest divisor of $n$ such that $a^d = 1$, then $\Phi_d(a) = 0$ by the lemma. If $d \neq n$, the basic relationship $X^n - 1 = \prod_{d|n}\Phi_d(X)$ shows that $a$ is at least a double root of $X^n - 1$, a contradiction. Therefore $a$ generates a cyclic subgroup of order $n$ in $\mathbf{F}_p^*$, and $p \mid n-1$. This completes the proof of the "cyclotomic reciprocity law."

**4. Abelian polynomials.** In the first two sections we saw that if $f(X)$ is a quadratic or cyclotomic polynomial, then the set $\mathrm{Spl}(f)$ can be described by congruences with respect to a certain modulus. This gives a rather precise solution to the vague "reciprocity problem."

Unfortunately, such a nice description of $\mathrm{Spl}(f)$ is not always possible. We can, however, describe exactly the set of polynomials for which congruence conditions give the answer we need.

First we must recall some Galois theory. Associated to each polynomial of degree

$n$ is the **root field** $K_f = Q(\alpha_1, \cdots, \alpha_n)$, where $\alpha_1, \cdots, \alpha_n$ are the complex roots of $f(X)$. (We avoid the more common term, "splitting field," because of possible confusion with polynomials "splitting modulo $p$.") The field $K_f$ is a finite Galois extension of $Q$, uniquely determined by $f(x)$. The Galois group of $K_f/Q$ is often called the **Galois group of $f(X)$**, and $f(X)$ is called an **abelian polynomial** if its Galois group is abelian.

The next theorem shows the importance this notion has for the reciprocity problem.

ABELIAN POLYNOMIAL THEOREM. *The set* $\mathrm{Spl}(f)$ *can be described by congruences with respect to a modulus depending only on* $f(X)$ *if and only if* $f(X)$ *is an abelian polynomial.*

Why should Galois groups have anything to do with polynomials splitting modulo primes? What are "congruence conditions" exactly? Enough machinery is developed in the rest of this section to establish the importance of the Galois groups, and to give a precise form of the theorem. A complete proof is far beyond the scope of this paper. In fact, the proof of the theorem involves almost all of "class field theory over the rationals." Perhaps the best avenue for an ambitious reader is to work through a basic text in algebraic number theory, and then go on to the cohomological treatment in Cassels and Fröhlich [3], or the analytic approaches of Lang [15], Weil [21], or Goldstein [7].

At this point we must escalate the prerequisites: the reader should be familiar with integral dependence, Dedekind domains, and the factorization of prime ideals in Galois extensions, or else be willing to suspend his disbelief. It is safe to skip this discussion and go on to Section 5.

Let $K$ be an algebraic extension of $Q$. The elements of $K$ whose (monic) minimal polynomial has coefficients in $Z$ make up the ring of **algebraic integers in $K$**, written $\mathcal{O}_K$. The ring $\mathcal{O}_K$ is a Dedekind domain if $K/Q$ is finite.

If $p$ is a prime in $Z$, the ideal $p\mathcal{O}_K$ factors uniquely into a product of prime ideals:

$$p\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_r.$$

If $\mathfrak{P}$ is one of the factors of $p$, the residue class ring $\mathcal{O}_K/\mathfrak{P}$ is a finite field extension of $Z/pZ$. This **residue class field extension** is cyclic, with Galois group generated by the **Frobenius map** $\phi$: $\phi(a) = a^p$ for all $a$ in $\mathcal{O}_K/\mathfrak{P}$.

Except for a finite number of exceptions (called **ramified primes**) the $\mathfrak{P}_i$ appearing in $p\mathcal{O}_K$ are all distinct. If $K/Q$ is Galois with group $G$, and $p$ is not ramified, then for each $\mathfrak{P}_i$ there is a unique $\sigma \in G$ such that $\sigma$ reduces to the Frobenius map modulo $\mathfrak{P}_i$. This automorphism is called the **Artin symbol** corresponding to $\mathfrak{P}$. We denote it by $\sigma_{\mathfrak{P}}$, so that the defining formula is

$$\sigma_{\mathfrak{P}}(a) \equiv a^p (\mathrm{mod}\, \mathfrak{P}) \text{ for all } a \in \mathcal{O}_K.$$

These Artin symbols $\sigma_{\mathfrak{P}}$ are not good enough for our purposes. We need to define an Artin symbol $\sigma_p$ corresponding to a prime number $p$ "downstairs." This is not possible in general, because different choices of the ideal $\mathfrak{P}$ may give different $\sigma_{\mathfrak{P}}$ in $G$. How are these various $\sigma_{\mathfrak{P}}$ related? If $\mathfrak{P}$ and $\mathfrak{Q}$ are two factors of $p\mathcal{O}_K$, then there is an automorphism $\tau$ in $G$ such that $\tau(\mathfrak{P}) = \mathfrak{Q}$. It turns out that $\sigma_{\mathfrak{Q}} = \tau\sigma_{\mathfrak{P}}\tau^{-1}$. All the $\sigma_{\mathfrak{P}}$ corresponding to a single $p$ are conjugate, and we call this *conjugacy class* the **Artin symbol corresponding to** $p$. In the good case that $G$ is abelian, we can identify a conjugacy class with its unique member, so that the Artin symbol for $p$ is an element $\sigma_p$ in $G$.

