A Mechanical Proof of Quadratic Reciprocity

David M. Russinoff

Microelectronics and Computer Technology Corporation
3500 West Balcones Center Drive, Austin, TX 78759

Abstract. We describe the use of the Boyer-Moore theorem prover in mechanically generating a proof of the Law of Quadratic Reciprocity: *for distinct odd primes p and q, the congruences $x^2 \equiv q$ (mod p) and $x^2 \equiv p$ (mod q) are either both solvable or both unsolvable, unless $p \equiv q \equiv 3$ (mod 4).* The proof is a formalization of an argument due to Eisenstein, based on a lemma of Gauss. The input to the theorem prover consists of nine function definitions, thirty conjectures, and various hints for proving them. The proofs are derived from a library of lemmas that includes Fermat's Theorem and the Gauss Lemma.

Keywords. Automatic theorem proving, Boyer-Moore prover, number theory, quadratic reciprocity.

1 Introduction

Questions of solvability of integer equations often lead to the study of congruences, which is therefore central to the theory of numbers. If a, b, and m are integers, then a and b are said to be *congruent modulo m*, and we write $a \equiv b \pmod{m}$, if the difference $a - b$ is a multiple of m. Problems concerning congruences are often reducible to the case in which the modulus m is prime. In particular, the formula $x^2 \equiv a \pmod{p}$, where p is a prime not dividing a, is of fundamental importance. If there exists a solution x to this congruence, then a is said to be a *quadratic residue modulo p*. This relation is represented by the *Legendre symbol* $(\frac{a}{p})$, defined by

$$(\frac{a}{p}) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue modulo } p \\ -1 \text{ if not} \end{cases}$$

where a is assumed not to be divisible by p.

As a refinement of Fermat's Theorem, which states that $a^{p-1} \equiv 1 \pmod{p}$, *Euler's Criterion* for quadratic residues gives a means of directly computing the value of the Legendre symbol:

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

For large primes p, however, this formula is impractical. Moreover, it is of little use in solving more general problems, such as the characterization of the set of primes p such that $(\frac{a}{p}) = 1$ for a given a.

A deeper result, known as the *Law of Quadratic Reciprocity*, gives a relationship between $(\frac{p}{q})$ and $(\frac{q}{p})$ for distinct odd primes p and q:

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

In other words, $(\frac{p}{q}) = (\frac{q}{p})$ iff either p or q is congruent to 1 modulo 4. Thus, we may show that 19 is not a quadratic residue modulo the prime 283 by observing that

$$(\frac{19}{283}) = -(\frac{283}{19}) = -(\frac{17}{19}) = -(\frac{19}{17}) = -(\frac{2}{17}) = -(\frac{6^2}{17}) = -1.$$

The significance of the reciprocity law extends well beyond the explicit evaluation of the Legendre symbol. As another illustration of its use, the following argument establishes the existence of infinitely many primes of the form $10k - 1$: Given any integer $n > 1$, let $N = 5(n!)^2 - 1$. Since $N \not\equiv 1 \pmod{5}$, N must have some prime divisor $p \not\equiv 1 \pmod{5}$. Since p exceeds n, which was arbitrarily chosen, we need only show that $p \equiv -1 \pmod{10}$. First note that from Fermat's Theorem and the congruence $5(n!)^2 \equiv 1 \pmod{p}$, it follows that $5 \equiv 5(n!)^{2(p-1)} \equiv 5(n!)^2(n!)^{2(p-2)} \equiv (n!)^{2(p-2)} \pmod{p}$, and hence $(\frac{5}{p}) = 1$. Since $5 \equiv 1 \pmod{4}$, we also have $(\frac{p}{5}) = 1$ by quadratic reciprocity. Thus, $p \equiv \pm 1 \pmod{5}$, as these are the only quadratic residues modulo 5. But $p \equiv 1 \pmod{5}$ is precluded by assumption, hence $p \equiv -1 \pmod{5}$. Finally, since p is odd, $p \equiv -1 \pmod{10}$.

The first proof of quadratic reciprocity was given by Gauss in 1796 in his *Disquisitiones Arithmeticae* [Gau66], which included the first systematic treatment of congruences. Gauss considered this result, which he called the *Theorema Aureum* (golden theorem), to be one of his most important achievements. Regarding its proof, he later wrote: “It tortured me for a whole year and eluded the most strenuous efforts ....” [Dun55] Although he eventually produced eight different proofs, he apparently found none of them to be completely satisfactory.

Gauss’ efforts to explicate the principles underlying quadratic reciprocity and its generalizations initiated a variety of research areas, including the theories of complex and algebraic numbers. Mathematicians have continued to be fascinated by this formula for two centuries, during which time at least one hundred distinct proofs of the reciprocity law have been published. These efforts have produced unforeseen benefits even in the present century, most significantly in the area of class field theory [ArT68].

In this paper, we describe a proof of the quadratic reciprocity law that differs from all previously published proofs inasmuch as it was constructed within a formal logic by a mechanical theorem prover. This logic and theorem prover compose the verification system of Boyer and Moore [BoM79,BoM88]. The logic includes a formalization of constructive arithmetic in which a number of elementary number-theoretic results have been formulated and verified by the theorem prover. In Section 2, we discuss the Boyer-Moore system and describe the process by which proofs are mechanically generated.

