MATH. SCAND. 45 (1979), 177–197

PROOF OF THE QUADRATIC RECIPROCITY LAW IN PRIMITIVE RECURSIVE ARITHMETIC

W. J. RYAN

1. Introduction.

The author extends Thoralf Skolem's [8] development of PR (primitive recursive) arithmetic beyond his proof of the fundamental theorem of arithmetic, by proving Wilson's and Fermat's theorems and the quadratic reciprocity law in PR arithmetic. In section 2, to allow the reader who is not familiar with PR arithmetic to follow our proof, we briefly introduce the PR functions, relations and concepts needed for this paper. In section 3 we prove in PR arithmetic our key theorem, Theorem 3.2, and then we derive certain consequences. (Theorem 3.2 is proved set-theoretically as Corollary 4 to Proposition 2 in no. 2 of § 4 of Chapter III of Bourbaki [1, p. 167].) Then in sections 4, 5 we show that the results obtained in section 3 enable us to transform the ordinary number-theoretic proof of the quadratic reciprocity law given in [6] into a proof in PR arithmetic.

This paper is the result of research on Corollary 1 to Theorem 3.4, which was suggested to the author by Professor R. L. Goodstein as a research problem.

2. Preliminaries.

There are two equivalent formulations of PR arithmetic: *sentential* PR arithmetic, introduced by Skolem [8], and *equational* PR arithmetic, introduced independently by Goodstein [4] and Curry [2]. Both formulations of PR arithmetic assume the natural numbers and the successor function, $x+1$, as given. Then functions are defined by recursion and composition. Proof is by mathematical induction, rules of equality, and, in the sentential formulation, the inference rules of propositional logic. The reader is referred to Skolem [8, 9] and Goodstein [5] for detailed expositions of the sentential and equational PR arithmetics, respectively.

Received June 9, 1977; in revised form May 11, 1979.

In this paper we use the notation of Goodstein [5] and Péter [7]. We use the logical connectives $\sim$ (negation), $\vee$ (disjunction), & (conjunction), $\rightarrow$ (implication) and $\leftrightarrow$ (equivalence). Note that while Skolem takes 1 as the first natural number, we follow current practice and use 0.

The functions of *addition, multiplication* and *exponentiation*, denoted as $x+y$, $x \cdot y$ and x^y, respectively, are defined recursively so that their usual properties hold (by convention we define $0^0=1$). Since we do not have negative integers in PR arithmetic, we cannot define subtraction in the usual way, and so, following current practice, we assume the recursive definition of *restricted subtraction*, denoted as $x \dot{-} y$, which satisfies

$$x \dot{-} y = \begin{cases} 0 & \text{if } x-y<0 \\ x-y & \text{if } x-y \geqq 0 \,, \end{cases}$$

where $x-y$ denotes ordinary subtraction. Then the *inequalities* $x<y$, $x \leqq y$, $x>y$ and $x \geqq y$ are defined in terms of restricted subtraction so that their usual properties concerning addition, multiplication and exponentiation hold. We have the following basic propositions concerning restricted subtraction:

PROPOSITION 2.1. (a) $x \cdot (y \dot{-} z) = x \cdot y \dot{-} x \cdot z$. (b) $(x+z) \dot{-} (y+z) = x \dot{-} y$. (c) $x \dot{-} (y+z) = (x \dot{-} y) \dot{-} z$.

PROPOSITION 2.2. (a) $y \dot{-} (y \dot{-} x) = x \dot{-} (x \dot{-} y)$. (b) $x + (y \dot{-} x) = y + (x \dot{-} y)$.

PROPOSITION 2.3. (a) $x \leqq y \leftrightarrow x = y \dot{-} (y \dot{-} x)$. (b) $x \leqq y \leftrightarrow y = x + (y \dot{-} x)$.

PROPOSITION 2.4. (a) $x \leqq y \leftrightarrow x \dot{-} y = 0$. (b) $x<y \leftrightarrow y \dot{-} x \neq 0$.

The *quotient function* $[x/y]$ and the *remainder function* RM (x/y) (which are denoted as $Q(x,y)$ and $R(x,y)$, respectively, by Goodstein [5, p. 86]) give the quotient and remainder, respectively, obtained by dividing x by y (by convention we have $[x/0]=0$ and RM $(x/0)=x$). We have the following proposition:

PROPOSITION 2.5. (a) $x=[x/y] \cdot y + \mathrm{RM}\,(x/y)$. (b) $y \neq 0 \rightarrow \mathrm{RM}\,(x/y)<y$. (c) RM (RM $(x/y)/y) =$ RM (x/y).

For any PR function $f(y)$, where there may be parameters in addition to y, the *summation function* $\sum_{y=m}^{n} f(y)$ and the *product function* $\prod_{y=m}^{n} f(y)$ (for arbitrary limits m and n) are defined by Péter [7, pp. 24–25] so that if $m \leqq n$, then the usual results hold, while if $n<m$, then

$$\sum_{y=m}^{n} f(y) = 0 \quad \text{and} \quad \prod_{y=m}^{n} f(y) = 1 \,.$$

Next, Péter [7, p. 26] defines the *signum functions* $\mathrm{sg}\,(x)$ and $\overline{\mathrm{sg}}\,(x)$ so that the following propositions hold:

PROPOSITION 2.6. (a) $\mathrm{sg}\,(0)=0$. (b) $x\neq 0 \leftrightarrow \mathrm{sg}\,(x)=1$. (c) $\mathrm{sg}\,(x)=1\dot{-}(1\dot{-}x)$.

PROPOSITION 2.7. (a) $\overline{\mathrm{sg}}\,(0)=1$. (b) $x\neq 0 \leftrightarrow \overline{\mathrm{sg}}\,(x)=0$. (c) $\overline{\mathrm{sg}}\,(x)=1\dot{-}x$. (d) $x=\mathrm{sg}\,(y)\cdot x+\overline{\mathrm{sg}}\,(y)\cdot x$.

Péter [7, p. 54] shows that for any n-place PR functions $f_1,\ldots,f_r$ and any n-place PR relations $P_1,\ldots,P_r$ such that for all $x_1,\ldots,x_n$ exactly one of $P_1(x_1,\ldots,x_n),\ldots,P_r(x_1,\ldots,x_n)$ holds, one can define a "patched together" PR function $g(x_1,\ldots,x_n)$ such that

$$g(x_1,\ldots,x_n) = \begin{cases} f_1(x_1,\ldots,x_n) & \text{if } P_1(x_1,\ldots,x_n) \text{ holds} \\ f_2(x_1,\ldots,x_n) & \text{if } P_2(x_1,\ldots,x_n) \text{ holds} \\ \ldots & \ldots \\ f_r(x_1,\ldots,x_n) & \text{if } P_r(x_1,\ldots,x_n) \text{ holds}\,. \end{cases}$$

For any PR relation $P(y)$, where there may be parameters in addition to y, we define the operators A^n_y, E^n_y, L^n_y, G^n_y and N^n_y as follows:

The *bounded universal operator* A^n_y is defined so that $A^n_y[P(y)]$ is a PR relation which holds if and only if $P(y)$ holds for all y, $0\leqq y\leqq n$. The operator A^n_y is read "for all y from 0 to n".

The *bounded existential operator* E^n_y is defined so that $E^n_y[P(y)]$ is a PR relation which holds if and only if there exists a y, $0\leqq y\leqq n$, such that $P(y)$ holds. The operator E^n_y is read "there exists a y between 0 and n (inclusive)".

The *bounded minimal operator* L^n_y is defined so that $L^n_y[P(y)]$ is a PR function which, if $E^n_y[P(y)]$, gives the least y, $0\leqq y\leqq n$, for which $P(y)$ holds, and which has the value 0 if $\sim E^n_y[P(y)]$. We always have $L^n_y[P(y)]\leqq n$, and, if $E^n_y[P(y)]$, we have $P(L^n_y[P(y)])$. The operator L^n_y is read "the least y from 0 to n".

Using [5, Example 3.6, p. 84], one defines the *bounded maximal operator* G^n_y so that $G^n_y[P(y)]$ is a PR function which, if $E^n_y[P(y)]$, gives the greatest $y, 0\leqq y\leqq n$, for which $P(y)$ holds, and which has the value n if $\sim E^n_y[P(y)]$. We always have $G^n_y[P(y)]\leqq n$, and, if $E^n_y[P(y)]$, we have $P(G^n_y[P(y)])$. The operator G^n_y is read "the greatest y from 0 to n".

