ON THE NATURE AND USE OF THE FUNCTIONS EMPLOYED IN THE RECOGNITION OF QUADRATIC RESIDUES*

BY

EMORY McCLINTOCK

INTRODUCTION.

The congruence $n \equiv x^2 (\text{mod } k)$ is possible, and n is therefore a quadratic residue of k, when n is a quadratic residue of each prime factor of k, so that in order to determine the possibility of the congruence in all cases we must be able to determine its possibility when k is any prime number. The case $k = 2$ is simple, but when k is an odd prime the problem presents some difficulties, and it has perhaps received more attention than any other in the theory of numbers. LEGENDRE introduced the symbol $(n/k) = \pm 1 \equiv n^{\frac{1}{2}(k-1)} (\text{mod } k)$, the sign being $+$ or $-$ as n is or is not a quadratic residue of the prime number k, and since his time the problem has consisted in determining the sign of (n/k) for any given values of n and k, n being prime to the odd prime k. The method of evaluation, or algorithm, of LEGENDRE, improved by JACOBI, is still the standard solution. It requires the use of the *law of quadratic reciprocity* formulated by LEGENDRE, though perceived earlier by EULER: *theorema fundamentale*, as it was called by GAUSS, who first supplied for it a satisfactory demonstration. The derivation of this law has attracted unusual attention from many mathematicians, eight demonstrations having been produced by GAUSS alone. The chief improvement since the time of JACOBI consists in an observation made independently by SCHERING and KRONECKER,† namely, that "GAUSS's characteristic," μ, is available for the proof of the law of reciprocity when k is not prime. The definition $(n/k) = (-1)^{\mu}$, employed by TANNERY in his proof of the usual algorithm, is one of two employed in the present paper, and is herein extended and applied to wider purposes, with only the slightest reference to the law of reciprocity. I find great advantage in substituting for the symbol μ the broader symbol $\mu(n, k)$, so as to be able to discuss the function μ for different values of n and k, and thereby to develop relations of the functions $\mu(n, k)$ im-

* Presented to the Society December 27, 1901. Received for publication November 30, 1901.

† See TANNERY, *Leçons d'Arithmétique* (Paris, 1894); BACHMANN, *Elemente der Zahlentheorie* (Leipzig, 1892); BAUMGART, *Ueber das quadratische Reciprocitätsgesetz* (Göttingen, 1885). These works will be referred to hereafter by the names of the authors.

mediately corresponding to certain elementary relations of the functions (n/k) which are previously set forth from another point of view. The elementary relations supply a simple algorithm for the evaluation of (n/k) without requiring the use of the law of reciprocity. Systems have been proposed in the past for the purpose of avoiding the use of that law, EISENSTEIN's being the best; and a comparison of the new algorithm is therefore desirable, both with that heretofore customary and with that of EISENSTEIN. This paper therefore comprises the following subjects:

I. The function (n/k) and its elementary relations;
II. Theorems, underlying the elementary relations, concerning $\mu(n, k)$;
III. The new algorithm derived from the elementary relations, and
IV. Comparison of the new algorithm with previous methods.

I. THE FUNCTION (n/k) AND ITS ELEMENTARY RELATIONS.

1. Consider the following table of two arguments, n and k, the latter odd:

	$n=1$	2	3	4	5	6	7	8	9
$k=1$	+	+	+	+	+	+	+	+	+
3	+	−		+	−		+	−	
5	+	−	−	+		+	−	−	+
7	+	+	−	+	−	−		+	+
9	+	+		+	+		+	+	
11	+	−	+	+	+	−	−	−	+
13	+	−	+	+	−	−	−	−	+
15	+	+		+			−	+	
17	+	+	−	+	−	−	−	+	+

It is constructed by writing a row and a column alternately in accordance with certain rules, and is assumed to be continued indefinitely. Beginning with + for $n=k=1$, the row $k=1$ is written by repeating + throughout, and the column $n=1$ in the same way. The row $k=3$ has one place thus filled. We fill one place adjacent by changing the sign, and we leave the third (kth) place vacant. The row is then written off in periods of three places by repetition. The column $n=2$ has now two places filled, + −. We fill two more places by repetition with change of sign, and then write off the column by copying periods of four places. The row $k=5$ has now two places filled, + −. We repeat these in inverse order, − +, without change of sign, thus completing four places, leaving the fifth (kth) place vacant, and go on to complete the row in periods of five places by repetition. The column $n=3$ has now three places supplied, say + v −, where v means vacancy. Three more places are filled by copying in direct order with change of sign, − v +, and the column is written off in periods of six places. The row $k=7$ has now three places filled, + + −,

and three more are obtained in inverse order with change of sign, $+ - -$, the rest following in periods of seven, the seventh (kth) place being left vacant. It is now possible to perceive the rules by which the table may be extended without limit, and by which every place shall be occupied by $+$, $-$, or a regular vacancy. For beginning each row, we find $\frac{1}{2}(k-1)$ places already written, belonging to columns previously constructed, and we obtain as many more by copying in inverse order, with change of sign if $\frac{1}{2}(k-1)$ is odd, and the kth place is left vacant; and the rest of the row is written off by repetition, in periods of k places each. For beginning each column, we find n places already written, belonging to rows previously constructed, and we obtain as many more by copying in direct order, with change of sign if n or $n-1$ is of the form $4r+2$; and the rest of the column is written off by repetition, in periods of $2n$ places each. The vacancies occur necessarily wherever n and k contain a common factor, and nowhere else: explicitly if n is a multiple of k, and as a consequence of the mode of writing the rows and columns if both n and k are multiples of some odd prime, say p; because in row p, column p, there is a primary vacancy, which by the rules of formation is repeated for every period of p places throughout the rows and columns, including the row $xp = k$ and the column $yp = n$.

2. The columns may be extended upwards by copying in periods of $2n$ places each, so that k may be negative, and the rows may be extended to the left by copying in periods of k places each, so that n may be negative, but the process cannot be extended so as to make both negative, for the rules of formation are not symmetrical. For example, the place where $k = -5$ and $n = 1$ is a place where $+$ must be written, by repetition from $k = 1$, $n = 1$; and from this, by row-repetition, we might write $+$ in the place where $k = -5$, $n = -4$. But since we have $-$ for $k = 11$, $n = 7$, we must repeat $-$ for $k = 11$, $n = -4$, and from this, by column-repetition, we might write $-$ in the place where $k = -5$, $n = -4$, contrary to the former result.