Our proof of quadratic reciprocity is a formalization of an elementary proof attributed to Eisenstein [Nag64], which is based on a remarkable transformation of Euler’s Criterion known as the *Gauss Lemma*. The mechanical derivation of this lemma and other results on which it depends is described elsewhere [BoM79,BoM84,Rus85,Rus90]. The proof of the Gauss Lemma is outlined here in Section 3.

The appeal of Eisensteins’s proof, which is perhaps the most illuminating of the elementary proofs of quadratic reciprocity, lies in a geometric interpretation of an arithmetic relation. The most interesting aspect of our mechanical version of this proof is the formalization of this geometric argument. In Sections 4 and 5, we describe the construction of the formal proof in detail, including a complete account of our input to the theorem prover.

2 The Boyer-Moore System

The Boyer-Moore system is founded on a quantifier-free first-order logic with equality and a syntax resembling that of LISP. Thus, terms are constructed from parentheses and symbols denoting variables and functions. By convention, we shall use lower-case alphabetic characters, which do not appear in symbols of the logic, to denote metavariables representing terms.

The basic theory includes axioms characterizing four primitive functions:

- `TRUE` and `FALSE` are functions of zero arguments. By convention, the constants `(TRUE)` and `(FALSE)`, abbreviated as `T` and `F`, respectively, are the values returned by predicate functions.

- `EQUAL` is a binary function. The value of `(EQUAL l r)` is either `T` or `F`, according to whether $\mathtt{l} = \mathtt{r}$.

- `IF` is a ternary function. The value of `(IF t l r)` is `r` if $\mathtt{t} = \mathtt{F}$, and `l` otherwise.

In terms of these primitives, functions are defined corresponding to each of the logical connectives, e.g.,

$$\texttt{(IMPLIES P Q)} = \texttt{(IF P (IF Q T F) T)}.$$

This allows formulas to be encoded as terms, i.e., given any formula ϕ we may construct a term `t` such that

$$\phi \leftrightarrow (\mathtt{t} \neq \mathtt{F})$$

is a theorem. For example, the formula $\mathtt{X} \neq \mathtt{Y} \rightarrow \texttt{(F X Y)} = \texttt{(G X)}$ is encoded as the term

```
(IMPLIES (NOT (EQUAL X Y)) (EQUAL (F X Y) (G X))).
```

When a term `t` appears in a context where a formula is expected, it is understood to be an abbreviation for the formula $\mathtt{t} \neq \mathtt{F}$.

Variables occurring in axioms and theorems are understood to be universally quantified. Thus, if a term `t` is a theorem and s is substitution of terms for variables, then the result $\mathtt{t}/s$ of applying s to `t` may be inferred as a theorem by the rule of *instantiation.*

The logic also includes

- a principle that generates sets of axioms specifying new types of inductively constructed objects,

- a principle for admitting axioms that define new recursive functions, and
- a principle of induction by which theorems pertaining to these objects and functions may be inferred.

Our proof will employ two types of inductively constructed objects, which are included in the basic theory:

- The type *number* formalizes Peano arithmetic through axioms involving the recognizer `NUMBERP`, the constant `(ZERO)`, the successor function `ADD1`, and its inverse `SUB1`. Standard abbreviations are recognized: `(ZERO)` = `0`, `(ADD1 (ZERO))` = `1`, etc. Other arithmetic functions are defined in terms of the primitives, including `LEQ` (the standard partial order), `LESSP` (strict partial order), `ZEROP` (a predicate that fails iff its argument is a non-zero number), `PLUS`, `DIFFERENCE`, `TIMES`, `QUOTIENT`, `REMAINDER` (the basic binary integer operations), `EXP` (exponentiation), `FACT` (the factorial function), `EVEN`, `DIVIDES`, and `PRIME` (predicates related to divisibility).
- The type *cons* formalizes ordered pairs by means of the recognizer `LISTP`, the constructor `CONS`, and the accessors `CAR` and `CDR`. According to the LISP convention, lists are represented by means of these functions and the special symbol `NIL`. Functions corresponding to other familiar LISP functions, such as `LENGTH`, `MEMBER`, `INTERSECTION`, and `DELETE`, are defined in terms of these primitives.

When a term is presented as a conjecture to the theorem prover, various heuristics are applied in an attempt to derive the conjecture as a consequence of previously established theorems. A conjecture may or may not be labelled by the user as a *rewrite rule*, which determines whether, once proved, it becomes available to the prover for use in proving subsequent conjectures. If a rewrite rule of the form

```
(IMPLIES h (EQUAL l r))
```

is encountered during an attempt to rewrite some instance `l'` of the term `l` in a context in which the hypothesis `h` can be established, then `l'` is replaced by the corresponding instance `r'` of `r`. The precise syntactic form of a rewrite rule is therefore important in determining its use. Since rewrite rules are applied to a conjecture in the reverse of the order in which they were proved, some control over the behavior of the prover is possible through the ordering of lemmas. A failed proof attempt may often be salvaged by reordering or expanding a sequence of lemmas.