EXERCISE. If you are familiar with number theory in quadratic fields, try to work out the Artin symbols for them. Start with the field $\boldsymbol{Q}(\sqrt{q})$ where $q$ is an odd prime, and identify the Galois group with $\{\pm 1\}$. Check that after this identification, the Artin symbol $\sigma_p$ is exactly the Legendre symbol $(q/p)$. (Were you wondering why $\sigma_p$ is called a "symbol"?) What about more complicated quadratic fields? Finally, try to compute the Artin symbols $\sigma_p$ for the cyclotomic field $\boldsymbol{Q}(\zeta_m)$. (Goldstein [7, p. 96 ff.] is one of many possible references.)

From here on, $\boldsymbol{K}/\boldsymbol{Q}$ is an abelian extension with group $G$. We denote by $\boldsymbol{Q}^*$ the multiplicative group of non-zero rational numbers, and we think of $\boldsymbol{Q}^*$ as the (multiplicative) free abelian group generated by the primes. For a fixed field $\boldsymbol{K}$, let $\Gamma \subseteq \boldsymbol{Q}^*$ be the free abelian subgroup generated by the unramified primes in $\boldsymbol{K}/\boldsymbol{Q}$. We extend the definition of the Artin symbol by setting $\sigma_{pq} = \sigma_p \cdot \sigma_q$, and $\sigma_a = \sigma_p^{-1}$ if $a = 1/p$. This procedure gives a *group homomorphism*, $\sigma: \Gamma \to G$, called the **Artin map.**

Can we find the kernel and image of this homomorphism? The image is easy to describe: *the Artin map $\sigma$ is surjective.* We shall get some idea of the proof in the next section.

What about the kernel? The result here is more complicated and requires some more terminology. If $a$ is an integer, the **ray group** $\Gamma_a$ is defined as follows: a rational number $r \neq 0$ is in $\Gamma_a$ if $r$ can be written as $c/d$ with $c$ and $d$ prime to $a$ and $c \equiv d \pmod{a}$. Then *the kernel of the Artin map for $\boldsymbol{K}/\boldsymbol{Q}$ contains the ray group $\Gamma_a$ for some $a = p_1^{e_1} \cdots p_s^{e_s}$, where $p_1, \cdots, p_s$ are the ramified primes in $K$, and $e_i \geqq 1$.*

The two italicized statements above make up the **Artin Reciprocity Law.** Emil Artin conjectured it in 1923 [**1**, p. 98], and proved it in 1927 [**1**, p. 131]. (Artin worked over arbitrary number fields, not just over $\boldsymbol{Q}$.) The theorem is central in all modern treatments of class field theory. It is proved in all the books recommended above, and in many others as well. We state it again for reference.

ARTIN RECIPROCITY LAW: *Let $\boldsymbol{K}/\boldsymbol{Q}$ be a finite abelian extension with Galois group $G$, and let $\Gamma$ be the subgroup of $\boldsymbol{Q}^*$ generated by the primes unramified in $\boldsymbol{K}$. Then the Artin symbol gives a surjective group homomorphism $\sigma: \Gamma \to G$ whose kernel contains the ray group $\Gamma_a$, where $a$ is an appropriate product of the ramified primes.*

The Artin Reciprocity Law is a precise form of half the Abelian Polynomial Theorem: if $f(X)$ is an abelian polynomial, then $\mathrm{Spl}(f)$ can be described by congruence conditions. To see why, we start with a crucial lemma.

LEMMA. *Suppose $f(X)$ is an abelian polynomial with root field $K$, Galois group $G$, and Artin map $\sigma: \Gamma \to G$. Then except perhaps for a finite number of exceptional primes, $f(X)$ splits modulo $p$ if and only if $\sigma_p$ is trivial.*

*Proof.* We can only give an outline here. If $p$ is unramified and $p\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_s$, then the Chinese Remainder Theorem gives

$$\mathcal{O}_K/p\mathcal{O}_K \cong \oplus_{i=1}^{s} \mathcal{O}_K/\mathfrak{P}_i.$$

On the other hand, except for a finite number of $p$,

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbf{F}_p[X]/(f_p(X)),$$

where $f_p(X)$ is the reduction of $f(X)$ modulo $p$. (This is a hard exercise; the exceptions all divide the discriminant of $f(X)$.) Therefore, except for finitely many $p$,

$$\mathbf{F}_p[X]/(f_p(X)) \cong \oplus_{i=1}^{s} \mathcal{O}_K/\mathfrak{P}_i.$$

When is the Artin symbol $\sigma_p$ trivial? By definition $\sigma_p$ induces the Frobenius map, $x \to x^p$, on each direct summand. The Frobenius map is trivial on $\mathcal{O}_K/\mathfrak{P}$ only if $\mathcal{O}_K/\mathfrak{P} \cong \mathbf{F}_p$, so that $\mathbf{F}_p[X]/(f_p(X)) \cong \mathbf{F}_p^n$ when $\sigma_p$ is trivial, and this is only possible when $f_p(X)$ factors into linear factors. All the steps are reversible, so the converse holds too.

