THE QUADRATIC LAW OF RECIPROCITY AND THE THEORY OF GALOIS FIELDS

by HANS J. ZASSENHAUS

(Received 18th November, 1950)

The theory of quadratic congruences modulo an integer is dominated by the *Quadratic Law of Reciprocity* (see § 1), which makes it possible to decide in a very short time whether a quadratic congruence

$$x^2 \equiv a(m)$$

is solvable or not. The law was first proved by Gauss.* It took him over a year to obtain his first proof, which depends on a tedious lemma in elementary number theory. He subsequently obtained seven further proofs, and today more than fifty proofs are known, most of them based on the ideas of Gauss. The object of the present paper is to present a proof which is a modernised version of Gauss's seventh proof, applying the ideas of that proof to a *finite* set of objects, the elements of a finite or Galois field.

The first section of this paper gives a group-theoretic treatment of the elementary properties of Legendre's symbol. In the second section we introduce Gaussian sums in finite fields. A comparison of two different expressions for these yields the quadratic law of reciprocities.

We conclude this introduction by giving a summary of the properties of Galois fields required in the course of the proof of the quadratic law of reciprocity.

1. The multiplicative group of a Galois field of N elements is a cyclical group of order $N-1$.

2. A Galois field has for its characteristic a prime number p, and therefore for its prime field a field isomorphic with F_p. the field of residue classes of the integers modulo p. We shall denote any field isomorphic with this field by F_p. The number of elements in any Galois field of characteristic p is of the form p^r where r is a positive integer. Conversely, corresponding to any prime number p and any positive integer r, there is a Galois field of characteristic p and with p^r elements. This Galois field, which is denoted by $GF(p^r)$, is uniquely determined up to isomorphism as a minimal splitting field of the polynomial $t^{p^r}-t$ over the field F_p.

3. The prime field F_p of $GF(p^r)$ consists of the set of p elements of $GF(p^r)$ which satisfy the equation

$$x^p = x.$$

4. The correspondence σ defined by

$$x \rightarrow x^p = x^\sigma, \quad x \in GF(p^r),$$

is an automorphism of $GF(p^r)$.

The proofs of these properties of Galois fields will be found in books on Modern Algebra or in the introduction to another paper in this number of these proceedings. (A Group-theoretic Proof of a Theorem of Maclagan-Wedderburn, pp. 53–63).

§ 1. *The Legendre Symbol.*

The Legendre symbol arises in connection with the problem of solving a quadratic congruence

$$ax^2 + bx + c \equiv 0\ (m),$$

* Gauss, *Disquisitiones Arithmeticae.* Proof 1 : Vol. I, p. 135 ; proof 7 : Vol. II, p. 234.

i.e., of finding an integer x which satisfies this relation. It can be shown that this problem can be reduced to that of solving a quadratic congruence of the form

$$x^2 \equiv d\ (p), \qquad \text{(1)}$$

where p is an odd prime.

It is much more important to establish a means of determining whether (1) has a solution than to find its set of solutions if it has any. To deal with the former problem, Legendre introduced a symbol $\left(\frac{d}{p}\right)$, defined in the following way:

$$\left(\frac{d}{p}\right)=1 \text{ if } d \not\equiv 0\ (p), \text{ but (1) has a solution;}$$

$$\left(\frac{d}{p}\right)=-1 \text{ if (1) has no solution;}$$

$$\left(\frac{d}{p}\right)=0 \text{ if } d\equiv 0\ (p).$$

This Legendre symbol is defined for every integer d in the numerator and for every prime greater than 2 in the denominator. Its value, for a given d and p, is either 1, -1 or 0. Obviously, from (1), its value is unaltered when d is replaced by any integer congruent to d modulo p. Thus its value depends only on the residue class R_d of integers modulo p to which d belongs. Thus we can define uniquely, by

$$\left(\frac{R_d}{d}\right)=\left(\frac{d}{p}\right),$$

the Legendre symbol of each element of F_p, the field of residue classes of the integers modulo p. Further, if we observe that, if any integer x satisfies (1), so do all the integers congruent to x modulo p, we see that the problem of solving the congruence (1) in the domain of all integers is equivalent to that of solving the equation

$$x^2=\alpha, \qquad \text{(2)}$$

where α is an element of F_p, in the field F_p. In consequence of this, the definition of the Legendre symbol $\left(\frac{\alpha}{p}\right)$, where α is an element of F_p, can be restated thus:

$\left(\frac{\alpha}{p}\right)=1$ if α is not 0, the zero element of F_p, and is the square of an element of F_p;

$\left(\frac{\alpha}{p}\right)=-1$ if α is not the square of any element of F_p;

$\left(\frac{0}{p}\right)=0.$

Since p is an odd prime, the elements 1, -1 and 0 of F_p are distinct, so the values of the Legendre symbol, hitherto considered as the integers 1, -1 and 0, may equally well be considered as the elements 1, -1 and 0 of F_p. This interpretation is frequently more convenient, for it often allows congruences to be replaced by equations. This is the case in the following important theorem of Euler.

$$\left(\frac{\alpha}{p}\right)=\alpha^{\frac{1}{2}(p-1)}. \qquad \text{(3)}$$

Proof: If $\alpha=0$, both sides of (3) are zero, and therefore (3) is true.

To deal with the case in which $\alpha\neq 0$, consider the correspondence

$$\xi \rightarrow \xi^2,$$

https://doi.org/10.1017/S2040618500035486 Published online by Cambridge University Press

where ξ is a non-zero element of F_p. This correspondence is an *operator* of the multiplicative group of F_p, *i.e.*, it is a homomorphism of this group onto a subgroup ; for $(\xi\eta)^2 = \xi^2\eta^2$. The kernel of this homomorphism is the set of elements of F_p for which $\xi^2 = 1$, *i.e.*, since F_p is a field, it is the two elements $+1$ and -1 of F_p. By the fundamental theorem on homomorphisms, it follows that the image of F_p under the homomorphism, *i.e.*, the set of elements of F_p which are non-zero and the squares of elements of F_p, forms a multiplicative group S_p isomorphic with the factor group of the multiplicative group of F_p over the normal divisor consisting of the pair of elements ± 1. The order of S_p is therefore half that of the multiplicative group of F_p, *i.e.*,

$$S_p : 1 = \tfrac{1}{2}(p-1).$$

Now, for each non-zero element of F_p, we have, by Fermat's theorem,

$$\xi^{p-1} = 1,$$

i.e.,

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

Hence (3) is true for all elements of S_p. Further, since the equation $\xi^{\frac{1}{2}(p-1)} = 1$ cannot be satisfied by more than $\frac{1}{2}(p-1)$ elements of F, it follows that, if $\left(\frac{\xi}{p}\right) = -1$, then $\xi^{\frac{1}{2}(p-1)} \neq 1$. But, if $\xi \neq 0$, $\{\xi^{\frac{1}{2}(p-1)}\}^2 = 1$ and therefore $\xi^{\frac{1}{2}(p-1)} = \pm 1$. Hence,

if
$$\left(\frac{\xi}{p}\right) = -1, \text{ then } \xi^{\frac{1}{2}(p-1)} = -1.$$

The formula (3) is thus established for all elements α of F_p.

From (3) it follows that

$$\left(\frac{\alpha\beta}{p}\right) = \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right), \qquad \text{...(4)}$$

i.e., that, in F_p,

$$0 \,.\, \alpha = \alpha \,.\, 0 = 0,$$

where 0 is the zero element of F_p ; while, for non-vanishing products,

$$\text{square} \times \text{square} = \text{square},$$

$$\text{square} \times \text{non-square} = \text{non-square} \times \text{square} = \text{non-square},$$

$$\text{non-square} \times \text{non-square} = \text{square}.$$

It follows also that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}, \qquad \text{...(5)}$$

i.e., that

$$\left(\frac{-1}{p}\right) = 1 \text{ if } p \equiv 1 \ (4),$$

$$\left(\frac{-1}{p}\right) = -1 \text{ if } p \equiv 3 \ (4).$$

The quadratic law of reciprocity and its complements I and II state the following properties of the Legendre symbols.