There is also a mechanism that allows the user to offer explicit advice pertaining to the proof of an individual lemma. This feature provides for three types of advice:

- *Use* a specified lemma (which might otherwise be overlooked and which may or may not have been designated as a rewrite rule), instantiated according to a given variable substitution;
- *Disable* the use of a specified lemma or function definition, in order to avoid leading the prover in an undesirable direction;
- *Induct* according to a scheme (which the prover might otherwise fail to select) suggested by the structure of a specified function definition.

In Section 3, we present several theorems that were established during the mechanical proof of the Gauss Lemma, omitting many intermediate lemmas that were also required. Sections 4 and 5, however, contain the complete ordered list of lemmas that were proved in the process of deriving the reciprocity law from the Gauss Lemma, including all advice that was offered to the prover. Note that the formulas labelled as conjectures are merely part of the commentary.

3 Quadratic Residues and the Gauss Lemma

Two numbers a and b are congruent modulo p iff they leave the same remainder upon division by p. Thus, we may represent congruences formally by means of the built-in function `REMAINDER`. For example, Fermat's Theorem [BoM84] is formulated as

Theorem 1 *(Fermat's Theorem)*

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL (REMAINDER M P) 0)))
         (EQUAL (REMAINDER (EXP M (SUB1 P)) P) 1))
```

Wilson's Theorem [Rus85], which states that for prime p, $(p-1)! \equiv -1 \pmod{p}$, is encoded as

Theorem 2 *(Wilson's Theorem)*

```
(IMPLIES (PRIME P)
         (EQUAL (REMAINDER (FACT (SUB1 P)) P) (SUB1 P)))
```

Since a number a that is indivisible by an odd prime p is a quadratic residue modulo p iff it is congruent to a square of some number between 0 and p, we define the predicate `RESIDUE` as follows:

Definition 1

```
(SQUARES N P)
      =
(IF (ZEROP N)
    (CONS 0 NIL)
  (CONS (REMAINDER (TIMES N N) P) (SQUARES (SUB1 N) P)))
```

Definition 2

```
(RESIDUE A P) = (MEMBER (REMAINDER A P) (SQUARES P P))
```

Our ultimate goal may be stated as

Conjecture 1 *(Law of Quadratic Reciprocity)*

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2))
              (PRIME Q) (NOT (EQUAL Q 2))
              (NOT (EQUAL P Q)))
         (EQUAL (EQUAL (RESIDUE Q P) (RESIDUE P Q))
                (EVEN (TIMES (QUOTIENT P 2) (QUOTIENT Q 2)))))
```

Euler's Criterion, as stated in Section 1, is an important ingredient in the proof of this result. It may be proved informally as follows: If $(\frac{a}{p}) = 1$, say $a \equiv n^2 \pmod{p}$, then

$$a^{(p-1)/2} \equiv (n^2)^{(p-1)/2} \equiv n^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Theorem. On the other hand, if $(\frac{a}{p}) = -1$, then it also follows from Fermat's Theorem that the set $\{1, 2, \ldots, p-1\}$ may be partitioned into pairs j, j' of distinct integers such that $jj' \equiv a \pmod{p}$. (Take $j' \equiv j^{p-2}a$

(mod p).) Since there are $(p-1)/2$ such pairs, it follows that $(p-1)! \equiv a^{(p-1)/2}$ (mod p). By Wilson's Theorem, we have $a^{(p-1)/2} \equiv -1 \pmod{p}$.

The most challenging aspect of the mechanization of this proof is the formalization of the process of partitioning a set into pairs, each of which contributes the same factor to the set's product. This problem was handled previously in our proof of Wilson's Theorem, and the solution is described in [Rus85]. The rest of the proof of Euler's Criterion is fairly straightforward, although over forty intermediate lemmas were required. We state the result as

Theorem 3 *(Euler's Criterion)*

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2)) (NOT (DIVIDES P A)))
         (EQUAL (REMAINDER (EXP A (QUOTIENT P 2)) P)
                (IF (RESIDUE A P) 1 (SUB1 P))))
```

The Gauss Lemma, which is derived from Euler's Criterion, states the following: For $k = 1, \ldots, \frac{p-1}{2}$, let r_k be the remainder of ka upon division by p, and let μ be the number of such k for which $r_k > \frac{p-1}{2}$. Then $(\frac{a}{p}) = (-1)^{\mu}$, i.e., a is a quadratic residue modulo p iff μ is even.

Our formulation of this lemma involves two definitions:

Definition 3

```
(MU N A P)
      =
(IF (ZEROP N)
    0
  (IF (LESSP (QUOTIENT P 2) (REMAINDER (TIMES A N) P))
      (ADD1 (MU (SUB1 N) A P))
    (MU (SUB1 N) A P)))
```

Definition 4