This lemma, combined with the Artin Reciprocity Law, guarantees that the set $\mathrm{Spl}(f)$ contains all primes $p$ such that $p \equiv 1 \pmod{a}$, with at most finitely many exceptions. (Check this!)

We need to change $\mathrm{Spl}(f)$ slightly at this point. Add to $\mathrm{Spl}(f)$ any primes $p \equiv 1 \pmod{a}$ not already there, and throw away any divisors of $a$. Call the resulting set $S$; this is the set we can describe by explicit congruence conditions.

Let $\boldsymbol{Q}^*(a)$ be the multiplicative subgroup generated by all primes $p$ which do not divide $a$. (A fraction $b/c$ in lowest terms is in $\boldsymbol{Q}^*(a)$ if both $b$ and $c$ are prime to $a$.) Let $S'$ be the subgroup of $\boldsymbol{Q}^*$ generated by $S$. The set $S$ has been chosen so that $\Gamma_a \subseteq S' \subseteq \boldsymbol{Q}^*$, and the importance of these inclusions comes out in the next lemma.

LEMMA. $\boldsymbol{Q}^*(a)/\Gamma_a \cong (\mathbf{Z}/a\mathbf{Z})^*$, *where $(\mathbf{Z}/a\mathbf{Z})^*$ is the group of invertible elements in $\mathbf{Z}/a\mathbf{Z}$.*

*Proof.* Define $\theta: \boldsymbol{Q}^*(a)/\Gamma_a \to (\mathbf{Z}/a\mathbf{Z})^*$ by $\theta(b/c) = bc^{-1} \pmod{a}$. Check as an exercise that $\theta$ is a surjective homomorphism with kernel exactly $\Gamma_a$.

This lemma supplies us with congruence conditions. Starting with $\mathrm{Spl}(f)$, pass to $S$, and consider the set $\theta(S')$ of residue classes modulo $a$. A given prime $p$ will lie in $S$ if and only if its residue class modulo $a$ lies in $\theta(S')$. Since $S$ and $\mathrm{Spl}(f)$ differ in at most $a$ finite number of primes, we shall be content with this result.

Next we attack the other half of the Abelian Polynomial Theorem: If $\mathrm{Spl}(f)$ can be defined by congruences, then $f(X)$ must be an abelian polynomial. We shall need a hard theorem which says (roughly) that the root field $\boldsymbol{K}_f$ of $f(X)$ is uniquely determined by the set $\mathrm{Spl}(f)$. We introduce some notation: If $S$ and $T$ are two sets of primes, then $S \subseteq^* T$ means that except for at most a finite number of exceptions every member of $S$ is a member of $T$. The precise statement is then:

INCLUSION THEOREM. *Suppose $f(X)$ and $g(X)$ are polynomials with root fields $\boldsymbol{K}_f$ and $\boldsymbol{K}_g$, respectively. Then $\boldsymbol{K}_f \subseteq \boldsymbol{K}_g$ if and only if $\mathrm{Spl}(g) \subseteq^* \mathrm{Spl}(f)$.*

Note the reversal! The similarity to Galois theory can be made very precise for abelian polynomials and is an important part of class field theory. The theorem itself holds for arbitrary $f(X)$ and $g(X)$.

It is not hard to prove that $\boldsymbol{K}_f \subseteq \boldsymbol{K}_g$ implies $\mathrm{Spl}(g) \subseteq^* \mathrm{Spl}(f)$. The converse requires analytic techniques, and is a corollary of the Tchebotarev Density Theorem discussed in the next section. See Cassels and Fröhlich [**3**, Exercise 6.1, p. 362] or Goldstein [**7**, Theorem 9–1–13, p. 164] for a proof.

Assume now that $\mathrm{Spl}(f)$ can be defined by congruences modulo an integer $a$. Actually we assume more: namely, that $\mathrm{Spl}(f)$ contains the ray group $\Gamma_a$. (Exercise: What's the difference between these assumptions?) According to Section 3, $\Gamma_a$ is $\mathrm{Spl}(\Phi_a(X))$, and the root field of $\Phi_a(X)$ is the cyclotomic field $\boldsymbol{Q}(\zeta_a)$, which is abelian over $\boldsymbol{Q}$. Since $\Gamma_a \subseteq \mathrm{Spl}(f)$, the Inclusion Theorem gives $\boldsymbol{K}_f \subseteq \boldsymbol{Q}(\zeta_a)$, so that $\boldsymbol{K}_f$ must also be abelian over $\boldsymbol{Q}$.