The *counting operator* N^n_y is defined so that $N^n_y[P(y)]$ is a PR function which gives the number of values of $y, 0\leqq y\leqq n$, for which $P(y)$ holds. The operator N^n_y is read "the number of y from 0 to n". For brevity, for any PR function $f(y)$, where there may be parameters in addition to y, we abbreviate the function $N^n_y[f(y)=0]$ as $N_f(n)$.

We give the following proposition solely for later reference:

PROPOSITION 2.8. $y\neq 0 \rightarrow [x/y]=G^x_z[z\cdot y\dot{-}x=0]$.

Next, we let $y \mid x$ denote the *divisibility relation* RM $(x/y)=0$. The usual divisibility properties concerning addition, multiplication and exponentiation are easily proved. Also we have the following proposition concerning divisibility and restricted subtraction, which is proved using Proposition 2.3(b):

PROPOSITION 2.9. $\{z \leqq x \ \& \ y \mid (x \dot{-} z)\} \rightarrow \{y \mid x \leftrightarrow y \mid z\}$.

Since we do not have ordinary subtraction in PR arithmetic, we define the *congruence relation* as follows: We let $x \equiv y \pmod{n}$ denote the relation RM $(x/n)=$ RM (y/n). Using Proposition 2.5(a), one verifies the usual congruence properties which concern addition, multiplication and exponentiation. In particular, we always have $x \equiv \mathrm{RM}\,(x/n) \pmod{n}$. We now give four propositions which concern congruences and restricted subtraction. The proof of each of Propositions 2.10–2.13 uses Proposition 2.3(b). In proving Proposition 2.11 we first obtain

$$n^2 + x \cdot y \; = \; (x + (n \dot{-} x)) \cdot (y + (n \dot{-} y)) + x \cdot y \, ,$$

and in proving Proposition 2.13 we consider the cases $n=0$ and $n \neq 0$.

PROPOSITION 2.10. $\{z \geqq x \ \& \ z \geqq y\} \rightarrow$
$\{x \equiv y \pmod{n} \leftrightarrow z \dot{-} x \equiv z \dot{-} y \pmod{n}\}$.

PROPOSITION 2.11. $\{n \geqq x \ \& \ n \geqq y\} \rightarrow (n \dot{-} x) \cdot (n \dot{-} y) \equiv x \cdot y \pmod{n}$.

PROPOSITION 2.12. $\{n \geqq x \ \& \ z \neq 0\} \rightarrow n \dot{-} x \equiv z \cdot n \dot{-} x \pmod{n}$.

PROPOSITION 2.13. $x \cdot n \dot{-} x \equiv n \dot{-} \mathrm{RM}\,(x/n) \pmod{n}$.

We denote as Prime (n) the PR relation which holds if and only if n is a prime number. Next, the PR function $\mathfrak{p}(n)$ enumerates in order the prime numbers with $\mathfrak{p}(0)=2$, $\mathfrak{p}(1)=3$, and so on. Lastly, the PR function $v(n,k)$ is defined so that the following proposition holds:

PROPOSITION 2.14. *For* $n \geqq 2$, $v(n,k)$ *gives the exponent of* $\mathfrak{p}(k)$ *in the prime factorization of* n, *and we have* $v(0,k)=v(1,k)=0$.

Theorems 2.15 and 2.16 constitute the fundamental theorem of arithmetic:

THEOREM 2.15. $n>1 \rightarrow n=\prod_{y=0}^{n} \mathfrak{p}(y)^{v(n,y)}$.

THEOREM 2.16. $n>1 \ \& \ n=\prod_{y=0}^{n} \mathfrak{p}(y)^{f(n,y)} \rightarrow A_y^n[f(n,y)=v(n,y)]$.

We conclude section 2 with a discussion of *induction restricted to an interval.* Let $P(y)$ be a PR relation, where there may be parameters in addition to y, let z be a variable which does not occur in $P(y)$, and let M and N be PR terms which do not contain z. Then if z is not contained in the hypotheses, if any, that are in effect at a certain point in a proof, then at that point in the proof either of the two following inferences can be made:

(i) If at that point in the proof we obtain $P(M)$ and from the hypotheses $P(z)$ and $M \leqq z < N$ we can obtain $P(z+1)$, then at that point in the proof we can infer

$$A_y^N[M \leqq y \rightarrow P(y)] ,$$

and, further, if $P(y)$ is an equation $f(y)=g(y)$, then we can also infer

$$\sum_{y=M}^{N} f(y) = \sum_{y=M}^{N} g(y) \quad \text{and} \quad \prod_{y=M}^{N} f(y) = \prod_{y=M}^{N} g(y) .$$

(ii) If at that point in the proof from the hypothesis $M \leqq z \leqq N$ we can obtain $P(z)$, then at that point in the proof we can infer

$$A_y^N[M \leqq y \rightarrow P(y)] ,$$

and, further, if $P(y)$ is an equation $f(y)=g(y)$, then we can also infer

$$\sum_{y=M}^{N} f(y) = \sum_{y=M}^{N} g(y) \quad \text{and} \quad \prod_{y=M}^{N} f(y) = \prod_{y=M}^{N} g(y) .$$

We establish the validity of (i): Let H be the conjunction of the hypotheses, if any, that are in effect at that point in the proof. Then

$$H \ \& \ P(z) \ \& \ M \leqq z < N \rightarrow P(z+1)$$

is a theorem, and so one can prove by induction on z, using Propositions 2.3(a) and 2.2(a), that

$$H \rightarrow A_y^{N \dot{-} (N \dot{-} z)}[M \leqq y \rightarrow P(y)]$$

is a theorem. It is easily shown that from

$$A_y^N[M \leqq y \rightarrow f(y)=g(y)]$$

one can obtain

$$\sum_{y=M}^{N} f(y) = \sum_{y=M}^{N} g(y) \quad \text{and} \quad \prod_{y=M}^{N} f(y) = \prod_{y=M}^{N} g(y) .$$

The validity of (ii) follows from (i).

REMARK. In applying induction restriction to an interval, we shall make use of the equivalence $A_y^N[0 \leqq y \to P(y)] \leftrightarrow A_y^N[P(y)]$.

3. Finite bijections.

Let $f(x)$, $g(x)$ and $h(y)$ be PR functions and let S_1 and S_2 be sets defined by:

$$S_1 = \{x \mid x \leqq n \;\&\; g(x)=0\}, \quad S_2 = \{y \mid y \leqq m \;\&\; h(y)=0\}\,.$$

Theorem 3.2 asserts that if $g(n)=h(m)=0$ and S_1 and S_2 are of the same cardinality, then the following three conditions are equivalent:

(i) the restriction of f to S_1 is a surjection onto S_2;
(ii) the restriction of f to S_1 is an injection into S_2;
(iii) the restriction of f to S_1 is a bijection onto S_2.

(In Theorem 3.3 we show that the condition $g(n)=h(m)=0$ can be eliminated.)

We first define a PR function $\sigma(n)$ by the equation $\sigma(n)=\sum_{x=0}^{n} \nu(n,x)$ which gives the following proposition:

PROPOSITION 3.1. *For $n \geqq 2$, $\sigma(n)$ gives the sum of the exponents in the prime factorization of n, with $\sigma(0)=\sigma(1)=0$. Moreover, if $m \neq 0$ and $n \neq 0$, then $\sigma(m \cdot n) = \sigma(m)+\sigma(n)$.*

THEOREM 3.2.

$$\begin{aligned}
&\{g(n)=h(m)=0 \;\&\; N_g(n)=N_h(m)\} \to \\
&\{A_y^m[h(y)=0 \to E_x^n[g(x)=0 \;\&\; f(x)=y]] \leftrightarrow \\
&\{A_x^n[g(x)=0 \to h(f(x))=0 \;\&\; f(x) \leqq m] \;\&\; \\
&A_x^n A_z^n[g(x)=g(z)=0 \;\&\; x \neq z \to f(x) \neq f(z)]\}\}\,.
\end{aligned}$$

PROOF. We first define "patched together" functions $\alpha(x)$ and $\beta(y)$ such that for all x, y,

$$\alpha(x) = \begin{cases} \mathrm{p}(f(x)) & \text{if } g(x)=0 \\ 1 & \text{if } g(x) \neq 0\,, \end{cases} \tag{1}$$

$$\beta(y) = \begin{cases} \mathrm{p}(y) & \text{if } h(y)=0 \\ 1 & \text{if } h(y) \neq 0\,. \end{cases} \tag{2}$$

Next, we let

$$A(n) = \prod_{x=0}^{n} \alpha(x), \quad B(m) = \prod_{y=0}^{m} \beta(y)\,. \tag{3}$$

Lastly, we define a "patched together" function $\gamma(n,y)$ such that for all n, y,

$$\gamma(n,y) = \begin{cases} v(A(n),y) \dot{-} 1 & \text{if } h(y)=0 \\ v(A(n),y) & \text{if } h(y) \neq 0 . \end{cases} \tag{4}$$

With (1), (2), (3) and Proposition 3.1 one proves by induction on n and m that $\sigma(A(n)) = N_g(n)$ and $\sigma(B(m)) = N_h(m)$, which with $N_g(n) = N_h(m)$ yields $\sigma(A(n)) = \sigma(B(m))$.