```
(GAUSS A P) = (EVEN (MU (QUOTIENT P 2) A P))
```

In these terms, the lemma may be stated as the equivalence of the predicates `GAUSS` and `RESIDUE` under suitable restrictions on their arguments. The proof, which involves some fifty additional lemmas, is outlined below.

Consider the integers

$$s_k = \begin{cases} r_k \text{ if } r_k \leq \frac{p-1}{2} \\ p - r_k \text{ if } r_k > \frac{p-1}{2}, \end{cases}$$

$k = 1, \ldots, \frac{p-1}{2}$. For $n \leq \frac{p-1}{2}$, the set $\{s_1, \ldots, s_n\}$ may be represented as a list returned by the following function:

Definition 5

```
(REFLECTIONS N A P)
        =
(IF (ZEROP N)
    NIL
  (IF (LESSP (QUOTIENT P 2) (REMAINDER (TIMES A N) P))
      (CONS (DIFFERENCE P (REMAINDER (TIMES A N) P))
            (REFLECTIONS (SUB1 N) A P))
    (CONS (REMAINDER (TIMES A N) P)
          (REFLECTIONS (SUB1 N) A P))))
```

The congruence class of the product of the s_k may be computed to be

$$\prod_{k=1}^{\frac{p-1}{2}} s_k \equiv (-1)^{\mu} a^{\frac{p-1}{2}} (\frac{p-1}{2})! \pmod{p}.$$

This congruence is represented by the instantiation of the following formula given by the substitution {N ← (QUOTIENT P 2)} (where the function TIMES-LIST is defined to return the product of the members of a list):

Theorem 4

```
(IMPLIES (NOT (ZEROP P))
         (EQUAL (REMAINDER (TIMES-LIST (REFLECTIONS N A P)) P)
                (IF (EVEN (MU N A P))
                    (REMAINDER (TIMES (EXP A N) (FACT N)) P)
                  (DIFFERENCE
                    P (REMAINDER
                        (TIMES (EXP A N) (FACT N)) P)))))
```

If $1 \leq i < j \leq \frac{p-1}{2}$, then r_i, r_j, $p - r_i$, and $p - r_j$ are pairwise distinct, hence $s_i \neq s_j$. Since each s_k belongs to the set $\{1, 2, \ldots, \frac{p-1}{2}\}$, this set must coincide with $\{s_1, \ldots, s_{\frac{p-1}{2}}\}$. Our formalization of this result involves a predicate PERM, which determines whether two lists have the same members, and a function POSITIVES, which returns an initial segment of the sequence of positive integers:

Theorem 5

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2)) (NOT (DIVIDES P A)))
         (PERM (POSITIVES (QUOTIENT P 2))
               (REFLECTIONS (QUOTIENT P 2) A P)))
```

It follows that $\prod_{k=1}^{\frac{p-1}{2}} s_k = (\frac{p-1}{2})!$:

Theorem 6

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2)) (NOT (DIVIDES P A)))
         (EQUAL (TIMES-LIST (REFLECTIONS (QUOTIENT P 2) A P))
                (FACT (QUOTIENT P 2))))
```

The Gauss Lemma now follows from Theorems 4 and 6:

Theorem 7 *(Gauss Lemma)*

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2))
              (NOT (DIVIDES P A)))
         (EQUAL (GAUSS A P) (RESIDUE A P)))
```

4 A Reformulation of the Reciprocity Law

In this section, we shall use the Gauss Lemma to reduce the reciprocity law to a simpler conjecture, which we then prove in the following section by means of a formalization of Eisenstein's argument. In these two sections, we present the input to the prover that produced these results in its entirety. The initial state of the prover included the library of lemmas developed during the derivation of the results listed in Section 3.

Along with the Gauss Lemma, we shall need an equation that is based on the following simple observation: For any x and any $p > 0$, $x = p\lfloor \frac{x}{p} \rfloor + \overline{x}$, where $\lfloor \frac{x}{p} \rfloor$ and $\overline{x}$ denote the (integer) quotient and remainder, respectively, of x divided by p. Replacing x with the product ka, where $k = 1, \ldots, \frac{p-1}{2}$, we have

$$a \sum_{k=1}^{\frac{p-1}{2}} k = p \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor + \sum_{k=1}^{\frac{p-1}{2}} \overline{ka}. \tag{1}$$

Our encoding of Equation (1) depends on a function that computes the sum of the members of a list, as well as two functions that construct the lists that are summed on the right side of the equation:

Definition 6

```
(SUM L) = (IF (LISTP L) (PLUS (CAR L) (SUM (CDR L))) 0))
```

Definition 7

```
(QUOTIENTS N A P)
         =
(IF (ZEROP N)
    NIL
  (CONS (QUOTIENT (TIMES A N) P)
        (QUOTIENTS (SUB1 N) A P)))
```

Definition 8

```
(REMAINDERS N A P)
         =
(IF (ZEROP N)
    NIL
  (CONS (REMAINDER (TIMES A N) P)
        (REMAINDERS (SUB1 N) A P)))
```

Equation (1) is a special case of the following, which was directly verified by the prover by induction:

Theorem 8

```
(EQUAL (TIMES A (SUM (POSITIVES N)))
       (PLUS (TIMES P (SUM (QUOTIENTS N A P)))
             (SUM (REMAINDERS N A P))))
```