One corollary of this discussion deserves special mention.

KRONECKER'S THEOREM. *Every abelian extension of $\boldsymbol{Q}$ is contained in a cyclotomic extension.*

*Proof. Exercise*: Combine the Artin Reciprocity Law with the argument above. (There is an elementary proof in Gaal [**5**, p. 242].)

**5. General polynomials. The Tchebotarev Density Theorem.** If $f(X)$ is an irreducible polynomial in $\boldsymbol{Z}[X]$ which is not abelian, then very little can be said about the set $\mathrm{Spl}(f)$. The best general result is a statement about the relative "size" of $\mathrm{Spl}(f)$. First we describe a numerical measure of sets of primes called the **density**.

Let $\Pi$ be the set of all prime numbers, and let $T \subseteq \Pi$ be any subset. For any real $x \geqq 1$, let

$$\delta(T,x) = \frac{\mathrm{card}\{p \in T \mid p < x\}}{\mathrm{card}\{p \in \Pi \mid p < x\}}.$$

DEFINITION. *If $T$ is a set of primes such that $\lim_{x\to\infty} \delta(x,T) = \delta(T)$, then $T$ has density $\delta(T)$.*

Note that the limit may not exist. In that case we say, naturally enough, that $T$ "does not have a density." If $T$ does have a density, then $0 \leqq \delta(T) \leqq 1$. Since $\Pi$ is infinite, any finite set of primes has density 0, and it is easy to see that if $S$ and $T$ differ by a finite set of primes, then $\delta(S) = \delta(T)$. Clearly $\delta(\Pi) = 1$.

One can prove that a set of primes is infinite by showing that it has a non-zero density. The first theorem of this type was proved by Lejeune Dirichlet in 1837.

DIRICHLET'S THEOREM. *Suppose $m$ is a positive integer and $a$ is an integer relatively prime to $m$. Then the set of all primes congruent to $a$ modulo $m$ has a density equal to $1/\phi(m)$.*

In particular, the set of all primes congruent to $a$ modulo $m$ is infinite. Although this much can be proved directly for some $a$ and $m$ (see Hardy and Wright [**8**, p. 13]), no general proof avoids analysis and the notion of density. Proofs of the theorem can be found all over; one is in Davenport [**4**, pp. 1 and 28].

The density result we need for the reciprocity problem is the *Tchebotarev Density Theorem*. We give a weakened version first.

WEAK TCHEBOTAREV THEOREM. *Let $f(X)$ be an irreducible polynomial in $\boldsymbol{Z}[X]$ with root field $\boldsymbol{K}_f$, and suppose that $[\boldsymbol{K}_f : \boldsymbol{Q}] = n$. Then* $\mathrm{Spl}(f)$ *has a density equal to $1/n$.*

This theorem implies part of Dirichlet's Theorem. Take $f(X)$ to be the cyclotomic polynomial $\Phi_m(X)$ so that $[\boldsymbol{K}_f : \boldsymbol{Q}] = \phi(m)$, so that the theorem gives $\delta[\mathrm{Spl}(\Phi_m)] = 1/\phi(m)$. By Section 3, a prime $p$ is in $\mathrm{Spl}(\Phi_m)$ if and only if $p \equiv 1 \pmod{m}$ and putting all this together gives Dirichlet's result for $a = 1$. The rest of Dirichlet's Theorem follows from the full Tchebotarev Theorem discussed below.

The interested reader should go back to Section 2 and examine quadratic polynomials from the point of view of density results. The following main result can be derived from either of the two theorems above: *Suppose $a$ is not a perfect square. Then the set of primes $p$ such that $(a/p) = +1$ has density $\frac{1}{2}$.* (What about those $p$ with $(a/p) = -1$? What about primes dividing $a$?)

To explain the strong form of Tchebotarev's theorem, we need to use Artin symbols again. To read the rest of this section you need either the last part of Section 4 or faith. It is safe to skip to Section 6.

Let $f(X)$ in $\boldsymbol{Z}[X]$ have root field $\boldsymbol{K}_f$ and Galois group $G$. The group $G$ is not necessarily abelian, and the Artin symbol corresponding to $p$ is a conjugacy class $C_p$ of elements of $G$. (There are a finite number of ramified $p$ for which $C_p$ cannot be defined. We ignore these.)

Tchebotarev proved his theorem in 1925 and his methods inspired Artin's proof of the Reciprocity Law.