3. The signs entered in the table, $+$ and $-$, are abbreviations of $+1$ and -1, and these quantities are functions of the integers n and k, the latter being always odd and prime to n. Let the function in question be denoted by (n/k). Then $(1/1) = 1$. From the rules of formation we have, when $n < k$, both being positive,

$$(k - n/k) = (-1)^{\frac{1}{2}(k-1)}(n/k); \tag{1}$$

again, for all values of n, with k positive and x integral,

$$(n/k) = (n - xk/k); \tag{2}$$

and finally, for all values of k, with n positive,

$$(n/k) = (-1)^{\frac{1}{2}xn(n-1)}(n/k - 2xn). \tag{3}$$

These three equations, with $(1/1) = 1$, supply the complete definition of the function (n/k), as has been shown in paragraph 1. Three other important elementary relations exist, namely,

$$(4) \qquad (2n/k) = (-1)^{\frac{1}{2}n(k-1)}(2n/k - 2n),$$

$$(5) \qquad (k'/k) = (-1)^{\frac{1}{4}(k-1)(k'-1)}(k/k'),$$

$$(6) \qquad (m/k)(n/k) = (mn/k).$$

4. For the proof of (4), these lemmas are useful:

$$(A) \qquad (2/k) = (-1)^{\frac{1}{2}c(c+1)} = (-1)^{\frac{1}{8}(k^2-1)}, \qquad \text{where} \qquad k = 2c + 1,$$

$$(B) \qquad (n/2n - k) = (-1)^{\frac{1}{2}n(n-1)}(n/k),$$

$$(C) \qquad (2/k)(n/k) = (2n/k).$$

Pursuing the course of paragraph 1 regarding the column $n = 2$, we obtain (A) by observing that $(2/1) = 1$ follows by (2) from $(1/1) = 1$, and that $(2/3) = -1$ follows by (1) from $(1/3) = 1$, which again comes by (3) from $(1/1) = 1$; after which, by (3), $(2/k) = (-1)^x(2/k - 4x)$, so that if $k = 4x + 1 = 2c + 1$, c is even and $(2/k) = (-1)^{\frac{1}{2}c}$, while if $k = 4x + 3 = 2c + 1$, c is odd and $(2/k) = (-1)^{\frac{1}{2}(c-1)}(2/3) = (-1)^{\frac{1}{2}(c+1)}$, both results combined forming (A). To obtain (B) we have

$$(k + m/k) = (m/k) = (-1)^{\frac{1}{2}m(m-1)}(m/k + 2m)$$
$$= (-1)^{\frac{1}{2}m(m-1)}(-1)^{\frac{1}{2}(k+2m-1)}(k + 2m - m/k + 2m).$$

Writing $n - k$ for m and remarking, concerning the exponents of -1, that $k^2 - 1$ and $2k - 2$ are divisible by 4, we have (B). To prove (C), we remark that it is true when $k = 1$, $k = 3$, etc., and we need to show that it is true for any given value of k provided it is true for all lower values. First, if $k > 2n$, and if k' is the positive value of $\pm(k - 4n)$, we have $k' < k$, and, by (3) and (B), $(n/k) = (n/k')$; also, $(2n/k) = (-1)^n(2n/k')$. By hypothesis, $(2n/k') = (2/k')(n/k')$, and, by (A), $(2/k') = (-1)^{\frac{1}{8}(k^2-1-8n)}$, since $(-1)^n = (-1)^{nk}$, so that $(2n/k) = (-1)^{\frac{1}{8}(k^2-1)}(n/k) = (2/k)(n/k)$. Secondly, if $k < 2n$, let

$$n = mk \pm n',$$

where m is a positive integer and $n' < \frac{1}{2}k$. If the sign is $+$, we have, by (2), $(n'/k) = (n/k)$ and $(2n'/k) = (2n/k)$, while if the sign is $-$, we have, by (1), $(n'/k) = (-1)^{\frac{1}{2}(k-1)}(n/k)$ and $(2n'/k) = (-1)^{\frac{1}{2}(k-1)}(2n/k)$; and we are thus enabled to deal with n' as in the first case we dealt with n.

5. We may now prove (4) by observing that, by (3),

$$(n/k - 2n) = (-1)^{-\frac{1}{2}n(n-1)}(n/k),$$

and, by (A), $(2/k-2n)=(-1)^{\frac{1}{2}n(n-k)}(2/k)$; which being combined by (C) we have $(2/k-2n)(n/k-2n)=(2n/k-2n)=(-1)^{\frac{1}{2}n(1-k)}(2n/k)$, or

$$(4) \qquad (2n/k)=(-1)^{\frac{1}{4}n(k-1)}(2n/k-2n);$$

from which, again, the corollary (5) immediately follows. For

$$(2n/k)=(-1)^{\frac{1}{2}(k-1)}(k-2n/k)$$

and $(2n/k-2n)=(k/k-2n)$, whence $(k-2n/k)=(-1)^{\frac{1}{4}(k-1)(n-1)}(k/k-2n)$. If in this we write k' for $k-2n$, multiplying the second member by $(-1)^{\frac{1}{4}(k^2-1)}=1$ and by $(-1)^{-n(k-1)}=1$, we have

$$(5) \qquad (k'/k)=(-1)^{\frac{1}{4}(k-1)(k'-1)}(k/k').$$

This is in fact the well known law of reciprocity, though it is not yet proved that (n/k), as here already defined, is the (n/k) to which the law of reciprocity has heretofore applied. What is needed for this purpose is proof that $(n/k)=1$ when n is a quadratic residue of k, or, more briefly, that

$$(D) \qquad (n^2/k)=1.$$

See paragraph 21.