If p and q are different odd primes, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ if either } p \equiv 1 \ (4) \text{ or } q \equiv 1 \ (4),$$

and

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \text{ if } p \equiv q \equiv 3 \ (4).$$

Complement I: $\left(\frac{-1}{q}\right)=1$ if $q\equiv 1$ (4),

$$\left(\frac{-1}{q}\right)=-1 \text{ if } q\equiv 3 \ (4).$$

Complement II: $\left(\frac{2}{q}\right)=1$ if $q\equiv \pm 1$ (8),

$$\left(\frac{2}{q}\right)=-1 \text{ if } q\equiv \pm 3 \ (8).$$

These statements may be collected into the following more compact forms:
The Quadratic Law of Reciprocity:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}. \qquad (6)$$

Complement I:

$$\left(\frac{-1}{q}\right)=(-1)^{\frac{1}{2}(q-1)}. \qquad (7)$$

Complement II:

$$\left(\frac{2}{q}\right)=(-1)^{\frac{1}{8}(q^2-1)}. \qquad (8)$$

The relation (6) is obviously equivalent to the Quadratic Law of Reciprocity itself, the relation (7) is the same as (5) and has therefore been proved already. To prove the relation (8) we express q in the form $8l+(2k+1)$, where k and l are integers, and observe that

$$\begin{aligned}\tfrac{1}{8}(q^2-1)&=8l^2+2l(2k+1)+\tfrac{1}{2}k(k+1)\\ &\equiv \tfrac{1}{2}k(k+1) \pmod 2\\ &\equiv \tfrac{1}{8}\{(2k+1)^2-1\} \pmod 2.\end{aligned}$$

Thus the value of $(-1)^{\frac{1}{8}(q^2-1)}$ depends only on the residue class of q modulo 8, and the value is 1 if $q\equiv\pm 1$ (8) and -1 if $q\equiv\pm 3$ (8).

If we introduce the symbol

$$\epsilon=(-1)^{\frac{1}{2}(q-1)}=\left(\frac{-1}{q}\right),$$

we may write (6) in the form

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

and hence, after multiplication on both sides by $\left(\frac{q}{p}\right)$, in the form

$$\left(\frac{p}{q}\right)=\left(\frac{\epsilon q}{p}\right).$$

§ 2. *Proof of the Quadratic Law of Reciprocity and its Second Complement.*

Let p and q be two different positive prime numbers. Let f be the order of p modulo q, *i.e.*, let f be the positive integer for which q is a factor of p^f-1 but is not a factor of $p^\nu-1$, where $0<\nu<f$. Then the multiplicative group of the Galois field $GF(p^f)$, being cyclical of order p^f-1, contains an element ζ of order q and therefore such that

$$\zeta^q=1 \quad\text{but}\quad \zeta\neq 1.$$

Since

$$\zeta^q-1=(\zeta-1)(\zeta^{q-1}+\zeta^{q-2}+\ldots+1)$$

and $\zeta\neq 1$, it follows that

$$\sum_{i=0}^{q-1}\zeta^i=0. \qquad (1)$$

https://doi.org/10.1017/S2040618500035486 Published online by Cambridge University Press

Since, if a and b are two integers, $\zeta^a = \zeta^b$ if and only if $a \equiv b\ (q)$, it is possible to define ζ^α, where α is any residue class of the integers modulo q, thus :

$$\zeta^\alpha = \zeta^a,$$

where a is any integer in the residue class α. As a result of this definition,

$$\zeta^\alpha \zeta^\beta = \zeta^{\alpha+\beta},$$

where α and β are any residue classes of the integers modulo q, *i.e.*, any elements of F_q.