TCHEBOTAREV DENSITY THEOREM. *Let $f(X) \in Z[X]$ be irreducible with Galois group $G$, and let $C$ be a fixed conjugacy class of elements of $G$. Let $S$ be the set of*

*primes p whose Artin symbol $C_p$ equals C. Then S has a density, and*

$$\delta(S) = \frac{\text{card}(C)}{\text{card}(G)}.$$

In particular, if $C = \{1\}$, then $S = \text{Spl}(f)$ (by a lemma in Section 4) and $\delta(S) = 1/\text{card}(G)$. We recover the weak theorem. If the group $G$ is abelian, then each conjugacy class has one member and the corresponding sets of primes each have density $1/\text{card}(G)$. This shows immediately that *the Artin map is surjective.* (Why?) Also explicit calculation of Artin symbols in cyclotomic fields gives a proof of Dirichlet's Theorem from Tchebotarev's Theorem.

**6. An algorithm for the reciprocity problem.** What have we learned so far about the reciprocity problem? Not much, in general, but we can claim to understand abelian polynomials completely. This knowledge at least gives a starting place for the study of polynomials with *solvable* Galois group. We do not discuss this here, but see Hasse [**9**, pp. 64–69] and Cassels and Fröhlich [**3**, Ex. 2.15, p. 354]. For polynomials with non-solvable groups, the only progress is the tantalizing example of Shimura mentioned in the introduction.

No satisfactory description of general sets $\text{Spl}(f)$ has been given up to now, but for fixed $f(X)$ and a particular prime $p$, we can at least ask whether $p$ lies in $\text{Spl}(f)$. This involves factoring $f(X)$ modulo $p$, which is a finite process. The point of this section is to do the factoring *efficiently*. The method we use is essentially due to Berlekamp [**12**, Chapter 6]. Our formulation, designed to give only that information relevant to the reciprocity problem, is slightly different from Berlekamp's.

The prerequisites for the discussion are the Chinese Remainder Theorem for polynomial rings, and some knowledge of finite fields. (The material needed is covered in Berlekamp [**2**] and Lang [**14**], especially pages 63 and 182.)

Suppose given a polynomial $f(X)$ in $\mathbf{Z}[X]$ of degree $n$, with no repeated factors, and let $f_p(X)$ be its reduction modulo $p$. Assume $f_p(X) = g_1(X) \cdots g_r(X)$ where $g_i(X)$ is irreducible of degree $d_i$. Our problem is to compute $d_1, \cdots, d_r$; we know $d_1 + \cdots + d_r = n$. For example, $p \in \text{Spl}(f)$ if $r = n$ and each $d_i = 1$.

First we compute the discriminant $D(f)$ by the classical formula (e.g., Lang [**14**, p. 139]). If $p$ divides $D(f)$, then $f_p(X)$ has a repeated factor. We declare such $p$ "bad" and do not consider them further. If $p$ does not divide $D(f)$, then the $g_i(X)$ are distinct irreducible polynomials and are therefore relatively prime. The Chinese Remainder Theorem gives:

$$(*) \qquad \mathbf{F}_p[X]/(f_p(X)) \cong \oplus_{i=1}^{r} \mathbf{F}_p[X]/(g_i(X)).$$

We write $\Lambda = \mathbf{F}_p[X]/(f_p(X))$ and $k_i = \mathbf{F}_p[X]/(g_i(X))$. Since $g_i(X)$ is irreducible of degree $d$, then $k_i = \mathbf{F}_q$, the unique finite field with $q = p^{d_i}$ elements. Since $[k_i : \mathbf{F}_p] = d_i$, we can recover all we need by computing the dimensions of the summands on the righthand side.

Here we have a case in which two isomorphic structures cannot be identified: the ring $\Lambda$ is given very concretely as an $n$-dimensional $\mathbf{F}_p$ space, with basis $1, x^2, \cdots, x^{n-1}$, where $x$ is the residue class of $X$ modulo $f(X)$. Addition is vector space addition, and multiplication is carried out modulo $f(X)$. Our problem is to extract the direct sum decomposition, or at least compute the $d_i$, from *this* description of $\Lambda$.

As preparation, consider a finite extension $k$ of $\mathbf{F}_p$, with $[k:\mathbf{F}_p] = d$, say. The mapping $\phi(z) = z^p: k \to k$ is a field isomorphism called the Frobenius map, and $\phi(z) = z$ if and only if $z \in \mathbf{F}_p$. Moreover, $\phi^i(z) = z$ for $1 \leqq i \leqq d$ if and only if $z \in \mathbf{F}_q \subseteq k$, where $q = p^i$. Thus, $d$ can be computed as the smallest integer such that $\phi^d =$ identity on $k$.

The Frobenius map $z \to z^p$ on $\Lambda$, which we also denote by $\phi$, is a ring isomorphism useful in studying the structure of $\Lambda$. For example, if $\Lambda \cong \mathbf{F}_p \oplus \cdots \oplus \mathbf{F}_p$ ($n$ summands), then $\phi =$ identity. More generally, the smallest $d$ such that $\phi^d =$ identity on $\Lambda$ (the order of $\phi$) equals the least common multiple of the $d_i$. Since $x$ generates $\Lambda$ as a ring, the order is the smallest $d$ such that $\phi^d(x) = x$, so it is easy to compute. We shall see in the next section that the order can give a lot of information in special cases. In general, however, we need a refinement.