6. That (6) becomes (D) when $m=n$ is obvious, since $(n/k)^2=(\pm 1)^2=1$. In view of (2), it is sufficient to prove (6) when both m and n are less than k. We observe that $(m/k)(n/k)=(mn/k)$ is true for the smallest values of k, and we need to show that it is true for any given value of k if it is true for all smaller values. Let us consider that mn is even, namely, $m=2^pa$ and $n=2^qb$, where p or q may be 0, and $p+q=r$, say $mn=2^rab$, where $r>0$ and ab is odd; for if not, m may be replaced by $m'=k-m$, even, because $(m/k)=(-1)^c(m'/k)$ and $(mn/k)=(-1)^c(m'n/k)$, by (1). Since, by (C),

$$(2^pa/k)=(2^p/k)(a/k),\ (2^qb/k)=(2^q/k)(b/k),\ (2^p/k)(2^q/k)=(2^r/k),$$

and

$$(2^rab/k)=(2^r/k)(ab/k),$$

it is sufficient to prove that $(ab/k)=(a/k)(b/k)$. Let $2^rab\pm d=ek$, where d and e are odd and less than k; so that $2^rab\equiv\mp d \pmod k$, $ek\equiv\pm d \pmod a$, etc. Let us assume for the present that d is prime to e, and therefore that both are prime to a and b. Let d have first the negative sign, so that

$$2^rab-d=ek;$$

then

$$(2^rab/k)=(d/k),\ (2^rab/e)=(d/e),\ (2^rab/d)$$
$$=(ek/d),\ (ek/a)=(-d/a),\ (ek/b)=(-d/b),$$

whence—the new letters indicating powers of -1 in accordance with (1), (5), (A), and (C)—

$$(ab/k) = (2^r/k)(d/k) = \text{A}(d/k), \quad (d/k) = \text{B}(k/d) = \text{BC}(e/d)(d/a)(d/b),$$
$$(e/d) = \text{D}(e/a)(e/b), \quad (a/k) = \text{E}(k/a) = \text{EF}(e/a)(d/a),$$
$$(b/k) = \text{G}(k/b) = \text{GH}(e/b)(d/b),$$

and

$$(ab/k) = \text{ABCD}(d/a)(d/b)(e/a)(e/b) = \text{EFGH}(d/a)(d/b)(e/a)(e/b) = (a/k)(b/k),$$

as required, provided ABCDEFGH $= 1$. Let $a = 2\alpha + 1$, $b = 2\beta + 1$, $d = 2\delta + 1$, $e = 2\epsilon + 1$, besides $k = 2c + 1$, as before; then the exponent of -1 in A is $\frac{1}{2}rc(c+1)$, in B is $c\delta$, in C is $\frac{1}{2}r\delta(\delta+1) + \delta(\alpha+\beta)$, in D is $\frac{1}{2}r\epsilon(\epsilon+1) + \epsilon(\delta+\alpha+\beta)$, in E is $c\alpha$, in F is α, in G is $c\beta$, and in H is β, and what is to be proved is the congruence

$$(\alpha+\beta)(\delta+1+c+\epsilon) + \delta(c+\epsilon) + \tfrac{1}{2}r(c^2+c+\delta^2+\delta+\epsilon^2+\epsilon) \equiv 0 \pmod 2.$$

Towards proving this we have $2^rab - d - ek = 2^r(4\alpha\beta + 2\alpha + 2\beta + 1) - 2\delta - 2 - 4c\epsilon - 2c - 2\epsilon = 0$. From this, if $r = 1$, we have $\delta + c + \epsilon \equiv 0 \pmod 2$, and $\alpha + \beta + c\epsilon + \frac{1}{2}(\delta + c + \epsilon) \equiv 0$; and by combining these with the congruence in question, the latter is reduced to an identity, $\frac{1}{2}(\delta + c + \epsilon)^2 \equiv 0 \pmod 2$. If r is even, $\delta + 1 + c + \epsilon \equiv 0 \pmod 2$, which again reduces the congruence to an identity, $\delta(c+\epsilon) \equiv \delta(\delta+1) \equiv 0 \pmod 2$. Finally, if r is greater than 2, and odd, $\delta + 1 + c + \epsilon \equiv 0 \pmod 2$, and $c\epsilon + \frac{1}{2}(\delta + 1 + c + \epsilon) \equiv 0$, by which the congruence is reduced to $\frac{1}{2}(\delta + 1 + c + \epsilon)^2 \equiv 0 \pmod 2$. We have hitherto taken d, in $2^rab \pm d = ek$, with the negative sign: if it be positive, changes must be made to correspond, so that F and H disappear, while A and D are increased respectively by c and ϵ, the required congruence thus becoming

$$(\alpha+\beta)(\delta+c+\epsilon) + (\delta+1)(c+\epsilon) + \tfrac{1}{2}r(c^2+c+\delta^2+\delta+\epsilon^2+\epsilon) \equiv 0 \pmod 2.$$

The given equation is now $2^r(4\alpha\beta + 2\alpha + 2\beta + 1) + 2\delta - 2c - 2\epsilon - 4c\epsilon = 0$. If $r = 1$, $\delta - c - \epsilon + 1 \equiv 0 \pmod 2$, and $\alpha + \beta + c\epsilon + \frac{1}{2}(\delta - c - \epsilon + 1) \equiv 0$, producing the identity $\frac{1}{2}(\delta - c - \epsilon + 1)(\delta - c - \epsilon - 1) \equiv 0$; if r is even, $\delta + c + \epsilon \equiv 0 \pmod 2$, producing $(\delta+1)(c+\epsilon) \equiv -\delta(\delta+1) \equiv 0$; and if r is odd and greater than 2, $\delta + c + \epsilon \equiv 0 \pmod 2$, and $c\epsilon + \frac{1}{2}(c + \epsilon - \delta) \equiv 0$, producing $\frac{1}{2}(\delta + c + \epsilon)^2 \equiv 0$. We have thus far assumed that d, in $mn \pm d = ek$, has no common factor with e, which if mn is even is necessarily true only when $mn < 2k$; and have proved, on that assumption, that $(m/k)(n/k) = (mn/k)$. Let $mt_1 = m'$, $nt_2 = n'$, and $t_1t_2 = t$; t_1 and t_2 being odd and prime to k, and such that m', n', $dt = d'$, and $et = e'$, are all respectively less than k. In the more general expression $m'n' \pm d' = e'k$, d' is not prime to e', but it is now easy to see that

$$(m'/k)(n'/k) = (mt_1/k)(nt_2/k) = (m/k)(n/k)(t_1/k)(t_2/k) = (mn/k)(t_1t_2/k)$$
$$= (\mp d/k)(t/k) = (\mp dt/k) = (\mp d'/k) = (m'n'/k);$$

because $2mt_1$, $2nt_2$, $2t_1t_2$, and $2dt$ are all respectively less than $2k$, and each of them may be represented by $2ab$ in $2ab \pm f = k$, the terms of which are prime to each other.