We now prove the direct part of the theorem. Assume

$$A_y^m[h(y) = 0 \to E_x^n[g(x) = 0 \;\&\; f(x) = y]] . \tag{5}$$

From (5), since $h(m)=0$, there exists an $x_0 \leqq n$ such that $g(x_0)=0$ and $f(x_0) = m$, and from (1) we have $\alpha(x_0) = \mathfrak{p}(f(x_0)) = \mathfrak{p}(m)$. Thus by (3) we have $m < \mathfrak{p}(m) \leqq A(n)$.

Let $y_0 \leqq m$. If $h(y_0)=0$, then by (5) there exists an $x_0 \leqq n$ such that $g(x_0)=0$ and $f(x_0) = y_0$, and with (1) we have $\alpha(x_0) = \mathfrak{p}(y_0)$. Thus with (3) and Proposition 2.14 we have $v(A(n), y_0) \neq 0$, and so with (2) and (4) we obtain

$$\mathfrak{p}(y_0)^{v(A(n),y_0)} = \beta(y_0) \cdot \mathfrak{p}(y_0)^{\gamma(n,y_0)} .$$

If $h(y_0) \neq 0$, we obtain this same result with (2) and (4), and so

$$\prod_{y=0}^{m} \mathfrak{p}(y)^{v(A(n),y)} = \prod_{y=0}^{m} \beta(y) \cdot \prod_{y=0}^{m} \mathfrak{p}(y)^{\gamma(n,y)} .$$

Recalling that $m < A(n)$, we multiply both sides of this last equation by $\prod_{y=m+1}^{A(n)} \mathfrak{p}(y)^{v(A(n),y)}$ and apply σ to both sides, and then with (3), Theorem 2.15 and Proposition 3.1 we obtain

$$\sigma(A(n)) = \sigma(B(m)) + \sigma\left(\prod_{y=0}^{m} \mathfrak{p}(y)^{\gamma(n,y)}\right) + \sigma\left(\prod_{y=m+1}^{A(n)} \mathfrak{p}(y)^{v(A(n),y)}\right),$$

and since $\sigma(A(n)) = \sigma(B(m))$, it follows that

$$\sigma\left(\prod_{y=0}^{m} \mathfrak{p}(y)^{\gamma(n,y)}\right) = 0 , \tag{6}$$

$$\sigma\left(\prod_{y=m+1}^{A(n)} \mathfrak{p}(y)^{v(A(n),y)}\right) = 0 . \tag{7}$$

Now let $x_0 \leqq n$ with $g(x_0)=0$. Then with (1) and (3) we have $\mathfrak{p}(f(x_0)) \mid A(n)$ (whence $f(x_0) \leqq A(n)$). Thus if it were the case that $m < f(x_0)$, then with Propositions 2.14 and 3.1 we would obtain a contradiction of (7). Thus $f(x_0) \leqq m$. Then, if it were the case that $h(f(x_0)) \neq 0$, then with (4) and $\mathfrak{p}(f(x_0)) \mid A(n)$ and Propositions 2.14 and 3.1 we would obtain a contradiction of (6). Thus $h(f(x_0)) = 0$, and so we obtain

$$(8) \qquad A_x^n[g(x) = 0 \rightarrow h(f(x)) = 0 \;\&\; f(x) \leqq m]\,.$$

Now let $x_0 \leqq n$ and $z_0 \leqq n$ with $g(x_0)=g(z_0)=0$ and $x_0 \neq z_0$. Without loss of generality, let $x_0 < z_0$. If it were the case that $f(x_0)=f(z_0)$, then with (1) we would have $\alpha(x_0)=\mathfrak{p}(f(x_0))=\mathfrak{p}(f(z_0))=\alpha(z_0)$, and it would follow that

$$\mathfrak{p}(f(x_0)) \mid \prod_{x=0}^{x_0} \alpha(x) \quad \text{and} \quad \mathfrak{p}(f(x_0)) \mid \prod_{x=x_0+1}^{n} \alpha(x)\,,$$

and with (3) we would have $\mathfrak{p}(f(x_0))^2 \mid A(n)$, which in turn would yield $1 \leqq v(A(n), f(x_0)) \dot{-} 1$. Thus, since by (8) we have $h(f(x_0))=0$ and $f(x_0) \leqq m$, from (4) we would have $1 \leqq \gamma(n, f(x_0))$, which would yield a contradiction of (6). Thus $f(x_0) \neq f(z_0)$, which completes the proof of the direct part of the theorem.

We now prove the converse part of the theorem. Assume

$$(9) \qquad A_x^n[g(x) = 0 \rightarrow h(f(x)) = 0 \;\&\; f(x) \leqq m]\,,$$

$$(10) \qquad A_x^n A_z^n[g(x) = g(z) = 0 \;\&\; x \neq z \rightarrow f(x) \neq f(z)]\,.$$

Assume $m < A(n)$ and let $m+1 \leqq y_0 \leqq A(n)$. Next, let $x_0 \leqq n$. If $g(x_0)=0$, then by (9), $f(x_0) \leqq m < y_0$, and so $f(x_0) \neq y_0$. Thus with (1) we see that $\mathfrak{p}(y_0) \nmid \alpha(x_0)$. The same result follows by (1) if $g(x_0) \neq 0$, and so by (3) we see that $\mathfrak{p}(y_0) \nmid A(n)$, and so $v(A(n), y_0)=0$ (Proposition 2.14), whence $\sum_{y=m+1}^{A(n)} v(A(n),y)=0$, which yields $\sum_{y=0}^{A(n)} v(A(n),y)=\sum_{y=0}^{m} v(A(n),y)$. We obtain this same result if $A(n) \leqq m$ (trivially, if $A(n)=m$), since if $y_0 > A(n)$, then $v(A(n), y_0)=0$ (Proposition 2.14). Thus with the above definition of σ,

$$(11) \qquad \sigma(A(n)) = \sum_{y=0}^{m} v(A(n), y)\,.$$

Now, using (1) and (3), one proves by induction on n that for all y,

$$(12) \qquad \mathfrak{p}(y) \mid A(n) \rightarrow E_x^n[g(x) = 0 \;\&\; f(x) = y]\,,$$

and, using this result, together with (1) and (3), one proves by induction on n that for all y,

$$\mathfrak{p}(y)^2 \mid A(n) \rightarrow E_x^n E_z^n[g(x) = g(z) = 0 \;\&\; x \neq z \;\&\; f(x) = f(z)]\,.$$

Thus for $y_0 \leqq m$ if it were the case that $\mathfrak{p}(y_0)^2 \mid A(n)$, then we would obtain a contradiction of (10). Thus $\mathfrak{p}(y_0)^2 \nmid A(n)$ and so

$$(13) \qquad A_y^m[v(A(n), y) \leqq 1]\,.$$

Now let $y_0 \leqq m$ with $v(A(n), y_0) \neq 0$, in which case $\mathfrak{p}(y_0) \mid A(n)$. Then by (12) there exists an $x_0 \leqq n$ such that $g(x_0)=0$ and $f(x_0)=y_0$. Thus from (9) we have $h(f(x_0))=h(y_0)=0$, and so

$$(14) \qquad A_y^m[v(A(n), y) \neq 0 \rightarrow h(y) = 0]\,.$$

If it were the case that $E_y^m[v(A(n),y)=0 \ \& \ h(y)=0]$, then from (13) and (14) we would clearly have $\sum_{y=0}^m v(A(n),y) < N_h(m)$, which with (11) would yield $\sigma(A(n)) < N_h(m) = N_g(n)$, contradicting $\sigma(A(n)) = N_g(n)$. Thus

$$\sim E_y^m[v(A(n),y) = 0 \ \& \ h(y) = 0] ,$$

whence

$$A_y^m[h(y) = 0 \rightarrow v(A(n),y) \neq 0] . \tag{15}$$

Now let $y_0 \leqq m$ with $h(y_0)=0$. Then from (15) we have $v(A(n),y_0) \neq 0$, whence by Proposition 2.14, $\mathfrak{p}(y_0) \mid A(n)$, and so from (12), $E_x^n[g(x)=0 \ \& \ f(x)=y_0]$, and the converse part of the theorem follows.