Suppose $\gamma$ denotes the isomorphism in the Chinese Remainder Theorem:

$$\gamma: \Lambda \cong k_1 \oplus \cdots \oplus k_r.$$

Then it is easy to see that

$$\gamma(\ker(\phi - I)) = \mathbf{F}_p \oplus \cdots \oplus \mathbf{F}_p, \ r \text{ summands},$$

where $I: \Lambda \to \Lambda$ is the identity map, and $\ker(\phi - I)$ is the kernel of the linear transformation $(\phi - I): \Lambda \to \Lambda$.

Similarly,

$$\gamma(\ker(\phi^2 - I)) = l_1 \oplus \cdots \oplus l_r,$$

where $l_i = \mathbf{F}_{p^2}$ if $\mathbf{F}_{p^2} \subseteq k_i$, and $l_i = \mathbf{F}_p = k_i$, otherwise.

Therefore, $\ker(\phi^2 - I)$ has $\mathbf{F}_p$-dimension equal to $2r -$(the number of summands with $d_i = 1$).

DEFINITION. *For each integer $i$, let $\nu_i =$ nullity $(\phi^i - I) = \dim(\ker(\phi^i - I))$, where "dim" denotes vector space dimension over the prime field $\mathbf{F}_p$.*

*For each integer $j$, let $\mu_j =$ the number of factors in the decomposition (*) which have dimension exactly equal to $j$.*

In this notation $\nu_1 = r$, the total number of factors, and $\nu_2 = 2r - \mu_1$. The reader should verify that

$$\begin{aligned} \nu_3 &= \mu_1 + 2\mu_2 + 3(r - \mu_1 - \mu_2) \\ &= 3r - 2\mu_1 - \mu_2. \end{aligned}$$

Generally, it is not hard to see that

$$(\#) \qquad \nu_k = kr - (k-1)\mu_1 - (k-2)\mu_2 - \cdots - \mu_{k-1}.$$

This relationship is very important. Knowing the $\mu_i$ is the same as knowing $d_1, d_2, \cdots, d_r$, so they give the factorization of $f_p(X)$. On the other hand, we shall see below that the $\nu_i$ are relatively easy to compute. The reader should use equation $(\#)$ to verify the following inversion formula:

$$(\#\#) \qquad \mu_k = 2\nu_k - \nu_{k-1} - \nu_{k+1}.$$

We summarize these facts in the theorem.

THEOREM. *Suppose, given* $\Lambda = \mathbf{F}_p[X]/(f_p(X)) = \boldsymbol{k}_1 \oplus \cdots \oplus \boldsymbol{k}_r$, *and let* $d_i = [\boldsymbol{k}_i : \mathbf{F}_p]$. *Let* $\phi$ *be the Frobenius automorphism of* $\Lambda$, *and let* $\nu_i =$ *nullity* $(\phi^i - I)$. *Then* $r = \nu_1$, *and there are exactly* $\mu_j = 2\nu_j - \nu_{j-1} - \nu_{j+1}$ *summands with* $d_i = j$, $j = 1, \cdots, d$. *Here* $d$ *is the smallest integer such that* $\phi^d = I$.

This theorem forms the basis of an efficient algorithm. First compute the matrix $[\phi]$ with respect to the basis $\{1, x, \cdots, x^{n-1}\}$ of $\Lambda$. (Berlekamp calls this the **Q-matrix**.) Then compute successively $\nu_i =$ nullity $([\phi]^i - I)$. Finally, compute the $\mu_i$ from the theorem. If $\mu_1 = n$, then $p$ belongs to $\mathrm{Spl}(f)$, and in more complicated situations the $\mu_i$ give information about the Artin symbol belonging to $p$.

Of course, we must examine this proposed algorithm. How hard is it? How long does it take? Can it produce significant results and lead to a better theoretical understanding of the problem?

First of all I have to admit that it is completely unreasonable to do the algorithm by hand. I worked on $f(X) = X^5 - X - 1$ with $p = 11$ for an hour and could not make it come out. It is much easier to factor by trial and error when $p$ is small, but large primes are impossible.

Fortunately it is not too difficult to write a FORTRAN program which will do calculations in the ring $\Lambda$. Since $\Lambda$ is an $n$-dimensional vector space over $\mathbf{F}_p$ with a nice basis $\{1, x, x^2, \cdots, x^{n-1}\}$, its elements can be represented as a $1 \times n$ FORTRAN array. The program written for the next section uses FORTRAN's integer arithmetic and works modulo a variable prime $p$.