II. Theorems, underlying the elementary relations, concerning $\mu(n, k)$.

7. Let n and c be positive integers, and let $k = 2c + 1$ be prime to n. Let the number of negative absolutely smallest residues in the series n, $2n$, $\cdots$, $cn \pmod k$ be denoted by $\mu(n, k)$, and let $\mu(n, 1) = 0$. The complementary series $(c+1)n$, $(c+2)n$, $\cdots$, $2cn \pmod k$, or $(k-c)n$, $(k-c+1)n$, $\cdots$, $(k-1)n \pmod k$, comprises the same residues in reverse order, with change of sign. The terms n, $2n$, $\cdots$, $2cn$ being incongruent, modulo k, all the residues of both series, $2c$ in number, are different, comprising the numbers, in some order, from $-c$ to $+c$ inclusive; those of the first series comprising, in some order, every number from 1 to c, each affected by either the positive or the negative sign, and those of the second series comprising the same numbers in reverse order, each with a change of sign. The number of negative residues in the first series being $\mu(n, k)$, that in the complementary series is, therefore, $c - \mu(n, k)$; or, if $n < k$, since $(k-r)n \equiv r(k-n) \pmod k$,

$$(7) \qquad \mu(k-n, k) = c - \mu(n, k) \equiv \tfrac{1}{2}(k-1) + \mu(n, k) \pmod 2.$$

Had $n \pm xk$, positive, with x integral, been taken instead of n in the first series, the residues would have been the same, so that

$$(8) \qquad \mu(n, k) = \mu(n \pm xk, k).$$

Let β, γ, δ be positive integers not greater than c, and let the residue $\beta m \pmod k$ be γ or $-\gamma$, and let $\gamma n \pmod k$ be δ or $-\delta$. Let the number of values of β for which $\beta m \equiv \gamma$, where γ is such that $\gamma n \equiv -\delta$, be denoted by r; for which $\beta m \equiv -\gamma$ when $\gamma n \equiv \delta$, by s; and for which $\beta m \equiv -\gamma$ when $\gamma n \equiv -\delta$, by t. Then in $r + s$ cases we shall have $\beta mn \equiv -\delta$, negative, so that $r + s = \mu(mn, k)$; also, $s + t = \mu(m, k)$, and $r + t = \mu(n, k)$; whence

$$(9) \quad \mu(mn, k) = \mu(m, k) + \mu(n, k) - 2t \equiv \mu(m, k) + \mu(n, k) \pmod 2.$$

8. A second modulus, $k + 2n$, is, with k, prime to n. If n is even, say $n = 2r$, the last residue of the series n, $2n$, $\cdots$, $(c+n)n \pmod{k+2n}$ is $2r(c+2r) - r(2c+1+4r) = -r$, negative, and if n is odd, say $n = 2r+1$, the last residue is $(2r+1)(c+2r+1) - r(2c+4r+3) = c + r + 1$, a positive quantity. The form of each residue being $an - b(k+2n)$, b must have r values, from 1 to r, for each of which there is one negative residue whose value is from $-c-1$ to $-c-n$ inclusive; because, for any given value of b, say $b = g$, there cannot be more than one such residue, since however small al-

gebraically the first may be, say $-c-n$, the next must be $-c$, outside of the limit; and there must be one, for if not, we shall have two adjacent residues, say $an-(g-1)(k+2n)$ and $(a+1)n-(g+1)(k+2n)$, differing in value by as much as $2k+3n$, which is absurd. In addition to the r negative values smaller algebraically than $-c$, there are in the series before us $\mu(n, k)$ negative residues, with values from -1 to $-c$, exactly the same as in the original series $n, 2n, \cdots, cn \pmod k$; for each residue in the original series, say $a=an-bk$, where $b<\frac{1}{2}(n+1)$, since $a<\frac{1}{2}k$, is represented in the larger series by $a=(a+2b)n-b(k+2n)$. Hence, whether $n=2r$ or $n=2r+1$,

$$\mu(n, k+2n)=\mu(n, k)+r. \tag{10}$$

9. All the numbers from 1 to c, each either positive or negative, are residues of the series $2n, 2\cdot 2n, \cdots, c\cdot 2n \pmod k$, where $k=2c+1$, being of the form $a\cdot 2n-bk$, where $b<n+1$ because $a<\frac{1}{2}k$, and are repeated identically as residues of the form $(a+b)2n-b(k+2n)$ in the series

$$2n, 2\cdot 2n, \cdots, (c+n)2n \pmod{k'},$$

where $k'=k+2n$. Every other negative residue of the latter series, say, $a=a\cdot 2n-bk'<-c$, where $a<c+n+1$ and $b<n+1$, is one of a pair, the other being $a'=a'\cdot 2n-b'k'$, where $a'=c+n+1-a$ and $b'=n+1-b$, the sum being $a+a'=-2c-n-1$; unless $a'=\frac{1}{2}(c+n+1)=a$ and $b'=\frac{1}{2}(n+1)=b$, which can occur only when n and $c+1$ are both odd, $c+1$ being $\frac{1}{2}(k+1)$.* Hence,

$$\mu(2n, k')\equiv\mu(2n, k)+\tfrac{1}{2}n(k+1) \pmod 2. \tag{11}$$

By (7) and (8), $\mu(2n, k')\equiv\mu(k, k')+\frac{1}{2}(k'-1) \pmod 2$, and $\mu(2n, k)=\mu(k', k)$, while $\frac{1}{2}n(k+1)-\frac{1}{2}(k'-1)=\frac{1}{2}(k-1)(n-1)\equiv\frac{1}{4}(k-1)(k'-1) \pmod 2$, since $\frac{1}{4}(k^2-1)\equiv 0$, so that

$$\mu(k, k')\equiv\mu(k', k)+\tfrac{1}{4}(k-1)(k'-1) \pmod 2.\dagger \tag{12}$$

* Similarly, every positive residue greater than c is one of a pair, say $a=a\cdot 2n-bk'$ and $a'=(c+n-a)2n-(n-1-b)k'$, the sum being $a+a'=2c+n+1$; with one exception when n and c, or $\frac{1}{2}(k-1)$, are both odd.