As a trivial consequence, we observe that the two sides of the equation have the same parity:

Theorem 9

```
(EQUAL (EVEN (TIMES A (SUM (POSITIVES N))))
       (EVEN (PLUS (TIMES P (SUM (QUOTIENTS N A P)))
                   (SUM (REMAINDERS N A P)))))
```

Advice: Use Theorem 8

Under the assumption that p is odd, μ is even iff $\sum_{k=1}^{\frac{p-1}{2}} \overline{ka}$ and $\sum_{k=1}^{\frac{p-1}{2}} s_k$ have the same parity. This observation corresponds to the following theorem:

Theorem 10 *(rewrite)*

```
(IMPLIES (NOT (EVEN P))
         (EQUAL (EVEN (MU N A P))
                (IFF (EVEN (SUM (REMAINDERS N A P)))
                     (EVEN (SUM (REFLECTIONS N A P))))))
```

Advice: Disable `EVEN`

Note that in order for the proof of this theorem to succeed, the prover had to be advised to disable the definition of `EVEN`. The reason for this is that several rewrite rules pertaining to this function, which were required for the proof, would no longer be applicable if the definition of this function were expanded.

It follows from $\{s_1, \ldots, s_{\frac{p-1}{2}}\} = \{1, \ldots, \frac{p-1}{2}\}$ that $\sum_{k=1}^{\frac{p-1}{2}} s_k = \sum_{k=1}^{\frac{p-1}{2}} k$. The formal proof of this fact depends on Theorem 5 and two preliminary lemmas:

Theorem 11 *(rewrite)*

```
(IMPLIES (MEMBER X M)
         (EQUAL (PLUS X (SUM (DELETE X M))) (SUM M)))
```

Theorem 12

```
(IMPLIES (PERM L M) (EQUAL (SUM L) (SUM M)))
```

Theorem 13 *(rewrite)*

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2)) (NOT (DIVIDES P A)))
         (EQUAL (SUM (REFLECTIONS (QUOTIENT P 2) A P))
                (SUM (POSITIVES (QUOTIENT P 2)))))
```

Advice: Use Theorem 12 with
{`M` ← `(REFLECTIONS (QUOTIENT P 2) A P)`,
`L` ← `(POSITIVES (QUOTIENT P 2))`}
Use Theorem 5
Disable `PRIME`

Next, we prove (as a consequence of Theorems 9 and 10) that a is a quadratic residue modulo p iff $\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor$ is even:

Theorem 14

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2))
              (NOT (EVEN A)) (NOT (DIVIDES P A)))
         (EQUAL (GAUSS A P)
                (EVEN (SUM (QUOTIENTS (QUOTIENT P 2) A P)))))
```

Advice: Use Theorem 9 with $\{\texttt{N} \leftarrow \texttt{(QUOTIENT P 2)}\}$
Disable PRIME*,* EVEN

It follows from Theorems 7 and 14 that $(\frac{p}{q}) = (\frac{q}{p})$ iff $\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor$ and $\sum_{k=1}^{\frac{q-1}{2}} \lfloor \frac{kp}{q} \rfloor$ have the same parity:

Theorem 15 *(rewrite)*

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2))
              (PRIME Q) (NOT (EQUAL Q 2))
              (NOT (EQUAL P Q)))
         (EQUAL (EQUAL (RESIDUE Q P) (RESIDUE P Q))
                (EVEN (PLUS (SUM (QUOTIENTS (QUOTIENT P 2) Q P))
                            (SUM (QUOTIENTS (QUOTIENT Q 2)
                                            P Q))))))
```

Advice: Use Theorem 7 with $\{\texttt{A} \leftarrow \texttt{Q}\}$
Use Theorem 7 with $\{\texttt{A} \leftarrow \texttt{P}, \texttt{P} \leftarrow \texttt{Q}\}$
Use Theorem 14 with $\{\texttt{A} \leftarrow \texttt{Q}\}$
Use Theorem 14 with $\{\texttt{A} \leftarrow \texttt{P}, \texttt{P} \leftarrow \texttt{Q}\}$
Disable PRIME1*,* EVEN*,* GAUSS*,* RESIDUE

In view of Theorem 15, our goal now is to prove the equation

$$\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor + \sum_{k=1}^{\frac{q-1}{2}} \lfloor \frac{kp}{q} \rfloor = \frac{p-1}{2}\frac{q-1}{2} \tag{2}$$

where p and q are distinct odd primes. Thus,

Conjecture 2

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2))
              (PRIME Q) (NOT (EQUAL Q 2))
              (NOT (EQUAL P Q)))
         (EQUAL (PLUS (SUM (QUOTIENTS (QUOTIENT P 2) Q P))
                      (SUM (QUOTIENTS (QUOTIENT Q 2) P Q)))
                (TIMES (QUOTIENT P 2) (QUOTIENT Q 2))))
```