The algorithm is very efficient in that *the number of operations required to factor* $f(X)$ *modulo* $p$ *is proportional to* $\log p$. In fact, the only part of the algorithm that depends essentially on $p$ is computing $x^p$ in the ring $\Lambda$. Abstractly speaking, how many steps does it take to compute $x^p$? Certainly less than $2 \cdot \log_2 p$, since $x^p$ can be computed by successively squaring together some multiplications by $x$. (Are you skeptical? If $p = 23 = 10111$ (binary), the steps are $x$, $x^2$, $x^4$, $x^5$, $x^{10}$, $x^{11}$, $x^{22}$, $x^{23}$, which requires $7 < 2 \cdot \log_2(23)$ steps.) The fascinating subject of number theory algorithms and the time needed to do them is discussed in Lehmer [**16**]. Knuth [**13**, p. 388 ff.] goes into more detail and discusses algorithms very similar to this one.

**7. Numerical results.** With the help of R. W. Latzer I have written a FORTRAN program to carry out the algorithm for the polynomials $X^5 - X - a$, where $a$ is an integer. This is the "Bring-Jerrard Quintic" which has the non-solvable Galois group $\mathfrak{S}(5)$ for general $a$, and in particular for $a = 1$, and $a = 2$. The program factored $X^5 - X - 1$ for all $p$ up to 23,099 in about two minutes, at which time the program overflowed the FORTRAN integer capacity. (I have learned that Professor J. D. Brillhart, using other methods, has factored many members of a more general family of quintics up to $p = 1000$.)

If $f(X)$ is any irreducible quintic polynomial, then $f_p(X)$ can factor in one of eight ways:

| | | |
|---|---|---|
| *Type* 0: | $p \mid D(f)$ | |
| *Type* 1: | Five linear factors | 1/120 |
| *Type* 23: | (Quadratic) (Quadratic) (Linear) | 15/120 |
| *Type* 24: | (Quadratic) (Three Linear) | 10/120 |
| *Type* 3: | (Cubic) (Linear) (Linear) | 20/120 |
| *Type* 4: | (Quartic) (Linear) | 30/120 |
| *Type* 5: | (Quintic) | 24/120 |
| *Type* 6: | (Quadratic) (Cubic) | 20/120 |

The factors are irreducible and distinct, when displayed. The type is the order $d$ of the Frobenius map when $p$ does not divide $D(f)$ except that Type 23 means (order = 2, nullity $\nu_1 = 3$) and Type 24 means (order = 2, nullity $\nu_1 = 4$). Thus, no nullities have to be computed, except when the order = 2. The fractions give the density of primes of each type, according to the Tchebotarev Density Theorem.

Finally, we give some examples of actual numerical results.

1. $f(X) = X^5 - X - 1$.

(a) $D(f) = 19 \cdot 151$, so 19 and 151 are bad.

(b) The primes of Type 1 (those in Spl($f$)) which are less than 23099 are 1973, 3769, 5101, 7727, 8161, 9631, 11093, 14629, 16903, 17737, 17921, 18097, 19477, 20759, 21727, and 22717. There are 16 primes in this list, giving a ratio of 16/2350 $\approx .0068$, as compared with a density of $1/120 \approx .00833$.

(c) The primes less than 500 are classified as follows:

*Type* 0. 19, 151.
*Type* 1. None.
*Type* 23. 67, 71, 239, 251, 313, 421, 433, and 491.
*Type* 24. 163, 193, 227, 307, 467, 487, and 499.
*Type* 3. 17, 41, 43, 47, 53, 107, 113, 179, 181, 191, 229, 281, 293, 311, 317, 347, 349, 373, 409, 457, and 463.

*Type* 4. 23, 29, 31, 61, 97, 101, 127, 131, 157, 173, 223, 241, 263, 269, 331, 359, 389, 439, 443, and 479.

*Type* 5. 3, 5, 11, 13, 79, 89, 109, 137, 139, 211, 257, 337, 379, 397, 431, 449, and 461.

*Type* 6. 2, 7, 37, 59, 73, 83, 103, 149, 167, 197, 199, 233, 271, 277, 283, 353, 367, 383, 401, and 419.

2. $f(X) = X^5 - X - 2$.

(a) $D(f) = 2^4 \cdot 3109$, so 2 and 3109 are bad.

(b) The primes of type 1 less than 23099 are 229, 271, 1637, 2647, 2857, 3673, 6323, 7103, 8123, 8999, 11161, 12197, 14341, 14503, 14929, 17183, 18679, 19457 and 20563. There are 19 primes in this list, giving $19/2350 \approx .00809$.

3. It is also possible to fix $p$ and let the coefficient $a$ in $X^5 - X - a$ vary modulo $p$. So far I have done this for all $p$ up to 239. For example, if $p = 31$, we get:

*Type* 0. $a \equiv 11, 20 \pmod{31}$.

*Type* 1. None.