† Of the theorems (7) to (12), that numbered (8) is little more than the formulation of a truism; a formula equivalent to a special case of (10), wherein n is odd and n and k are both prime, appears as a step in BUSCHE'S proof of the law of reciprocity (see BAUMGART'S collection of proofs); and (12) is new only in its derivation, being well-known in certain demonstrations of that law, the quantity $\mu(k', k)$ being denoted by ν. The best demonstration is that of ZELLER, which might be incorporated in the present theory if there were need of an independent proof of (12) distinct from that of (11), of which (12) is an immediate corollary. ZELLER'S method, even as recently reproduced by BAUMGART and by BACHMANN, is confined needlessly to purely prime values of k and k'.

10. That the definition $\mu(n, 1) = 0$ is not arbitrary may be seen upon substituting 1 for k and 0 for $\mu(n, k)$ in the congruences numbered (7) to (12), causing both sides of each to vanish identically: both sides of (7), (8) and (9), obviously; of (10), because $\mu(n, 2n+1) = r$, since the series $n, 2n, \cdots, nn \pmod{2n+1}$ supplies negative residues only in the even terms, r in number; of (11), because $\mu(2n, 2n+1) = n$, by (7); and of (12), because $\mu(1, k') = 0$, there being no negative residues in the series $1, 2, \cdots, \frac{1}{2}(k'-1) \pmod{k'}$.

11. The congruences relating to μ are, as has been seen, derived readily from the definition of μ, but the properties expressed by them are not all independent. We have seen that the sixth, numbered (12), follows at once from (7), (8) and (11). It may be shown that independent proof is required for three only, provided the three are rightly chosen. One combination which may serve as a basis for the others comprises (8), (9) and (10). Assuming these to be known, we have from (9)

$$\mu(n^2, k) \equiv 0 \pmod 2. \tag{13}$$

By (10) and (8), when m is even,

$$\mu(m, k) = \mu(m, k+2m) - \tfrac{1}{2}m = \mu(m, k+m^2) - \tfrac{1}{2}m = \mu(m+k+m^2, k+m^2) - \tfrac{1}{2}m.$$

If we put $m = k-1$, we have $m + k + m^2 = k^2$, and, observing (13), we have

$$\mu(k-1, k) \equiv \tfrac{1}{2}(k-1) \pmod 2; \tag{14}$$

Since $\mu(k-n, k) = \mu(kn-n, k) \equiv \mu(k-1, k) + \mu(n, k) \pmod 2$, by (9), we have now the proof of (7). By (10), $\mu(2, 1+4) = \mu(2, 1) + 1 = 1$, and in general, $\mu(2, 1+4m) = m$, or $\mu(2, k) = \frac{1}{2}c$ if c is even; also, by (7), $\mu(2, 3) = 1$ since $\mu(1, 3) = 0$ and $\frac{1}{2}(3-1) = 1$, and as before,

$$\mu(2, 3+4m) = 1 + m,$$

or $\mu(2, k) = \frac{1}{2}(c+1)$ if c is odd. (Both of these results might be had directly from the series $2, 4, \cdots, 2c$, modulo k.) Hence

$$\mu(2, k) \equiv \tfrac{1}{2}c(c+1) \equiv \tfrac{1}{8}(k^2-1) \pmod 2. \tag{15}$$

Therefore $\mu(2, k+2n) \equiv \mu(2, k) + \frac{1}{2}n(n+k) \pmod 2$, and by (10) $\mu(n, k+2n) \equiv \mu(n, k) - \frac{1}{2}n(n-1) \pmod 2$. Combining these, by (9), we have $\mu(2, k+2n) + \mu(n, k+2n) \equiv \mu(2n, k+2n) \equiv \mu(2n, k) + \frac{1}{2}n(k+1)$, which proves (11).

12. Similarly, we may derive (7) and (10) from (8), (9) and (11), assumed to be known. From (11), by repetition, $\mu(2, k+4) \equiv \mu(2, k) + 1 \pmod 2$;

also, $\mu(2, 3) = 1$, since $\mu(2, 1) = 0$. We thus obtain (15), and may now derive (10) from (11) by reversing the process of paragraph 11, for odd values of n; (10) being derived from (11), for even values of n, by repetition. After this, we may obtain (7) as in the preceding paragraph.

13. Let

$$(n/k) = (-1)^{\mu(n,k)}. \tag{16}$$

Under this definition the elementary relations numbered (1), (2), (6) and (5) are at once proved by the μ-theorems (7), (8), (9) and (12) respectively. Let the μ-theorem (10) be applied x times, with $k - 2n$ substituted for k; then, since $(-1)^{\frac{1}{2}n(n-1)} = (-1)^r$, whether $n = 2r$ or $n = 2r + 1$, we have the elementary relation numbered (3). If in the μ-theorem (11) we write k for k' and $k - 2n$ for k, we shall have the proof of the elementary relation numbered (4), since $\frac{1}{2}n(k - 2n + 1) \equiv \frac{1}{2}n(k - 1) \pmod 2$. Of these six elementary relations (1), (2), (6) and (5) are known, the latter being the law of reciprocity. It is to be noted that (1) and (4) may be derived from (2), (3) and (6), as has been shown of the corresponding μ-theorems in paragraph 11, or (1) and (3) from (2), (4) and (6), corresponding to paragraph 12. The proof of the law of reciprocity, (5), as a corollary of (4), if we know (1) and (2), has been given in paragraph 5, under the form

$$(k - 2n/k) = (-1)^{\frac{1}{2}(k-1)(n-1)}(k/k - 2n). \tag{17}$$

III. The new algorithm, and its derivation from the elementary relations.

14. When, in (n/k), either n or k is divisible by a square number, the quotient may be put in its place. For, since $(m/k) = \pm 1$, $(m/k)^2 = 1 = (m^2/k)$, by (6), so that

$$(m^2n/k) = (n/k). \tag{18}$$

Also, that

$$(n/h^2k) = (n/k) \tag{19}$$

when n is odd, follows from (18) by (5), since $h^2k \equiv k \pmod 8$; and for the same reason $(2/h^2k) = (2/k)$, by (15), and $(2/h^2k)(n/h^2k) = (2n/h^2k) = (2/k)(n/k) = (2n/k)$, showing that (19) holds when n is even.*