We now define, for each prime number p and each element α of F_q, the *Gaussian sum* $G(\alpha, p)$, thus :

$$G(\alpha, p) = \Sigma \zeta^{\alpha\xi}, \qquad \text{(2)}$$

where summation is over all elements ξ of F_q for which $\left(\frac{\xi}{q}\right) = 1$. The Gaussian sum is an element of $GF(p^f)$. If $\alpha = 0$, the zero element of F_q, each of the $\frac{1}{2}(q-1)$ terms on the right side of (2) is equal to 1, the unity element of $GF(p^f)$ and therefore $G(0, p)$ is equal to $\frac{1}{2}(q-1)$ times the unity element of $GF(p^f)$. If α is not the zero element of F_q, $G(\alpha, p)$ is equal to $\Sigma\zeta^\beta$, summation being over all elements β of F_q which have the same Legendre symbol as α. It follows that the Gaussian sum depends only on p, q and the Legendre symbol $\left(\frac{\alpha}{q}\right)$ of α. Suppressing p, we may therefore introduce the notation

$$G_{\left(\frac{\alpha}{q}\right)} = G(\alpha, p).$$

We note that the suffix $\left(\frac{\alpha}{q}\right)$ can only take the values 1, -1 and 0. We now find the values of G_1, G_{-1} and G_0.

As we have just shown, G_0, *i.e.*, $G(0, p)$, is equal to $\frac{1}{2}(q-1)$ times the unity element of $GF(p^f)$ and therefore of its subfield F_p. Hence

$$G_0 = \tfrac{1}{2}(q-1) \text{ times the unity element of } F_p.$$

To evaluate G_1 and G_{-1}, we note that

$$\begin{aligned} G_1 + G_{-1} &= \sum_{\left(\frac{\alpha}{q}\right)=1} \zeta^\alpha + \sum_{\left(\frac{\beta}{q}\right)=-1} \zeta^\beta \\ &= \sum_{0 \neq \gamma \in F_q} \zeta^\gamma = -1, \end{aligned} \qquad \text{(3)}$$

by (1), where 1 is the unity of $GF(p^f)$, *i.e.*, of its subfield F_p ; and that

$$\begin{aligned} G_1\, G_{-1} &= \sum_{\left(\frac{\alpha}{q}\right)=1} \zeta^\alpha \sum_{\left(\frac{\beta}{q}\right)=-1} \zeta^\beta \\ &= \sum_{\left(\frac{\alpha}{q}\right)=-\left(\frac{\beta}{q}\right)=1} \zeta^{\alpha+\beta} = \sum_{\gamma \in F_q} n_\gamma \zeta^\gamma, \end{aligned} \qquad \text{(4)}$$

where, for each γ in F_q, n_γ is the number of solutions (α, β) of the equation

$$\gamma = \alpha + \beta, \text{ with } \left(\frac{\alpha}{q}\right) = -\left(\frac{\beta}{q}\right) = 1. \qquad \text{(5)}$$

Now if ξ is any element of F_q with $\left(\frac{\xi}{q}\right) = 1$, there is a one-one correspondence between the solutions of (5) and the solutions $\alpha' = \alpha\xi$, $\beta' = \beta\xi$ of the equations

$$\gamma\xi = \alpha' + \beta', \text{ with } \left(\frac{\alpha'}{q}\right) = -\left(\frac{\beta'}{q}\right) = 1. \qquad \text{(6)}$$

There is also, for each δ for which $\left(\frac{\delta}{q}\right) = -\left(\frac{\gamma}{q}\right)$, a one-one correspondence between the solutions of (5) and the solutions $\alpha'' = \beta\gamma^{-1}\delta$, $\beta'' = \alpha\gamma^{-1}\delta$ of the equation

$$\delta = \alpha'' + \beta'', \text{ with } \left(\frac{\alpha''}{q}\right) = -\left(\frac{\beta''}{q}\right) = 1. \quad \text{......(7)}$$

Since, by suitable choices of ξ and δ, $\gamma\xi$ and δ can be made to be any elements of F_q with Legendre symbols 1 and -1 respectively, it follows that n_γ has the same value for all non-zero elements γ of F_q; let this value be n.