*Type* 23. $a \equiv 2, 3, 28, 29 \pmod{31}$.

*Type* 24. $a \equiv 0, 15, 16 \pmod{31}$.

*Type* 3. $a \equiv 7, 24 \pmod{31}$.

*Type* 4. $a \equiv 1, 5, 8, 9, 14, 17, 22, 23, 26, 30 \pmod{31}$.

*Type* 5. $a \equiv 6, 10, 12, 13, 18, 19, 21, 25 \pmod{31}$.

*Type* 6. $a \equiv 4, 27 \pmod{31}$.

**8. What is a reciprocity law?** A general reciprocity law should provide a description of the set $\mathrm{Spl}(f)$ associated with a polynomial $f(X)$. The algorithm discussed in this paper is such a description, but few number theorists would consider it a reciprocity law. More is wanted, but the exact requirements are still vague and undefined.

A good general reciprocity law should specialize to the Artin Reciprocity Law in the case of abelian polynomials. A very good reciprocity law should include a one-to-one correspondence between certain sets of prime numbers and field extensions, giving more substance to the Inclusion Theorem in Section 5. Such a correspondence should generalize the known abelian theorems of class field theory. Y. Ihara [**11**] is beginning to make some progress toward this goal in the function field case.

Even if a good correspondence cannot be set up, any reciprocity law must be set in a general framework, and should unify various kinds of number theoretic phenomena. The examples in Shimura [**19**] are related to the theory of elliptic curves, but they are very special, and it is not clear how to use them as a foundation for a general reciprocity law. (The specialist should look at Ihara's discussion of this question.)

I would like to mention briefly another direction of research which may lead to reciprocity laws. The Artin Reciprocity Law can be interpreted as a theorem about certain classes of analytic functions: see Artin's original paper [**1**, p. 97] or the section "Abelian $L$-functions are Hecke $L$-functions" in Goldstein [**7**, p. 182]. There seem to be important non-abelian analogues to this viewpoint which involve group

representations and automorphic forms, and the interested reader should look at the introduction to Jacquet-Langlands' book [12] or Shalika's paper [18].

Finally, I have to confess that I still do not know what a reciprocity law is, or what one should be. The reciprocity problem, like so many other number theory problems, can be stated in a fairly simple and concrete way. However, the simply stated problems are often the hardest, and a complete solution seems to be far out of reach. In fact, we probably will not know what we are looking for until we have found it.

This research was supported in part by a grant from the National Science Foundation under grant GP 29696.

## References

1. E. Artin, Collected Papers, Addison-Wesley, Reading, Mass., 1965.
2. E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.
3. J. W. S. Cassels and A. Fröhlich, Algebraic Number Theory, Thompson, Washington, 1967.
4. H. Davenport, Multiplicative Number Theory, Markham, Chicago, 1971.
5. L. Gaal, Classical Galois Theory with Examples, Markham, Chicago, 1971.
6. C. F. Gauss, Disquisitiones Arithmeticae, transl. A. A. Clarke, Yale, New Haven, 1966.
7. L. Goldstein, Analytic Number Theory, Prentice-Hall, Englewood Cliffs, N. J., 1971.
8. G. Hardy and E. Wright, An Introduction to the Theory of Numbers, 4th ed. Oxford, 1960.
9. H. Hasse, Bericht über neuere Untersuchungen und Problemen aus der Theorie der algebraischen Zahlkörper, Teil I, Ia, II, 2nd edit., Physica-Verlag, Würzburg, 1965.
10. A. M. Legendre, Recherches d'Analyse Indéterminée, Hist. Acad., Paris, 1785.
11. Y. Ihara, Non-abelian class fields over function fields in special cases, to appear in Proc. of the Intern. Congress of Math., Nice, 1970.
12. H. Jacquet and R. P. Langlands, Automorphic Forms on Gl(2), Springer-Verlag Lecture Notes in Mathematics, No. 114, Berlin, 1970.
13. D. Knuth, The Art of Computer Programming, Volume 2: Seminumerical Algorithms, Addison-Wesley, Reading, Mass., 1969.
14. S. Lang, Algebra, Addison-Wesley, Reading, Mass., 1965.
15. ———, Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1971.
16. D. H. Lehmer, Computer Technology Applied to the Theory of Numbers, Studies in Number Theory, MAA, Prentice-Hall, Englewood Cliffs, N.J., 1969.
17. I. Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, 2nd ed., Wiley, New York, 1966.
18. J. Shalika, Some Conjectures in Class Field Theory, in AMS, Proc. of Symposia in Pure Math., Volume XX: Stony Brook Number Theory Institute, Providence, 1971.
19. G. Shimura, A non-solvable reciprocity law, J. Reine Angew. Math., 221 (1966) 209–220.
20. B. van der Waerden, Modern Algebra, Vol. I, Revised English Edition, Ungar, New York, 1953.
21. A. Weil, Basic Number Theory, Springer, New York, 1967.