*Any relation regarding $(2n/k)$ holds good regarding $(2.4^rn/k)$, by (18). It might be stated that $(n/h)(n/k) = (n/hk)$, from which (19) follows; but this known theorem is not necessary to the algorithm. From the present point of view, it may be proved, for the case in which all the numbers are odd, by applying (5) to both sides of $(hk/n) = (h/n)(k/n)$, noting that $(-1)^{\frac{1}{2}(hk-1)} = (-1)^{\frac{1}{2}(h+k-2)}$, each side being $(-1)^{r+s}$ if $h = 2r + 1$ and $k = 2s + 1$; after which it may be shown similarly that $(2/h)(2/k) = (2/hk)$, producing $(2n/h)(2n/k) = (2n/hk)$. The relations (18) and (19) are known, but (19) cannot come into play when the law of reciprocity is employed in practice, and is therefore not well known.

15. Apart from the possibility of shortening the work by the throwing out of square factors when observed, the method now presented for the evaluation of the function (n/k), where k is odd and n any number prime to it, consists in reducing the larger of the two numbers n and k, by the help of certain rules, so as to make it the smaller, but still positive, always paying due attention to the sign of the function, then in reducing the other, and so on alternately until one or the other is reduced to 1, under the form $(1/k) = 1$ or $(n/1) = 1$. The sign of the result indicates the original value of (n/k) as $+1$ or -1. Under each rule of reduction the sign of the function is changed only in case some specified number happens to be oddly even, that is to say, to be of the form $4m + 2$, as, for example, 26.

16. *Rules of Reduction:*

	The sign of (n/k) is not changed when these numbers are reduced:	*Unless these numbers are oddly even:*
(20)	n to $n - xk$	[No exception]
(21)	n to $xk - n$	$k - 1$.
(22)	k to $k - 2xn$ or to $2xn - k$	n or $n - 1$ if x is odd
[n even and x odd, the following:]		
(23)	k to $k - xn$ or to $xn - k$	both n and $k - x$.

These rules may also be formulated as follows:

(20) $$(n/k) = (n - xk/k),$$

(21) $$(n/k) = (-1)^{\frac{1}{2}(k-1)}(xk - n/k),$$

(22) $$(n/k) = (-1)^{\frac{1}{2}xn(n-1)}(n/\pm k \mp 2xn),$$

(23) $$(n/k) = (-1)^{\frac{1}{4}n(k-x)}(n/\pm k \mp xn) \text{ [}n \text{ even, } x \text{ odd]}.$$

Of the four rules, the first two, those relating to n, are known.

17. *Illustrations of the use of the four rules:*

Of (20): $(82/11) = (82 - 7.11/11) = (5/11)$.

Of (21): $(62/13) = (5.13 - 62/13) = (3/13)$.

$(82/11) = -(8.11 - 82/11) = -(6/11)$.

Of (22): $(19/79) = (19/79 - 4.19) = (19/3)$.

$(10/79) = (10/8.10 - 79) = (10/1)$.

$(38/79) = -(38/79 - 2.38) = -(38/3)$.

$(42/79) = -(42/2.42 - 79) = -(42/3)$.

Of (23):

$$(2/15) = (2/15 - 7.2) = (2/1).$$

$$(6/43) = (6/43 - 7.6) = (6/1).$$

$$(10/51) = -(10/51 - 5.10) = -(10/1).$$

$$(10/47) = -(10/5.10 - 47) = -(10/3).$$

For reducing n by (20) or (21), we have to divide n by k, using (20) if the least residue in absolute value is positive, (21) if it is negative. Thus for (82/11) the least residue is 5, so that (20) should be used, while for (62/13) the least residue is -3, indicating the use of (21). To reduce k, we must divide by $2n$ if n is odd, employing (22), without regard to the sign of the residue; but if n is even, we must divide k by n to obtain the least residue, likewise regardless of its sign, using (22) if the quotient is even or (23) if it is odd. Thus, to reduce 79 in (19/79), we must employ (22) because 19 is odd; to reduce 79 in (38/79), where n is even, the quotient is 2, and (22) must be used; but to reduce 51 in (10/51), 10 being even, we must employ (23) because the quotient, 5, is odd.

18. The rules of reduction, numbered (20) to (23), come directly from the elementary relations numbered (2), (1), (3) and (4) respectively. The last case requires attention. By repetition, if n be written for $2n$, the exponent of -1 is $\frac{1}{4}n[k-1+k-1-n+\cdots+k-1-(x-1)n]$, which is $\frac{1}{4}nx(k-1) - \frac{1}{8}n^2x(x-1)$. If n is divisible by 4, this $\equiv 0 \pmod 2$, and may not untruthfully be represented, as in (23), by $\frac{1}{4}n(k-x)$. If n is oddly even, both $\frac{1}{2}n$ and x are odd, and either may be suppressed as a factor, modulo 2. The expression thus becomes $\frac{1}{4}n(k-1) - \frac{1}{4}n(x-1) \equiv \frac{1}{4}n(k-x)$ as before. The second parts of (22) and (23) follow from the first, respectively, by reason of the theorem

(24) $$(n/k) = (n/-k).$$

This follows, by (3), from

(25) $$(n/2n-k) = (-1)^{\frac{1}{2}n(n-1)}(n/k),$$

which is proved as in paragraph 4.

19. For convenience, a negative value for k has been admitted in (24), although the definition $(n/k) = (-1)^{\mu(n,\,k)}$ relates only to positive values of n and k, and it must therefore be observed that (1) is compatible with negative values of n, by a fair extension, and (3) with negative values of k. It is in no case necessary, and is always undesirable, when dealing with actual numbers, to permit the appearance of the negative sign within the parenthesis which forms the function-symbol.

20. In addition to the four rules of reduction, we are also at liberty to avail ourselves, should it appear advantageous, of the rule of transposition known as the law of reciprocity (5). This rule may be stated thus:

	The sign of (k/k') *is not changed when this transposition takes place:*	*Unless these numbers are oddly even:*
(26)	(k/k') to (k'/k)	both $k-1$ and $k'-1$.