If $n_0 > 0$, then the equation

$$0 = \alpha + \beta, \text{ with } \left(\frac{\alpha}{q}\right) = -\left(\frac{\beta}{q}\right) = -1, \quad \text{......(8)}$$

has at least one solution. For any such solutions $\beta = -\alpha$, *i.e.*, $-1 = \beta\alpha^{-1}$, and therefore

$$\left(\frac{-1}{q}\right) = \left(\frac{\beta}{q}\right)\left(\frac{\alpha^{-1}}{q}\right) = \left(\frac{\beta}{q}\right)\left(\frac{\alpha}{q}\right)^{-1} = -1.$$

Conversely, if $\left(\frac{-1}{q}\right) = -1$ and α is any element of F_q, and if $\beta = -\alpha$, then $\left(\frac{\beta}{q}\right) = -1$; there is thus one solution of (8) for every α for which $\left(\frac{\alpha}{q}\right) = 1$. Hence

$$n_0 = \begin{cases} 0 & \text{if } \left(\frac{-1}{q}\right) = 1, \\ \frac{1}{2}(q-1) & \text{if } \left(\frac{-1}{q}\right) = -1; \end{cases}$$

or, using the symbol

$$\epsilon = \left(\frac{-1}{q}\right) = (-1)^{\frac{1}{2}(q-1)},$$

introduced earlier,

$$n_0 = \tfrac{1}{2}(1-\epsilon) \,.\, \tfrac{1}{2}(q-1). \quad \text{......(9)}$$

Since, in the sum

$$\sum_{\left(\frac{\alpha}{q}\right) = -\left(\frac{\beta}{q}\right) = 1} \zeta^{\alpha+\beta}$$

the total number of terms is $\{\frac{1}{2}(q-1)\}^2$, we have, from (4),

$$n_0 + (q-1)n = \{\tfrac{1}{2}(q-1)\}^2;$$

hence, using (9), we have

$$n = \tfrac{1}{4}(q + \epsilon - 2).$$

But, by (4),

$$\begin{aligned} G_1 G_{-1} &= n_0\zeta^0 + n \sum_{0 \neq \gamma \epsilon F_q} \zeta^\gamma \\ &= (n_0 - n) \text{ times the unity element of the } F_p \text{ in } GF(p^f). \end{aligned}$$

Hence,

$$G_1 G_{-1} = \tfrac{1}{4}(1 - \epsilon q) \text{ times the unity of the } F_p \text{ in } GF(p^f). \quad \text{......(10)}$$

From (3) and (10) it follows that G_1 and G_{-1} are the elements of $GF(p^f)$ which satisfy the quadratic equation

$$x^2 + x + \tfrac{1}{4}(1 - \epsilon q) = 0, \quad \text{......(11)}$$

where it is to be understood that $\frac{1}{4}(1-\epsilon q)$ means this integer multiplied by the unity element of the F_p in $GF(p^f)$.

If $p>2$, the usual method can be used to solve the quadratic equation, giving

$$(x+\tfrac{1}{2})^2=\tfrac{1}{4}\epsilon q.$$

Hence if a suitable solution in $GF(p^f)$ of $y^2=\epsilon q$ is denoted by $\sqrt{\epsilon q}$, we have

$$G_\delta=-\tfrac{1}{2}+\tfrac{1}{2}\delta\sqrt{\epsilon q}, \qquad (12)$$

for $\delta=+1$ and -1.

Now, whether $p>2$ or not, the correspondence

$$\eta\to\eta^p, \quad \eta\epsilon GF(p^f),$$

is an automorphism of $GF(p^f)$. Applying this automorphism to $G(\alpha, p)$, we have

$$\{G(\alpha, p)\}^p=\Bigl(\sum_{\left(\frac{\xi}{q}\right)=1}\zeta^{\alpha\xi}\Bigr)^p=\sum_{\left(\frac{\xi}{q}\right)=1}\zeta^{\alpha\xi p}=G(\alpha p, p)$$

and therefore, using the other notation for the Gaussian sum and putting $\left(\frac{\alpha}{q}\right)=\delta$, where $\delta=\pm 1$, we have

$$(G_\delta)^p=G_{\left(\frac{p}{q}\right)\delta}, \qquad (13)$$

since $\left(\frac{\alpha p}{q}\right)=\left(\frac{\alpha}{q}\right)\left(\frac{p}{q}\right)=\delta\left(\frac{p}{q}\right)$.