We now prove that the hypothesis $g(n)=h(m)=0$ of Theorem 3.2 can be eliminated.

THEOREM 3.3.

$$\begin{aligned}
&\{N_g(n) = N_h(m)\} \rightarrow \\
&\{A_y^m[h(y) = 0 \rightarrow E_x^n[g(x) = 0 \ \& \ f(x) = y]] \leftrightarrow \\
&\quad \{A_x^n[g(x) = 0 \rightarrow h(f(x)) = 0 \ \& \ f(x) \leqq m] \ \& \\
&\quad A_x^n A_z^n[g(x) = g(z) = 0 \ \& \ x \neq z \rightarrow f(x) \neq f(z)]\}\} .
\end{aligned}$$

PROOF. Clearly true for $N_g(n)=N_h(m)=0$. If $N_g(n)$ and $N_h(m)$ are nonzero, then let $n' = G_x^n[g(x)=0]$ and $m' = G_y^m[h(y)=0]$. We then have $g(n')=h(m')=0$ and $N_g(n')=N_h(m')$, and the theorem follows from Theorem 3.2 in a straightforward manner.

COROLLARY.

$$A_y^n E_x^n[f(x) = y] \leftrightarrow \{A_x^n[f(x) \leqq n] \ \& \ A_x^n A_z^n[x \neq z \rightarrow f(x) \neq f(z)]\} .$$

PROOF. Define $g(x) = x \dot{-} n$ and $h(y) = y \dot{-} n$.

THEOREM 3.4.

$$\{N_g(n) = N_h(m) \ \& \ A_y^m[h(y) = 0 \rightarrow E_x^n[g(x) = 0 \ \& \ f(x) = y]]\} \rightarrow$$

$$\sum_{x=0}^{n} \overline{\mathrm{sg}}\,(g(x)) \cdot f(x) = \sum_{y=0}^{m} \overline{\mathrm{sg}}\,(h(y)) \cdot y .$$

PROOF. We define a "patched together" function $\delta(x,y)$ such that for all x, y,

$$\delta(x,y) = \begin{cases} 0 & \text{if } f(x) \neq y \vee g(x) \neq 0 \vee h(y) \neq 0 \\ y & \text{if } f(x) = y \ \& \ g(x) = 0 \ \& \ h(y) = 0 . \end{cases}$$

Then we prove that $\sum_{x=0}^{n}\sum_{y=0}^{m}\delta(x,y)=\sum_{x=0}^{n}\overline{\mathrm{sg}}\,(g(x))\cdot f(x)$ and $\sum_{y=0}^{m}\sum_{x=0}^{n}\delta(x,y)=\sum_{y=0}^{m}\overline{\mathrm{sg}}\,(h(y))\cdot y$, using Theorem 3.3.

Corollary 1. $A_y^n E_x^n[f(x)=y] \to \sum_{x=0}^{n} f(x)=\sum_{y=0}^{n} y$.

Proof. Define $g(x)=x\dot{-}n$ and $h(y)=y\dot{-}n$.

Corollary 2.

$$\{A_x^n[m \leqq x \to m \leqq f(x) \leqq n]\ \&$$

$$A_x^n A_z^n[m \leqq x\ \&\ m \leqq z\ \&\ x \neq z \to f(x) \neq f(z)]\} \to \sum_{x=m}^{n} f(x) = \sum_{y=m}^{n} y\,.$$

Proof. For $n<m$ we use the definition of the summation function (section 2), while if $m\leqq n$, then we define $g(x)=m\dot{-}x$ and $h(y)=m\dot{-}y$.

Theorem 3.5.

$$\{N_g(n) = N_h(m)\ \&\ A_y^m[h(y) = 0 \to E_x^n[g(x) = 0\ \&\ f(x) = y]]\} \to$$

$$\prod_{x=0}^{n} \{\overline{\mathrm{sg}}\,(g(x))\cdot f(x)+\mathrm{sg}\,(g(x))\} =$$

$$\prod_{y=0}^{m} \{\overline{\mathrm{sg}}\,(h(y))\cdot y+\mathrm{sg}\,(h(y))\}\,.$$

Proof. We define a "patched together" function $\varepsilon(x,y)$ such that for all x,y,

$$\varepsilon(x,y) = \begin{cases} 1 & \text{if } f(x)\neq y \vee g(x)\neq 0 \vee h(y)\neq 0 \\ y & \text{if } f(x)=y\ \&\ g(x)=0\ \&\ h(y)=0\,. \end{cases}$$

The proof then follows the lines of the proof of Theorem 3.4.

Corollary.

$$\{A_x^n[m \leqq x \to m \leqq f(x) \leqq n]\ \&$$

$$A_x^n A_z^n[m \leqq x\ \&\ m \leqq z\ \&\ x \neq z \to f(x) \neq f(z)]\} \to$$

$$\prod_{x=m}^{n} f(x) = \prod_{y=m}^{n} y\,.$$

Proof. Parallel to the proof of Corollary 2 to Theorem 3.4.

Proposition 3.6. $m>n \to\ \sim A_y^m E_x^n[f(x)=y]$.

PROOF. From $A^m_y E^n_x[f(x)=y]$ there would exist an $x_0 \leqq n$ with $f(x_0)=m$. Further, we would have $A^n_y E^n_x[f(x)=y]$, and with the Corollary to Theorem 3.3 we would obtain $m=f(x_0)\leqq n$, contradicting $m>n$.

COROLLARY. $m>n \rightarrow E^m_y A^n_x[f(x)\neq y]$.

Next, for any PR relation $P(x,y)$, where there may be parameters in addition to x and y, we define a PR function $\psi_P(m,n,w)$ such that if:

(i) $m\leqq n$,

(ii) for each x_0, $m\leqq x_0\leqq n$, there exists a unique y_0 such that $m\leqq y_0\leqq n$ and $P(x_0,y_0)$ holds,

(iii) for each x_0, $m\leqq x_0\leqq n$, we have $\sim P(x_0,x_0)$,

(iv) for each x_0, $m\leqq x_0\leqq n$, and each y_0, $m\leqq y_0\leqq n$, if $P(x_0,y_0)$ holds, then $P(y_0,x_0)$ also holds,

then the sequence S: $\psi_P(m,n,m)$, $\psi_P(m,n,m+1),\ldots,\psi_P(m,n,n)$ is a permutation of the sequence $m,m+1,\ldots,n$, and, as we prove in Lemma 2 for Theorem 3.11, P holds for the first and second members of S, the third and fourth members of S, and so on.

DEFINITION 3.7. For any PR relation $P(x,y)$, where there may be parameters in addition to x and y, we let $\psi_P(m,n,w)$ denote the PR function defined recursively (with $\psi_P(m,n,0)=0$ and $\psi_P(m,n,w+1)$ defined by a "patched together" function) so that the following three propositions hold:

PROPOSITION 3.8. $w\leqq m \rightarrow \psi_P(m,n,w)=w$.

PROPOSITION 3.9.

$$w > m \ \& \ \mathrm{RM}\,(w/2) \neq \mathrm{RM}\,(m/2) \rightarrow$$

$$\psi_P(m,n,w) = L^n_y[m \leqq y \ \& \ P(\psi_P(m,n,w\dot{-}1),y)]\,.$$

PROPOSITION 3.10.

$$w > m \ \& \ \mathrm{RM}\,(w/2) = \mathrm{RM}\,(m/2) \rightarrow$$

$$\psi_P(m,n,w) = L^n_y[A^{w\dot{-}1}_z[\psi_P(m,\,n,z) \neq y]]\,.$$

REMARK. We note that for any w and m, the hypothesis of exactly one of Propositions 3.8–3.10 holds.