This recourse is of no value, as a rule, except when n is not much smaller than k. As an illustration of the exceptional case, the reduction $(6929/6931) = (6931/6929) = (2/6929) = (2/1) = 1$ is better than the reduction $(6929/6931) = (6929/6927) = (2/6927) = (2/1) = 1$; but it is only a little better, and four rules are remembered, or referred to, more easily than five. Apart from the exceptional case mentioned, it is possible to find, or to invent, other instances in which the law of reciprocity might be used to advantage, as may happen when its employment results in the appearance of a large square. For example, in one of LEGENDRE's numerical illustrations we find $(421/1459) = (1459/421) = (196/421) = (14^2/421) = 1$.* The difficulty in any such case consists in recognizing the rare opportunity beforehand.

21. In the function (n/k), k may or may not be a prime number. When it happens to be prime, a well known lemma of Gauss teaches that both sides of the congruence $n^c \cdot c! \equiv (n/k) \cdot c! \pmod{k}$, where $k = 2c+1$ (a congruence arising from the continued product of the terms $n, 2n \cdots, cn$), may be divided by $c!$, whence in this case $n^c \equiv (n/k) \pmod{k}$, which is 1 or -1 according as n is or is not a quadratic residue of k; because the residues, known to be roots of $n^c \equiv 1$, and non-residues, roots of $n^c \equiv -1$, are equal in number, and if the congruence $n \equiv x^2 \pmod{k}$ is possible, $(n/k) \equiv (x^2/k) = 1$. To learn whether n is a quadratic residue of k, a given prime, which is an important problem in the theory of numbers, it thus becomes necessary to determine whether $n^c \pmod{k}$, which when k is prime has the same value as one of our functions (n/k), is 1 or -1; and we may use for this purpose the algorithm which lowers alternately the values of n and k in the function (n/k), without inquiring whether the lower values of k are or are not prime.

IV. COMPARISON OF THE NEW ALGORITHM WITH PREVIOUS METHODS.

22. When $n > k$, the new method of reduction is the same as the old in requiring the employment of the two rules, numbered (20) and (21), which have

* Even in this first example of the sort which has presented itself, the regular method is equally lucky, giving $(421/1459) = (421/225) = (421/15^2) = 1$.

for their object the reduction of n. When $n < k$, n being odd, the new method substitutes the rule (22), which reduces k, for the rule (26), or law of reciprocity, which effects a transformation without reduction, the latter, however, being still available whenever use can be found for it. The sign is changed, by (22), n being odd, when $n-1$ is oddly even, and by (26), when both $n-1$ and $k-1$ are oddly even. As an illustration, the reduction $(13/29) = (13/3)$ is simpler than $(13/29) = (29/13) = (3/13) = (13/3)$, since one operation takes the place of three. In fact, when n is odd, the application of the rule (22) is exactly equivalent analytically to the application of (26) after (20) [or (21)], after (26), x being even in (20) or (21). In the following illustration of the old process, wherein k consists of the first few digits of π and n of those of the common logarithm of 2, only odd values appear:

$$\begin{aligned}(30103/314159) &= -(314159/30103) = -(13129/30103) = -(30103/13129)\\ &= -(3845/13129) = -(13129/3845) = -(2251/3845)\\ &= -(3845/2251) = (657/2251) = (2251/657) = (377/657)\\ &= (657/377) = (97/377) = (377/97) = (11/97) = (97/11)\\ &= (9/11) = 1.\end{aligned}$$

By using the third rule wherever $n < k$, instead of the law of reciprocity, this is shortened to

$$\begin{aligned}(30103/314159) &= -(30103/13129) = -(3845/13129) = -(3845/2251)\\ &= (657/2251) = (657/377) = (97/377) = (97/11) = (9/11) = 1.\end{aligned}$$

At each point where $n < k$, one operation serves instead of three.*

* The new third rule (22) is most valuable when applied to even values of n. Confined to odd values it is

(22a) $$(k/k') = (-1)^{\frac{1}{2}x(k-1)}(k/ \pm [k' - 2xk]),$$

being equivalent to a combination of the three known operations,

$$(k/k') = (-1)^{\frac{1}{4}(k-1)(k'-1)}(k'/k);$$

$$(k'/k) = (k' - 2xk/k), \quad \text{or} \quad (k'/k) = (-1)^{\frac{1}{2}(k-1)}(2xk - k'/k);$$

and

$$(k' - 2xk/k) = (-1)^{\frac{1}{4}(k-1)(k'-2xk-1)}(k/k' - 2xk),$$

or

$$(2xk - k'/k) = (-1)^{\frac{1}{4}(k-1)(2xk-k'-1)}(k/2xk - k').$$

So simple a combination of these formulæ has probably not been looked for, yet that they might be consolidated in some way must have occurred to others, and may possibly have suggested the algorithms of EISENSTEIN and SYLVESTER. From another point of view, one branch of (22a), having + where (22a) has $\pm$, has, for prime values of k and k', been used as a step, implicitly by BOUNIAKOWSKY, and explicitly by BUSCHE, in their demonstrations (as given by BAUMGART) of the law of reciprocity.

23. The law of reciprocity cannot be applied when n is even, and under the customary system it is therefore necessary, with $n < k$, to make n odd by reducing (n/k) to $(\frac{1}{2}n/k)$ by means of a fourth well-known rule, namely:

	The sign of (n/k) is not changed when this number is reduced:	*Unless one of these numbers is oddly even:*
(27)	n to $\frac{1}{2}n$	$\frac{1}{2}(k-1)$ or $\frac{1}{2}(k+1)$

Expressed as a formula, this fourth customary rule is

$$(n/k) = (2/k)(\tfrac{1}{2}n/k) = (-1)^{\frac{1}{8}(k^2-1)}(\tfrac{1}{2}n/k).$$

It is of course still available, like the old third rule, or law of reciprocity, in connection with the algorithm herein presented, if any unexpected use for it happens to appear, as for instance when $\frac{1}{2}n$ is a square, as in $n = 98$; but such cases must be rare. In lieu of it we have the fourth rule (23) of paragraph 16 if x is odd, otherwise the third rule (22). For example, by the customary method,

$$(10/103) = (2/103)(5/103) = (5/103) = (103/5) = (2/5) = -1;$$

but by the third rule, $(10/103) = -(10/3) = -(1/3) = -1$. Again,

$$(14/93) = (2/93)(7/93) = -(7/93) = -(93/7) = -(2/7) = -1;$$

but by the new fourth rule, $(14/93) = -(14/5) = -(1/5) = -1$. The object to be attained is the reduction of the larger number, k. By the new method, the object is effected instantly, leaving n the larger, ready for the next reduction. By the old method, n must be halved, by the rule here numbered (27); the law of reciprocity (26) must next be applied, producing $(k/\frac{1}{2}n)$; then k is reduced by (20) or (21); and finally the law of reciprocity must be applied again before the next reduction can be effected.