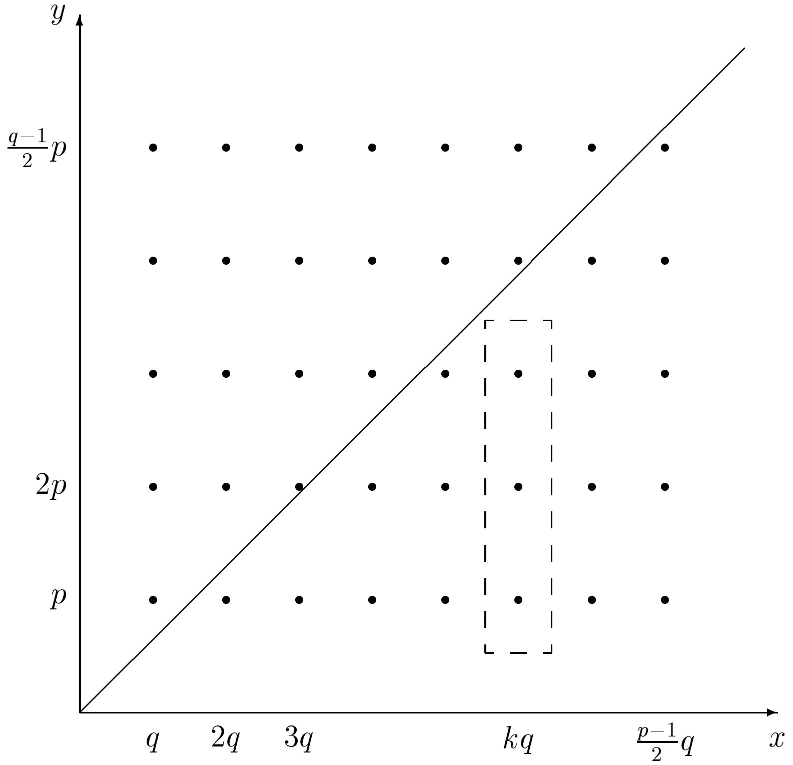

Figure 1: Eisenstein's Proof

5 A Formalization of Eisenstein's Proof

Eisenstein's proof of Equation (2) refers to Figure 1, which depicts the case $p = 17$, $q = 11$. The lattice in the figure consists of the points (iq, jp) with $1 \leq i \leq \frac{p-1}{2}$ and $1 \leq j \leq \frac{q-1}{2}$. Clearly, the number of lattice points is given by the right side of Equation (2). Since $iq = jp$ requires that i and j be divisible by p and q, respectively, none of these points can lie on the line $y = x$.

The equation follows from the observation that the sums on the left side represent the numbers of lattice points that lie below and above the line $y = x$, respectively. In order to see this, consider, for example, a typical term $\lfloor \frac{kq}{p} \rfloor$ of the first sum. This is the number of positive multiples of p that do not exceed kq, which is also the number of lattice points in the boxed column of Figure 1. The proof is completed by summing over all $\frac{p-1}{2}$ columns and repeating the argument for the $\frac{q-1}{2}$ rows of points that lie above the line $y = x$.

The essence of the geometric component of this argument may be formulated as follows: Given a number x and a sequence $L = (a_1, \ldots, a_\ell)$ of numbers, let $w(x, L)$ denote the number of $i \leq \ell$ such that $a_i < x$. If $K = (b_1, \ldots, b_k)$ is another sequence of numbers with no entries in common with L, then

$$\sum_{i=1}^{k} w(b_i, L) + \sum_{j=1}^{\ell} w(a_j, K) = k\ell. \tag{3}$$

Our formalization of Equation (3) is based on two definitions:

Definition 9

```
(W X L)
   =
(IF (LISTP L)
    (IF (LESSP (CAR L) X)
        (ADD1 (W X (CDR L)))
      (W X (CDR L)))
  0)
```

Definition 10

```
(WINS K L)
     =
(IF (LISTP K)
    (PLUS (W (CAR K) L) (WINS (CDR K) L))
  0)
```

Thus, the value of `(WINS K L)` is the total number of pairs of which the first and second components are members of `K` and `L`, respectively, and the first exceeds the second. `K` and `L` are assumed to be lists of numbers, i.e., they satisfy

Definition 11

```
(ALL-NUMBERP L)
      =
(IF (LISTP L)
    (AND (NUMBERP (CAR L)) (ALL-NUMBERP (CDR L)))
  T)
```

The proof of Equation (3) will also involve two companion functions to W and WINS:

Definition 12

```
(L X L)
   =
(IF (LISTP L)
    (IF (LESSP X (CAR L))
        (ADD1 (L X (CDR L)))
      (L X (CDR L)))
  0)
```

Definition 13

```
(LOSSES K L)
     =
(IF (LISTP K)
    (PLUS (L (CAR K) L) (LOSSES (CDR K) L))
  0)
```

The relationship between W and L is given by

Theorem 16 *(rewrite)*

```
(IMPLIES (AND (NUMBERP X) (ALL-NUMBERP L) (NOT (MEMBER X L)))
         (EQUAL (PLUS (L X L) (W X L))
                (LENGTH L)))
```

Similarly, the next two theorems establish the relationship between WINS and LOSSES:

Theorem 17 *(rewrite)*

```
(IMPLIES (AND (NOT (LISTP (INTERSECT K L)))
              (ALL-NUMBERP K) (ALL-NUMBERP L))
         (EQUAL (PLUS (WINS K L) (LOSSES K L))
                (TIMES (LENGTH K) (LENGTH L))))
```

Theorem 18

```
(EQUAL (LOSSES K L) (WINS L K))
```

Equation (3) is represented by the following, which is derived from Theorems 17 and 18. Note that one of these theorems was supplied as a hint and the other was discovered automatically as a rewrite rule:

Theorem 19 *(rewrite)*

```
(IMPLIES (AND (NOT (LISTP (INTERSECT K L)))
              (ALL-NUMBERP K) (ALL-NUMBERP L))
         (EQUAL (PLUS (WINS K L) (WINS L K))
                (TIMES (LENGTH K) (LENGTH L))))
```

Advice: Use Theorem 18

The lists to which Theorem 19 will be applied are lists of multiples of the primes p and q, which are constructed by the following function:

Definition 14

```
(MULTS N P)
     =
(IF (ZEROP N) NIL (CONS (TIMES N P) (MULTS (SUB1 N) P)))
```

The next three theorems will ensure that the hypotheses of Theorem 19 are satisfied:

Theorem 20 *(rewrite)*

```
(IMPLIES (NOT (ZEROP P)) (ALL-NUMBERP (MULTS N P)))
```

Theorem 21 *(rewrite)*

```
(IMPLIES (AND (PRIME P) (PRIME Q) (NOT (EQUAL P Q))
              (LESSP I Q) (LESSP J P))
         (NOT (MEMBER (TIMES I P) (MULTS J Q))))
```

Advice: Induct according to `(MULTS J Q)`

Theorem 22 *(rewrite)*

```
(IMPLIES (AND (PRIME P) (PRIME Q)
              (NOT (EQUAL P Q)) (LESSP I Q))
         (NOT (LISTP (INTERSECT (MULTS I P)
                                (MULTS (QUOTIENT P 2) Q)))))
```

Advice: Disable `PRIME1`, `QUOTIENT`
Induct according to `(MULTS I P)`

The length of a list returned by MULTS is easily seen to be its first argument:

Theorem 23 *(rewrite)*

```
(IMPLIES (NUMBERP N) (EQUAL (LENGTH (MULTS N P)) N))
```

In light of Theorems 19, 20, 22, and 23, Conjecture 2 is reduced to

Conjecture 3

```
(IMPLIES (AND (PRIME P) (PRIME Q) (NOT (EQUAL P Q)))
         (EQUAL (SUM (QUOTIENTS (QUOTIENT P 2) Q P))
                (WINS (MULTS (QUOTIENT P 2) Q)
                      (MULTS (QUOTIENT Q 2) P))))
```

In order to prove Conjecture 3, we must show that for $j = 1, \ldots, \frac{p-1}{2}$,

$$\lfloor \frac{jq}{p} \rfloor = w(jq, M), \tag{4}$$

where M is the sequence $(p, 2p, \ldots, \frac{q-1}{2}p)$ of multiples of p. We shall derive Equation (4) as a conjunction of two inequalities. First, in order to prove

$$w(jq, M) \leq \lfloor \frac{jq}{p} \rfloor, \tag{5}$$

five theorems are required:

Theorem 24

```
(IMPLIES (NOT (ZEROP P))
         (LESSP A (TIMES (ADD1 (QUOTIENT A P)) P)))
```

Theorem 25 *(rewrite)*

```
(NOT (LESSP N (W A (MULTS N P))))
```

Theorem 26 *(rewrite)*

```
(IMPLIES (AND (LESSP A (TIMES M P)) (LEQ M N))
         (LESSP A (TIMES N P)))
```

Theorem 27

```
(IMPLIES (LESSP A (TIMES M P))
         (LESSP (W A (MULTS N P)) M))
```

Theorem 28

```
(IMPLIES (NOT (ZEROP P))
         (LEQ (W A (MULTS N P)) (QUOTIENT A P)))
```

Advice: Use Theorem 24
Use Theorem 27 with $\{$`M` $\leftarrow$ `(ADD1 (QUOTIENT A P))`$\}$

Inequality (5) now follows from Theorem 28 by means of the substitution

$$\{\texttt{A} \leftarrow \texttt{(TIMES J Q)}, \texttt{N} \leftarrow \texttt{(QUOTIENT Q 2)}\}. \tag{6}$$

Next, we prove the remaining inequality,

$$\lfloor \frac{jq}{p} \rfloor \leq w(jq, M). \tag{7}$$

Theorem 29

```
(IMPLIES (LEQ M N)
         (LEQ (W A (MULTS M P)) (W A (MULTS N P))))
```

Advice: Induct according to `(MULTS N P)`

Theorem 30

```
(IMPLIES (LESSP (TIMES N P) A)
         (LEQ N (W A (MULTS N P))))
```

Advice: Induct according to `(MULTS N P)`

Theorem 31

```
(IMPLIES (AND (NOT (ZEROP P))
              (NOT (DIVIDES P A))
              (LEQ (QUOTIENT A P) N))
         (LEQ (QUOTIENT A P) (W A (MULTS N P))))
```