LEMMA 1.

$$A^n_x[m \leqq x \to E^n_y[m \leqq y \ \& \ P(x,y)]] \to$$
$$A^n_w[m \leqq w \to m \leqq \psi_P(m,n,w) \leqq n] \,.$$

PROOF. Assume the hypothesis of the lemma. We derive

$$(1) \qquad A^t_w[m \leqq w \leqq n \to m \leqq \psi_P(m,n,w) \leqq n]$$

using induction on t. Clearly (1) holds for $t=0$.

Assuming that (1) holds for $t=k$, we prove that (1) holds for $t=k+1$ by letting $w \leqq k+1$ with $m \leqq w \leqq n$. If $w<k+1$, then $m \leqq \psi_P(m,n,w) \leqq n$ by the induction hypothesis. If $w=k+1$, then we obtain $m \leqq \psi_P(m,n,w) \leqq n$ by considering the three cases determined by the hypotheses of Propositions 3.8–3.10. In applying Proposition 3.9 we use the induction hypothesis and the hypothesis of the lemma, and in applying Proposition 3.10 we use the Corollary to Proposition 3.6 to obtain $E^n_y A^{w \dot{-} 1}_z[\psi_P(m,n,z) \neq y]$, and then use Proposition 3.8 to show that $\psi_P(m,n,w) \not< m$. The lemma then follows easily.

LEMMA 2.

$$\{A^n_x[m \leqq x \to E^n_y[m \leqq y \ \& \ P(x,y)]] \ \&$$
$$m \leqq w \leqq n \ \& \ \mathrm{RM}\,(w/2) = \mathrm{RM}\,(m/2)\} \to$$
$$P(\psi_P(m,n,w), \psi_P(m,n,w+1)) \,.$$

PROOF. By Lemma 1 we have $m \leqq \psi_P(m,n,w) \leqq n$. Then use the first hypothesis of the lemma and, noting $w+1>m$ and $\mathrm{RM}\,((w+1)/2) \neq \mathrm{RM}\,(m/2)$, use Proposition 3.9.

THEOREM 3.11.

$$\{A^n_x[m \leqq x \to E^n_y[m \leqq y \ \& \ P(x,y)]] \ \&$$
$$A^n_x A^n_y[m \leqq x \ \& \ m \leqq y \ \& \ P(x,y) \to P(y,x)] \ \&$$
$$A^n_x[m \leqq x \to \sim P(x,x)] \ \&$$
$$A^n_x A^n_y A^n_z[m \leqq x \ \& \ m \leqq y \ \& \ m \leqq z \ \& \ y \neq z \ \& \ P(x,y) \to \sim P(x,z)]\}$$
$$\to \prod_{x=m}^{n} \psi_P(m,n,x) = \prod_{y=m}^{n} y \,.$$

PROOF. We note that the hypotheses of the theorem are conditions (ii)–(iv) given in the remark preceding Definition 3.7. We denote the hypotheses of the theorem by $\boldsymbol{H}_1$, $\boldsymbol{H}_2$, $\boldsymbol{H}_3$ and $\boldsymbol{H}_4$, respectively, and we abbreviate the function $\psi_P(m, n, x)$ by $\psi(x)$. We now derive the relation

$$A^n_x A^n_z[m \leqq x \;\&\; m \leqq z \;\&\; x \neq z \rightarrow \psi(x) \neq \psi(z)] \tag{1}$$

using induction (restricted to an interval) on n. We see that (1) holds for 0 since we cannot have $x_0 \leqq 0$, $z_0 \leqq 0$ and $x_0 \neq z_0$.

Assume as induction hypothesis that (1) holds for some $k < n$, and let $m \leqq x_0 \leqq k+1$ and $m \leqq z_0 \leqq k+1$ with $x_0 \neq z_0$. Without loss of generality, let $x_0 < z_0$. With $\boldsymbol{H}_1$ and Lemma 1 we have $m \leqq \psi(x_0) \leqq n$, $m \leqq \psi(z_0) \leqq n$, $m \leqq \psi(x_0+1) \leqq n$ and $m \leqq \psi(z_0 \dot{-} 1) \leqq n$. We have two cases to consider:

Case 1. If $\mathrm{RM}\,(z_0/2) \neq \mathrm{RM}\,(m/2)$, then $\mathrm{RM}\,((z_0 \dot{-} 1)/2) = \mathrm{RM}\,(m/2)$, and so with $\boldsymbol{H}_1$ and Lemma 2 we have

$$P(\psi(z_0 \dot{-} 1), \psi(z_0)) . \tag{2}$$

Subcase 1*a*. If $\mathrm{RM}\,(x_0/2) \neq \mathrm{RM}\,(m/2)$, then $m \leqq x_0 \dot{-} 1$ and so with Lemma 1 we have $m \leqq \psi(x_0 \dot{-} 1) \leqq n$. Since $\mathrm{RM}\,((x_0 \dot{-} 1)/2) = \mathrm{RM}\,(m/2)$, by Lemma 2 we have $P(\psi(x_0 \dot{-} 1), \psi(x_0))$. We have $x_0 \dot{-} 1 \neq z_0 \dot{-} 1$, and so by the induction hypothesis we have $\psi(x_0 \dot{-} 1) \neq \psi(z_0 \dot{-} 1)$. From (2) and $\boldsymbol{H}_2$ we have $P(\psi(z_0), \psi(z_0 \dot{-} 1))$. If it were the case that $\psi(x_0) = \psi(z_0)$, then with $P(\psi(x_0 \dot{-} 1), \psi(x_0))$ we would have $P(\psi(x_0 \dot{-} 1), \psi(z_0))$, which with $\boldsymbol{H}_2$ would yield $P(\psi(z_0), \psi(x_0 \dot{-} 1))$, and so with $\boldsymbol{H}_4$ we would have $\sim P(\psi(z_0), \psi(z_0 \dot{-} 1))$. Thus $\psi(x_0) \neq \psi(z_0)$.

Subcase 1*b*. If $\mathrm{RM}\,(x_0/2) = \mathrm{RM}\,(m/2)$, then with Lemma 2,

$$\mathrm{P}(\psi(x_0), \psi(x_0+1)) . \tag{3}$$

We have $x_0 + 1 \leqq z_0$. If $x_0 + 1 = z_0$, then from (3) we have $P(\psi(x_0), \psi(z_0))$, which with $\boldsymbol{H}_3$ yields $\psi(x_0) \neq \psi(z_0)$. If $x_0 + 1 < z_0$, then

$$\mathrm{RM}\,((x_0+1)/2) \neq \mathrm{RM}\,(m/2) \quad \text{and} \quad \mathrm{RM}\,((z_0 \dot{-} 1)/2) = \mathrm{RM}\,(m/2) ,$$

and so $x_0 + 1 \neq z_0 \dot{-} 1$, and by the induction hypothesis we obtain $\psi(x_0+1) \neq \psi(z_0 \dot{-} 1)$, and so with (3) and $\boldsymbol{H}_4$ we obtain $\sim P(\psi(x_0), \psi(z_0 \dot{-} 1))$. If it were the case that $\psi(x_0) = \psi(z_0)$, then from (2) we would obtain $P(\psi(z_0 \dot{-} 1), \psi(x_0))$, which with $\boldsymbol{H}_2$ would yield $P(\psi(x_0,), \psi(z_0 \dot{-} 1))$. Thus again $\psi(x_0) \neq \psi(z_0)$.

Case 2. Let $\mathrm{RM}\,(z_0/2) = \mathrm{RM}\,(m/2)$. By the Corollary to Proposition 3.6, $E^n_y A^{z_0 \dot{-} 1}_w[\psi(w) \neq y]$, which with Proposition 3.10 yields $A^{z_0 \dot{-} 1}_w[\psi(w) \neq \psi(z_0)]$, and again $\psi(x_0) \neq \psi(z_0)$.

Thus (1) holds for all $k \leqq n$, and so holds for n. The theorem then follows with $\boldsymbol{H}_1$, Lemma 1 and the Corollary to Theorem 3.5.

4. Wilson's and Fermat's theorems.

We begin with the following necessary lemma:

LEMMA.

$$\mathrm{Prime}\,(p) \to A_x^{p\dot{-}2}[2 \leqq x \to E_y^{p\dot{-}2}[2 \leqq y \;\&\; x\cdot y \equiv 1 \pmod{p}]]\,.$$

PROOF. Let $2\leqq x_0\leqq p\dot{-}2$ and derive $A_w^{p\dot{-}1}[\mathrm{RM}\,(x_0\cdot w/p)\leqq p\dot{-}1]$ and

$$A_w^{p\dot{-}1}A_z^{p\dot{-}1}[w \neq z \to \mathrm{RM}\,(x_0\cdot w/p) \neq \mathrm{RM}\,(x_0\cdot z/p)]\,.$$

Then by the Corollary to Theorem 3.3, there exists a $y_0\leqq p\dot{-}1$ such that $\mathrm{RM}\,(x_0\cdot y_0/p)=1$, whence $x_0\cdot y_0\equiv 1 \pmod{p}$. Then show that $2\leqq y_0\leqq p\dot{-}2$.