In the case in which $p>2$,

$$(G_\delta)^p=(-\tfrac{1}{2}+\tfrac{1}{2}\delta\sqrt{\epsilon q})^p=(-\tfrac{1}{2})^p+(\tfrac{1}{2}\delta)^p(\sqrt{\epsilon q})^p=-\tfrac{1}{2}+\tfrac{1}{2}\delta(\sqrt{\epsilon q})^p,$$

since $-\tfrac{1}{2}$ and $\tfrac{1}{2}\delta$ lie in the subfield F_p of $GF(p^f)$; and

$$G_{\left(\frac{p}{q}\right)\delta}=-\frac{1}{2}+\frac{1}{2}\left(\frac{p}{q}\right)\delta\sqrt{\epsilon q}.$$

It follows from (13) that

$$(\sqrt{\epsilon q})^p=\left(\frac{p}{q}\right)\delta\sqrt{\epsilon q}.$$

Thus, if $\left(\frac{p}{q}\right)=1$,

$$(\sqrt{\epsilon q})^p=\sqrt{\epsilon q}\,;$$

hence $\sqrt{\epsilon q}$ is in F_p and therefore $\left(\frac{\epsilon q}{p}\right)=1$. In this case, therefore, $\left(\frac{p}{q}\right)=\left(\frac{\epsilon q}{p}\right)$.

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

$$(\sqrt{\epsilon q})^p=-\sqrt{\epsilon q}\,;$$

hence $\sqrt{\epsilon q}$ is not in F_p and therefore $\left(\frac{\epsilon q}{p}\right)=-1$. Thus, in this case also $\left(\frac{p}{q}\right)=\left(\frac{\epsilon q}{p}\right)$.

This completes the proof of the quadratic law of reciprocity itself.

There remains to be completed the proof of the second complement, dealing with the case in which $p=2$. In that case (13) reads

$$(G_\delta)^2=G_{\left(\frac{2}{q}\right)\delta},$$

i.e.,

$$(G_\delta)^2=\begin{cases} G_\delta & \text{if } \left(\frac{2}{q}\right)=1,\\ G_{-\delta} & \text{if } \left(\frac{2}{q}\right)=-1.\end{cases} \qquad (14)$$

https://doi.org/10.1017/S2040618500035486 Published online by Cambridge University Press

We note that if x is either element of the subfield F_2 of $GF(2^f)$, then $x^2+x=0$, and that therefore no other element of $GF(2^f)$ satisfies this equation. This has the following consequences.

If $\frac{1}{4}(1-\epsilon q)\equiv 0\ (2)$, then both elements of F_2 are roots of (11) and no other elements of $GF(2^f)$ are. Hence, for each δ, $G_\delta \epsilon F_2$ and therefore $G_\delta{}^2=G_\delta$. Thus, by (14), $\left(\frac{2}{q}\right)=1$.

If $\frac{1}{4}(1-\epsilon q)\equiv 1\ (2)$, then neither element of F_2 is a root of (11), and therefore neither of the roots G_δ of (11) lies in F_2. Hence, for these roots G_δ, $G_\delta{}^2\neq G_\delta$ (for the two elements of F_2 and therefore no other elements of $GF(2^f)$ satisfy the equation $x^2=x$). Hence $G_\delta{}^2=G_{-\delta}$ and therefore, by (14), $\left(\frac{2}{q}\right)=-1$.

Now if $\frac{1}{4}(1-\epsilon q)\equiv 0\ (2)$, $1-\epsilon q\equiv 0\ (8)$, *i.e.*, $\epsilon q\equiv 1\ (8)$ and therefore $q\equiv \pm 1\ (8)$; while if $\frac{1}{4}(1-\epsilon q)\equiv 1\ (2)$, $1-\epsilon q\equiv 4\ (8)$, *i.e.*, $\epsilon q\equiv -3\ (8)$ and therefore $q\equiv \pm 3\ (8)$. Hence, if

$$q\equiv \pm 1\ (8),\ \left(\frac{2}{q}\right)=1\ ;\ \text{if } q\equiv \pm 3\ (8),\ \left(\frac{2}{q}\right)=-1.$$

This completes the proof of the second complement.

McGill University,
Montreal, Canada.

https://doi.org/10.1017/S2040618500035486 Published online by Cambridge University Press