24. Having compared separately the steps to be taken when n is odd and when n is even, let us take a more extended example illustrating the use of all the rules [A] of the method heretofore in use and [B] of the method now set forth:

$$\begin{aligned}[A]\quad (1294/2477) &= (2/2477)(647/2477) = -(647/2477)\\ &= -(2477/647) = (111/647) = -(647/111) = (19/111)\\ &= -(111/19) = (3/19) = -(19/3) = -(1/3) = -1.\end{aligned}$$

[B] $(1294/2477) = -(1294/111) = (38/111) = (38/3) = -(1/3) = -1.$

Another case is that taken for illustration by TANNERY, (3988/887), which according to custom should run thus:*

$$(3988/887) = (440/887) = (4.110/887) = (110/887) = (2/887)(55/887)$$

$$= (55/887) = -(887/55) = -(7/55) = (55/7) = -(1/7) = -1.$$

Having now the means of depressing k directly, we can write

$$(3988/887) = (440/887) = (440/7) = -(1/7) = -1.$$

The old system depresses only n, while the new depresses n and k alternately, going, so to speak, on two legs instead of one, and so dispensing with the crutch known as the law of reciprocity.

25. Various substitutes have been proposed, without much success, for the method customarily employed for the evaluation of (n/k). BAUMGART describes such systems devised respectively by GAUSS, SYLVESTER, EISENSTEIN, LEBESGUE, GEGENBAUER and KRONECKER. Of these the simplest and best would seem decidedly to be that of EISENSTEIN, which has been chosen for reproduction in BACHMANN's recent text-book on the theory of numbers,† and which, indeed, by reason of its effective development and demonstration, based upon the law of reciprocity, is deserving of special remark. The practical working of EISENSTEIN's algorithm will alone be considered here.

26. EISENSTEIN's method provides for a succession of divisions with even quotients, so as to produce in each case the least possible positive or negative remainder. It may best be explained by numerical illustration. For present convenience, the successive divisions will be arranged in pairs, each pair occupying one line. The example taken is that chosen by BAUMGART, improved by an obvious correction and by observation of the detailed rules given by BACHMANN. When, as in this case, $n < k$, the first division is taken with the quotient 0. The evaluation of (2933/3785) proceeds by the following steps:

---

* The evaluation given by TANNERY is erroneous.

† BACHMANN, in fact, does not illustrate, or even explain, the algorithm which I have described as customary, but replies to his own statement of the problem, "ist eine gegebene ungerade Primzahl q von einer andern ungeraden Primzahl p quadratischen Rest oder Nichtrest?" by "können wir dafür eine sehr einfache Regel angeben, welche EISENSTEIN aufgestellt hat."

	Divd.		Qt.	Divr.		Rem.
	2933	=	0 ·	3785	+	2933
	2933	=	2 ·	2081	−	1229
	1229	=	4 ·	377	−	279
	279	=	2 ·	181	−	83
×	83	=	6 ·	15	−	7

	Divd.		Qt.	Divr.		Rem.
	3785	=	2 ·	2933	−	2081
	2081	=	2 ·	1229	−	377
×	377	=	2 ·	279	−	181
×	181	=	2 ·	83	+	15
×	15	=	2 ·	7	+	1

Having continued the process till 1 is reached, we proceed to mark those cases in which the divisor is of the form $4r + 3$, namely, 279, 83, 15, and 7. As regards these marked cases, *for a first process*, count the number of remainders of the form $4r + 3$ and of the form $-(4r + 1)$. There are two, namely, -181 and 15. *For a second process*, count among the marked cases on the left side the number of negative remainders (namely, -7), and on the right side the number of remainders for which the quotient is not divisible by 4 (namely, -181, 15, and 1). By either process of counting the number is even, and this means that $(2933/3785) = 1$. The two processes are equally simple, or perhaps the second is less troublesome than the first, particularly in a long calculation.

27. What I have called the first process is that of EISENSTEIN. The second process, introduced merely for comparison, will be recognized as the present algorithm limited to odd values of n. The first, third, . . ., operations, those on the left side, are, for positive remainders, performed by the first rule (20) of paragraph 16, and for negative remainders by the second rule (21); while the alternate operations, those on the right side, are performed by the third rule (22). By the new algorithm, untrammeled, we should write $(2933/3785) = (2933/2081) = (852/2081) = (213/2081) = (213/49) = 1$.

28. A vital defect of EISENSTEIN's algorithm remains to be pointed out, apparently for the first time. It is a general system, yet there are cases to which its application is insufferably tedious. Take (293/287). By the old algorithm this is solved at once thus, $(293/287) = (6/287) = (2/287)(3/287) = (3/287) = -(287/3) = (1/3) = 1$; and by the new thus, $(293/287) = (6/287) = (6/1) = 1$. But by the system of EISENSTEIN, accepted by one writer at least as an improvement on earlier methods, we should have

$$293 = 2.287 - 281 \qquad 287 = 2.281 - 275$$

$$281 = 2.275 - 269 \qquad 275 = 2.269 - 263$$

$$269 = 2.263 - 257 \qquad 263 = 2.257 - 251$$

and so on, requiring 42 more operations, with the subsequent counting of the cases in which the divisor is of the form $4r + 3$ and the remainder of the same form or of the form $-(4r + 1)$. The smaller the difference between n and k, other things being equal, the greater is the difficulty. Take $(293/97)$:

$$293 = 4.97 - 95 \qquad 97 = 2.95 - 93$$

$$95 = 2.93 - 91 \qquad 93 = 2.91 - 89$$

and so on, through 44 more operations, besides the subsequent counting. By either the old or the present method, this would be: $(293/97) = (2/97) = (2/1) = 1$.

MORRISTOWN, NEW JERSEY.