THEOREM 4.1 (*Wilson's theorem*).

$$p > 1 \to \{(p\dot{-}1)! \equiv p\dot{-}1 \pmod{p} \leftrightarrow \mathrm{Prime}\,(p)\}\,.$$

PROOF. The direct part of the theorem is easily proved. So assume Prime (p). If $p=2$ or $p=3$, then we obtain $(p\dot{-}1)!\equiv p\dot{-}1 \pmod{p}$ by computation. So assume $p\geqq 5$. Let $P(x,y)$ denote the relation $x\cdot y\equiv 1 \pmod{p}$. Then by the Lemma and Theorem 3.11, denoting $\psi_P(2,p\dot{-}2,x)$ by $\psi(x)$, we obtain $\prod_{x=2}^{p\dot{-}2}\psi(x)=\prod_{y=2}^{p\dot{-}2}y=(p\dot{-}2)!$, whence, multiplying both sides by $p\dot{-}1$, we obtain

$$(1) \qquad (p\dot{-}1)\cdot\prod_{x=2}^{[(p\dot{-}2)/2]+1}\{\psi(2\cdot(x\dot{-}1))\cdot\psi(2x\dot{-}1)\} = (p\dot{-}1)!\,.$$

Using the Lemma and Lemma 2 for Theorem 3.11, we derive

$$\prod_{x=2}^{[(p\dot{-}2)/2]+1}\{\psi(2\cdot(x\dot{-}1))\cdot\psi(2x\dot{-}1)\} \equiv 1 \pmod{p}\,,$$

and with (1) we obtain $(p\dot{-}1)!\equiv p\dot{-}1 \pmod{p}$.

THEOREM 4.2 (*Fermat's theorem*).

$$\mathrm{Prime}\,(p) \;\&\; p\nmid a \to a^{p\dot{-}1} \equiv 1 \pmod{p}\,.$$

PROOF. Using the Corollary to Theorem 3.5, we obtain

$$\prod_{x=1}^{p\dot{-}1}\mathrm{RM}\,(x\cdot a/p) = \prod_{y=1}^{p\dot{-}1} y = (p\dot{-}1)!\,,$$

and so clearly $\prod_{x=1}^{p\dot{-}1}(x\cdot a)\equiv(p\dot{-}1)! \pmod{p}$, and the proof is finished in a straightforward manner.

5. The quadratic reciprocity law.

Using Fermat's theorem (Theorem 4.2), we obtain:

PROPOSITION 5.1. $\text{Prime}(p)\ \&\ p\nmid a \rightarrow E^p_x[a\cdot x \equiv b \pmod{p}]$.

Throughout this section we denote $[(p\dot{-}1)/2]$ and $[(q\dot{-}1)/2]$ by p' and q', respectively. Also, using the notation of Gauss [3, p. 88], we make the following two definitions (recall that $\mathrm{RM}(x/n) \equiv x \pmod{n}$ and $n>0 \rightarrow \mathrm{RM}(x/n)<n$):

DEFINITION 5.2. $a\mathrm{R}n \leftrightarrow E^n_x[x^2 \equiv a \pmod{n}]$.

DEFINITION 5.3. $a\mathrm{N}n \leftrightarrow \sim a\mathrm{R}n$.

The expression $a\mathrm{R}n$ is read "a is a quadratic residue of n", and the expression $a\mathrm{N}n$ is read "a is a quadratic nonresidue of n".

PROPOSITION 5.4.

$$\{\text{Prime}(p)\ \&\ 2\nmid p\ \&\ p\nmid a\} \rightarrow$$
$$\{\{a\mathrm{R}p \leftrightarrow a^{p'} \equiv 1 \pmod{p}\}\ \&\ \{a\mathrm{N}p \leftrightarrow a^{p'} \equiv p\dot{-}1 \pmod{p}\}\}\,.$$

PROOF. As in [6, p. 70] we obtain

$$a\mathrm{R}p \rightarrow a^{p'} \equiv 1 \pmod{p}\,. \tag{1}$$

Alternatively, assume $a\mathrm{N}p$ and let $P(x,y)$ denote the relation $x\cdot y \equiv a \pmod{p}$. Since for all x_0, $1 \leqq x_0 \leqq p\dot{-}1$, $p\nmid x_0$, with Proposition 5.1 we obtain

$$A^{p\dot{-}1}_x[1 \leqq x \rightarrow E^{p\dot{-}1}_y[1 \leqq y\ \&\ P(x,y)]]\,,$$

and so with Theorem 3.11 and Wilson's theorem (Theorem 4.1), abbreviating $\psi_P(1,p\dot{-}1,x)$ by $\psi(x)$, we have $\prod_{x=1}^{p\dot{-}1}\psi(x) \equiv p\dot{-}1 \pmod{p}$, and so with $p\dot{-}1 = 2p'$ we obtain

$$\prod_{x=1}^{p'}\{\psi(2\cdot(x\dot{-}1)+1)\cdot\psi(2x)\} \equiv p\dot{-}1 \pmod{p}\,. \tag{2}$$

With Lemma 2 for Theorem 3.11 we obtain

$$A^{p'}_x[1 \leqq x \rightarrow \psi(2\cdot(x\dot{-}1)+1)\cdot\psi(2x) \equiv a \pmod{p}]\,,$$

and so $\prod_{x=1}^{p'}\{\psi(2\cdot(x\dot{-}1)+1)\cdot\psi(2x)\} \equiv \prod_{x=1}^{p'} a \pmod{p}$. Thus with (2) we have $\prod_{x=1}^{p'} a \equiv p\dot{-}1 \pmod{p}$, and so

$$a\mathrm{N}p \rightarrow a^{p'} \equiv p\dot{-}1 \pmod{p}\,. \tag{3}$$

The converses of (1) and (3) follow from $p\dot{-}1 \not\equiv 1 \pmod{p}$.

Definition 5.5. For any PR function $g(X_m, y)$, where X_m denotes the m parameters, if any, which g contains in addition to y, we define a PR function $T_g(X_m, n)$ by the equation $T_g(X_m, n) = \sum_{y=1}^{n} \operatorname{sg}(g(X_m, y))$.

Proposition 5.6. *For $n > 0$, $T_g(X_m, n)$ gives the number of values of y, $1 \leqq y \leqq n$, for which $g(X_m, y) \neq 0$. Further, for $n > 0$, if $g(X_m, n+1) = 0$, then $T_g(X_m, n+1) = T_g(X_m, n)$, and if $g(X_m, n+1) \neq 0$, then $T_g(X_m, n+1) = T_g(X_m, n) + 1$.*

Next, for any PR functions $f(X_m, y)$ and $g(X_m, y)$ $(m \geqq 0)$, we define a "patched together" function $\eta_{f,g}(X_m, n, y)$ so that the following two propositions hold:

Proposition 5.7. $g(X_m, y) = 0 \to \eta_{f,g}(X_m, n, y) = f(X_m, y)$.

Proposition 5.8. $g(X_m, y) \neq 0 \to \eta_{f,g}(X_m, n, y) = n \dot{-} \mathrm{RM}(f(X_m, y)/n)$.

We were able to eliminate the use of the negative number -1 from the statement of Wilson's theorem (Theorem 4.1) by using $p \dot{-} 1$ instead. We use the following procedure for eliminating the need for negative numbers in proofs concerning congruences: We replace any negative number $-x$ occurring in a proof in ordinary number theory by $n \dot{-} \mathrm{RM}(x/n)$, where n is the modulus in question, observing that for $n > 0$,

$$n \dot{-} \mathrm{RM}(x/n) \equiv -x \pmod{n}.$$

Proposition 5.9 thus corresponds to the assertion in ordinary number theory that a product is nonnegative if it contains an even number of negative factors and is nonpositive otherwise.