Advice: Use Theorem 29 with $\{$`M` $\leftarrow$ `(QUOTIENT A P)`$\}$
Use Theorem 30 with $\{$`N` $\leftarrow$ `(QUOTIENT A P)`$\}$

Note that Inequality (7) is the instantiation of the conclusion of Theorem 31 under the substitution (6). In order to establish the corresponding instantiation of the third hypothesis of this theorem, three additional lemmas are required. The proof of the first of these lemmas involves an induction scheme that must be explicitly supplied to the prover. A new function is defined solely for this purpose:

Definition 15

```
(LQQ-INDUCT A B C D)
         =
(IF (ZEROP B) T
  (IF (ZEROP D) T
    (IF (LESSP A D) T
      (IF (LESSP C B) T
        (LQQ-INDUCT (DIFFERENCE A D) B (DIFFERENCE C B) D)))))
```

Theorem 32

```
(IMPLIES (AND (NOT (ZEROP B)) (LEQ (TIMES A B) (TIMES C D)))
         (LEQ (QUOTIENT A D) (QUOTIENT C B)))
```

Advice: Induct according to `(LQQ-INDUCT A B C D)`

Theorem 33

```
(IMPLIES (LEQ J A) (LEQ (TIMES J Q) (TIMES A Q)))
```

Theorem 34

```
(IMPLIES (LEQ J (QUOTIENT P 2))
         (LEQ (QUOTIENT (TIMES J Q) P) (QUOTIENT Q 2)))
```

Advice: Use Theorem 32
with {`A` ← `(TIMES J Q)`, `B` ← `2`, `C` ← `Q`, `D` ← `P`}
Use Theorem 33 with {`A` ← `(QUOTIENT P 2)`}

Inequality (7) now follows from Theorems 31 and 34. Thus, Equation (4) is derived from Theorems 28, 31, and 34:

Theorem 35 *(rewrite)*

```
(IMPLIES (AND (PRIME P)
              (NOT (DIVIDES P Q))
              (NOT (ZEROP J))
              (LEQ J (QUOTIENT P 2)))
         (EQUAL (W (TIMES J Q) (MULTS (QUOTIENT Q 2) P))
                (QUOTIENT (TIMES J Q) P)))
```

Advice: Use Theorem 31 with {`A` ← `(TIMES J Q)`, `N` ← `(QUOTIENT Q 2)`}
Use Theorem 28 with {`A` ← `(TIMES J Q)`, `N` ← `(QUOTIENT Q 2)`}
Use Theorem 34

Using Theorem 35 as a rewrite rule, the following is easily proved by induction:

Theorem 36 *(rewrite)*

```
(IMPLIES (AND (PRIME P) (NOT (DIVIDES P Q))
              (LEQ J (QUOTIENT P 2)))
         (EQUAL (SUM (QUOTIENTS J Q P))
                (WINS (MULTS J Q) (MULTS (QUOTIENT Q 2) P))))
```

Advice: Induct according to `(MULTS J Q)`

Substituting `(QUOTIENT P 2)` for `J` in Theorem 36 yields Conjecture 3, and the reciprocity law is essentially proved. Applying Theorems 15, 19, 20, 21, 22, and 36 as rewrite rules, we have

Theorem 37 *(Law of Quadratic Reciprocity)*

```
(IMPLIES (AND (PRIME P) (NOT (EQUAL P 2))
              (PRIME Q) (NOT (EQUAL Q 2))
              (NOT (EQUAL P Q)))
         (EQUAL (EQUAL (RESIDUE Q P) (RESIDUE P Q))
                (EVEN (TIMES (QUOTIENT P 2) (QUOTIENT Q 2)))))
```

Advice: Disable `RESIDUE`, `INTERSECT`

References

[ArT68] Artin, E. and Tate, J., Class Field Theory, Benjamin, New York, 1968.

[BoM79] Boyer, R. S. and Moore, J S., A Computational Logic, Academic Press, New York, 1979.

[BoM84] Boyer, R. S. and Moore, J, *Proof Checking the RSA Public Key Encryption Algorithm*, Am. Math. Monthly 91,3(1984), 181-189.

[BoM88] Boyer, R. S. and Moore, J, A Computational Logic Handbook, Academic Press, Boston, 1988.

[Dun55] Dunnington, G., Carl Friedrich Gauss: Titan of Science, Exposition Press, New York, 1955.

[Gau66] Gauss, K. F., Disquisitiones Arithmeticae, translated by A. Clarke, Yale U. Press, 1966.

[Nag64] Nagell, T., Introduction to Number Theory, Chelsea Press, New York, 1964.

[Rus85] Russinoff, D. M., *An Experiment with the Boyer-Moore Theorem Prover: A Proof of Wilson's Theorem*, J. Automated Reasoning 1 (1985) 121-139.

[Rus90] Russinoff, D. M., *A Mechanical Proof of Quadratic Reciprocity*, forthcoming technical report, MCC, Austin, TX, 1990.