Proposition 5.9.

$$n > 0 \to$$

$$\left\{\left\{2 \mid T_g(X_m, t) \to \prod_{y=1}^{t} \eta_{f,g}(X_m, n, y) \equiv \prod_{y=1}^{t} f(X_m, y) \pmod{n}\right\} \ \& \right.$$

$$\left\{2 \nmid T_g(X_m, t) \to \right.$$

$$\left.\left.\prod_{y=1}^{t} \eta_{f,g}(X_m, n, y) \equiv n \dot{-} \mathrm{RM}\left(\left\{\prod_{y=1}^{t} f(X_m, y)\right\} \Big/ n\right) \pmod{n}\right\}\right\}.$$

Proof. We first observe that for $t \geqq 1$, $T_g(X_m, t)$ is the number of factors of the form $n \dot{-} \mathrm{RM}(f(X_m, y)/n)$ in the product $\prod_{y=1}^{t} \eta_{f,g}(X_m, n, y)$.

Proof is by induction on t. The proposition holds for $t=0$ by Definition 5.5 and the definitions of the summation and product functions (section 2).

Assume that the proposition holds for $t=k$. If $k=0$, then, using Definition 5.5 and Propositions 5.7, 5.8 and 2.6, we show that the proposition holds for $t=k+1$.

Alternatively, assume that $k \neq 0$. First, let $2 \mid T_g(X_m, k+1)$. If $g(X_m, k+1)=0$, then we obtain the desired result with Proposition 5.6, the induction hypothesis and Proposition 5.7. If $g(X_m, k+1) \neq 0$, then we obtain the desired result with Proposition 5.6, the induction hypothesis and Propositions 5.8, 2.5 (b) and 2.11.

Next, let $2 \nmid T_g(X_m, k+1)$. If $g(X_m, k+1)=0$, then we obtain the desired result with Proposition 5.6, the induction hypothesis and Propositions 5.7 and 2.13. If $g(X_m, k+1) \neq 0$, then we first use Proposition 5.6, the induction hypothesis and Proposition 5.8. Next, if $\prod_{y=1}^{k} f(X_m, y)=0$, then the desired results follows immediately, while if $\prod_{y=1}^{k} f(X_m, y) \neq 0$, then we use Propositions 2.5 (b), 2.10 and 2.12.

Preparing for our proof of the lemma of Gauss, we make the following two definitions:

Definition 5.10. $\tau(a,p,x)=\mathrm{RM}\,(x \cdot a/p)$.

Definition 5.11. $\omega(a,p,x)=\mathrm{RM}\,(x \cdot a/p) \dot{-} p'$.

Proposition 5.12. $\omega(a,p,x)=0 \leftrightarrow \mathrm{RM}\,(x \cdot a/p) \leqq p'$.

Proposition 5.13.

$$2 \nmid p \rightarrow \{\omega(a,p,x) \neq 0 \leftrightarrow [(p+1)/2] \leqq \mathrm{RM}\,(x \cdot a/p)\}\,.$$

With Propositions 5.7, 5.8 and 2.5 (c) and Definition 5.10, we also have the following two propositions:

Proposition 5.14.

$$\omega(a,p,x) = 0 \rightarrow \eta_{\tau,\omega}(a,p,p,x) = \mathrm{RM}\,(x \cdot a/p)\,.$$

Proposition 5.15.

$$\omega(a,p,x) \neq 0 \rightarrow \eta_{\tau,\omega}(a,p,p,x) = p \dot{-} \mathrm{RM}\,(x \cdot a/p)\,.$$

Remark. The following lemma asserts that if p is an odd prime with $p \nmid a$ and

$$S = \{\mathrm{RM}\,(a/p), \mathrm{RM}\,(2a/p), \ldots, \mathrm{RM}\,(p' \cdot a/p)\}\,,$$

and $r_1,\ldots,r_n$ denote the members of S exceeding p', and $s_1,\ldots,s_k$ denote the remaining members of S, then the sequence $s_1,\ldots,s_k,p\dot{-}r_1,\ldots,p\dot{-}r_n$ is a permutation of the sequence $1,2,\ldots,p'$.

LEMMA.

$$\begin{gathered}\{\mathrm{Prime}\,(p)\ \&\ 2\nmid p\ \&\ p\nmid a\}\rightarrow\\ \{A_x^{p'}[1\leqq x\rightarrow 1\leqq \eta_{\tau,\omega}(a,p,p,x)\leqq p']\ \&\\ A_x^{p'}A_z^{p'}[1\leqq x\ \&\ 1\leqq z\ \&\ x\neq z\rightarrow\\ \eta_{\tau,\omega}(a,p,\ p,x)\neq \eta_{\tau,\omega}(a,p,p,z)]\}\ .\end{gathered}$$

PROOF. First, for any $x_0, 1\leqq x_0\leqq p'$, from Propositions 5.12–5.15 it follows that if $\omega(a,p,x_0)=0$, then $\eta_{\tau,\omega}(a,p,p,x_0)$ corresponds to an s_i in the preceding remark, while if $\omega(a,p,x_0)\neq 0$, then $\eta_{\tau,\omega}(a,p,p,x_0)$ corresponds to a $p\dot{-}r_j$ in the preceding remark. The proof then follows in the usual way (see, e.g., [6, p. 70, proof of Theorem 3.2]).

Before proving the lemma of Gauss, we observe that for any odd prime p, $T_\omega(a,p,p')$ gives the number of members of the set

$$\{\mathrm{RM}\,(a/p),\mathrm{RM}\,(2a/p),\ldots,\mathrm{RM}\,(p'\cdot a/p)\}$$

which exceed p' (see Propositions 5.6 and 5.13).

THEOREM 5.16 (*Lemma of Gauss*).

$$\{\mathrm{Prime}\,(p)\ \&\ 2\nmid p\ \&\ p\nmid a\}\rightarrow\{a\mathrm{R}p\leftrightarrow 2\,|\,T_\omega(a,p,p')\}\ .$$

PROOF. Since $\prod_{x=1}^{p'}\mathrm{RM}\,(x\cdot a/p)\equiv\{\prod_{x=1}^{p'}x\}\cdot a^{p'}\pmod p$, with Proposition 5.9, Definition 5.10, the Lemma, the Corollary to Theorem 3.5 and Proposition 2.13 we obtain

$$2\,|\,T_\omega(a,p,p')\rightarrow\prod_{x=1}^{p'}x\equiv\left\{\prod_{x=1}^{p'}x\right\}\cdot a^{p'}\pmod p\,, \tag{1}$$

$$2\nmid T_\omega(a,p,p')\rightarrow\prod_{x=1}^{p'}x\equiv\left\{\prod_{x=1}^{p'}x\right\}\cdot a^{p'}\cdot(p\dot{-}1)\pmod p\,. \tag{2}$$

The theorem then follows with Proposition 5.4.

LEMMA 1.

$$\{\mathrm{Prime}\,(p)\ \&\ 2\nmid p\ \&\ 2\nmid a\ \&\ p\nmid a\}\rightarrow\left\{a\mathrm{R}p\leftrightarrow 2\left|\ \sum_{x=1}^{p'}[x\cdot a/p]\right.\right\}.$$

PROOF. Trivial for $a=1$. So let $a\geqq 3$. With Propositions 2.5 (a) and 2.7 (d) we have

$$(1)\qquad a\cdot\sum_{x=1}^{p'} x = p\cdot\sum_{x=1}^{p'}[x\cdot a/p]+\sum_{x=1}^{p'}\overline{\mathrm{sg}}\,(\omega(a,p,x))\cdot \mathrm{RM}\,(x\cdot a/p)+$$
$$\sum_{x=1}^{p'}\mathrm{sg}(\omega(a,p,x))\cdot\mathrm{RM}\,(x\cdot a/p)\,.$$

Next, with the Lemma for Theorem 5.16, Corollary 2 to Theorem 3.4 and Propositions 5.14 and 5.15 we obtain

$$\sum_{x=1}^{p'} x = \sum_{x=1}^{p'}\overline{\mathrm{sg}}\,(\omega(a,p,x))\cdot\mathrm{RM}\,(x\cdot a/p)+$$
$$\sum_{x=1}^{p'}\mathrm{sg}\,(\omega(a,p,x))\cdot(p\dot{-}\mathrm{RM}\,(x\cdot a/p))\,,$$

which subtracted from (1) yields

$$(a\dot{-}1)\cdot\sum_{x=1}^{p'}x = \left\{p\cdot\sum_{x=1}^{p'}[x\cdot a/p]+\sum_{x=1}^{p'}\mathrm{sg}\,(\omega(a,p,x))\cdot\mathrm{RM}\,(x\cdot a/p)\right\}\dot{-}$$
$$\sum_{x=1}^{p'}\{\mathrm{sg}\,(\omega(a,p,x))\cdot p\dot{-}\mathrm{sg}\,(\omega(a,p,x))\cdot\mathrm{RM}\,(x\cdot a/p)\}$$
$$= \left\{p\cdot\sum_{x=1}^{p'}[x\cdot a/p]+\sum_{x=1}^{p'}\mathrm{sg}\,(\omega(a,p,x))\cdot\mathrm{RM}\,(x\cdot a/p)\right\}\dot{-}$$
$$\left\{\sum_{x=1}^{p'}\mathrm{sg}\,(\omega(a,p,x))\cdot p\dot{-}\sum_{x=1}^{p'}\mathrm{sg}\,(\omega(a,p,x))\cdot\mathrm{RM}\,(x\cdot a/p)\right\}$$
$$= \left\{p\cdot\sum_{x=1}^{p'}[x\cdot a/p]+2\cdot\sum_{x=1}^{p'}\mathrm{sg}\,(\omega(a,p,x))\cdot\mathrm{RM}\,(x\cdot a/p)\right\}\dot{-}$$
$$p\cdot T_\omega(a,p,p')$$

(see Definition 5.5). Thus, since $(a\dot{-}1)\cdot\sum_{x=1}^{p'}x\neq 0$, we have

$$p\cdot T_\omega(a,p,p') < p\cdot\sum_{x=1}^{p'}[x\cdot a/p]+2\cdot\sum_{x=1}^{p'}\mathrm{sg}\,(\omega(a,p,x))\cdot\mathrm{RM}\,(x\cdot a/p)\,,$$

and then, since $2\,|\,(a\dot{-}1)$, the lemma follows from the lemma of Gauss (Theorem 5.16) and Proposition 2.9.

LEMMA 2.

$$\{\mathrm{Prime}\,(p)\ \&\ \mathrm{Prime}\,(q)\ \&\ p\neq q\ \&\ 2\nmid p\ \&\ 2\nmid q\ \&\ 1\leqq x\leqq p'\}\rightarrow$$
$$\sum_{y=1}^{q'}\mathrm{sg}\,(x\cdot q\dot{-}y\cdot p) = [x\cdot q/p]\,.$$

PROOF. If $\sum_{y=1}^{q'} \mathrm{sg}(x\cdot q \dot{-} y\cdot p)=0$, then $\mathrm{sg}(x\cdot q \dot{-} 1\cdot p)=0$, whence $x\cdot q<p$, and so $[x\cdot q/p]=0$.

If $\sum_{y=1}^{q'} \mathrm{sg}(x\cdot q \dot{-} y\cdot p)\neq 0$, then $E_y^{q'}[1\leqq y \ \&\ y\cdot p<x\cdot q]$, and so, denoting $G_y^{q'}[1\leqq y \ \&\ y\cdot p<x\cdot q]$ by y_0, we have $1\leqq y_0$ and $y_0\cdot p<x\cdot q$. We also have $y_0\leqq q'$.

If $y_0<q'$, then clearly $\sum_{y=y_0+1}^{q'} \mathrm{sg}(x\cdot q \dot{-} y\cdot p)=0$, and so

$$(1) \qquad \sum_{y=1}^{q'} \mathrm{sg}(x\cdot q \dot{-} y\cdot p) = \sum_{y=1}^{y_0} \mathrm{sg}(x\cdot q \dot{-} y\cdot p)\,,$$

while if $y_0=q'$, then (1) holds trivially.

From $y_0\cdot p<x\cdot q$ we have $A_w^{y_0}[1\leqq w \rightarrow \mathrm{sg}(x\cdot q \dot{-} w\cdot p)=1]$, and so with (1) we obtain

$$(2) \qquad \sum_{y=1}^{q'} \mathrm{sg}(x\cdot q \dot{-} y\cdot p) = y_0\,.$$

Now let $w_0\leqq x\cdot q$ with $y_0<w_0$. If $w_0\leqq q'$, then from the above definition of y_0 we have $w_0\cdot p \not< x\cdot q$, whence $x\cdot q\leqq w_0\cdot p$. If, on the other hand, $q'<w_0$, then $(q'+1)\cdot p\leqq w_0\cdot p$. Also, from $x\leqq p'$ we have $x\cdot q\leqq p'\cdot q$, and so, since $p'\cdot q\leqq (q'+1)\cdot p$, we again have $x\cdot q\leqq w_0\cdot p$. Further, from $p\nmid x\cdot q$ we have $x\cdot q<w_0\cdot p$, whence $w_0\cdot p \dot{-} x\cdot q\neq 0$. Thus $y_0=G_y^{x\cdot q}[y\cdot p \dot{-} x\cdot q=0]$ and so with Proposition 2.8 and (2) we again have the desired result.

THEOREM 5.17 (*Quadratic reciprocity law*).

$$\{\mathrm{Prime}(p)\ \&\ \mathrm{Prime}(q)\ \&\ p\neq q\ \&\ 2\nmid p\ \&\ 2\nmid q\}\rightarrow$$
$$\{\{p\mathrm{R}q \leftrightarrow q\mathrm{R}p\} \leftrightarrow 2\,|\,p'\cdot q'\}\,.$$

PROOF. We first observe that

$$(1) \qquad \sum_{x=1}^{p'}\sum_{y=1}^{q'} \mathrm{sg}(x\cdot y) = p'\cdot q'\,.$$

Next, if $1\leqq x_0\leqq p'$ and $1\leqq y_0\leqq q'$, then since $p\nmid x_0\cdot q$ we have $x_0\cdot q\neq y_0\cdot p$, and so either $x_0\cdot q<y_0\cdot p$ or $y_0\cdot p<x_0\cdot q$, and in either case we have

$$\mathrm{sg}(x_0\cdot y_0) = \mathrm{sg}(x_0\cdot q \dot{-} y_0\cdot p)+\mathrm{sg}(y_0\cdot p \dot{-} x_0\cdot q)\,.$$

Thus we have

$$\sum_{x=1}^{p'}\sum_{y=1}^{q'} \mathrm{sg}(x\cdot y) = \sum_{x=1}^{p'}\sum_{y=1}^{q'} \mathrm{sg}(x\cdot q \dot{-} y\cdot p)+\sum_{y=1}^{q'}\sum_{x=1}^{p'} \mathrm{sg}(y\cdot p \dot{-} x\cdot q)\,,$$

and so with (1) and Lemma 2 we have

$$p'\cdot q' = \sum_{x=1}^{p'}[x\cdot q/p]+\sum_{y=1}^{q'}[y\cdot p/q]\,,$$

and the theorem then follows by Lemma 1.

ACKNOWLEDGEMENTS. The author takes this opportunity to thank Professor R. L. Goodstein and Professor H. A. Pogorzelski for their counsel and encouragement. The author also thanks the referee for his helpful suggestions concerning the organization of this paper. This paper was written while the author was a Research Associate in Mathematics at the University of Maine at Orono, Orono, Maine.

REFERENCES

1. N. Bourbaki, *Elements of Mathematics, Theory of Sets*, Addison–Wesley, Reading, Massachusetts, 1968.
2. H. B. Curry, *A formalization of recursive arithmetic*, Amer. J. Math. 63 (1941), 263–282.
3. C. F. Gauss, *Disquisitiones Arithmeticae*, Yale University Press, New Haven, 1966.
4. R. L. Goodstein, *Function theory in an axiom-free equation calculus*, Proc. London Math. Soc. (2) 48 (1945), 401–434.
5. R. L. Goodstein, *Recursive Number Theory*, North-Holland Publishing Company, Amsterdam, 1964.
6. I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, Second edition, Wiley, New York, 1966.
7. R. Péter, *Recursive Functions*, Academic Press, New York, 1967.
8. T. Skolem, *Begründung der elementaren Arithmetik durch die rekurrierende Denkweise ohne Anwendung scheinbarer Veränderlichen mit unendlichem Ausdehnungsbereich*, Skr. Norske Vid.-Akad. Oslo I No. 6b, 1923.
9. T. Skolem, *The foundations of elementary arithmetic established by means of the recursive mode of thought, without the use of apparent variables ranging over infinite domains*, English translation of Skolem [8], in *From Frege to Gödel*, edited by J. van Heijenoort, Harvard University Press, Cambridge, Massachusetts, 1967, 302–333.

MRC BOX 27
BANGOR, MAINE 04401
U.S.A.