CONGRUENCE REPRESENTATIONS IN ALGEBRAIC NUMBER FIELDS(1)

BY

ECKFORD COHEN

1. **Introduction.** In a recent paper [6] the author discussed arithmetic functions defined on residue class rings in the rational field. The basic ideas of that paper were later extended to the case of algebraic fields [7]. Arithmetic functions in the algebraic case were defined as follows:

Let F be a finite extension of the rational field and let A be an arbitrary integral ideal ($A \neq 0$) of F. If K is an arbitrary fixed field of characteristic zero containing all the roots of unity, then we say that a single-valued function f is (A, K) arithmetic if, for all integers $\beta \in F$, $f(\beta) \in K$ and $f(\beta) = f(\beta')$ when $\beta \equiv \beta' \pmod{A}$.

Denoting the ideal different of F by $\mathfrak{d}$, we choose an integral ideal B such that $(B, A) = 1$ and $\zeta = B/A\mathfrak{d}$ is principal. (This may be accomplished by choosing B to be any ideal prime to A lying in the same ideal class as $A\mathfrak{d}$.) Then we define a function $\epsilon_\nu(\beta)$ for integral values of the argument β by

$$\epsilon_\nu(\beta) = e^{2\pi i \operatorname{tr}(\beta\nu\zeta)}, \tag{1.1}$$

where ν is an arbitrary integer of F and tr represents the trace in F. If we denote the norm of A by $N(A) = N$, and the ring of residue classes (mod A) by $R(A)$, we see that there exist $N(A)$ functions $\epsilon_\nu(\beta)$ corresponding to the elements ν of $R(A)$. These are the exponential functions of Hecke [14, p. 220], which furnish the simplest examples of (A, K) arithmetic functions. These functions possess the basic dual properties,

$$\epsilon_\nu(\beta + \beta') = \epsilon_\nu(\beta)\epsilon_\nu(\beta'), \qquad \epsilon_{\nu+\nu'}(\beta) = \epsilon_\nu(\beta)\epsilon_{\nu'}(\beta). \tag{1.2}$$

By taking K to be the complex field C, we may then conceive of the ϵ_ν as a complete set of additive characters of $R(A)$.

Two arithmetic functions f, g admit of composition under the Cauchy product [2; 6], defined by $f \cdot g = h$,

$$h(\rho) = \sum_{\rho \equiv \xi + \eta \pmod{A}} f(\xi)g(\eta), \tag{1.3}$$

where ρ is an algebraic integer and the summation is over integers ξ, η distinct (mod A) such that $\rho \equiv \xi + \eta \pmod{A}$. It is clear how (1.3) may be extended to give Cauchy products of an arbitrary number of functions.

In [7] the foundations of a theory of arithmetic functions and their

Presented to the Society, April 26, 1952; received by the editors July 17, 1952.

(1) This research was completed under contract with the Office of Air Research.

Cauchy products were sketched. It was shown that the set of all (A, K) arithmetic functions forms a commutative semisimple algebra. A principle relating to the number of solutions of equations in the ring $R(A)$ was also proved (see Theorem 3). It is the twofold purpose of this paper to illustrate the algebraic viewpoint with a discussion of certain subalgebras of arithmetic functions, and to apply the additive principle noted above to certain congruence problems arising in algebraic fields.

One of the simplest and most useful arithmetic functions is the Rademacher sum [20, §2.2] which generalizes the familiar Ramanujan sum. This function forms the basis for the discussion in §3 illustrating the algebraic properties of arithmetic functions. The results of this section generalize results for the rational case proved in [6, §3]. We note in particular an extension to algebraic fields of Carmichael's orthogonality relation for Ramanujan sums [3, §1].

In §5 the important Hecke sum [14, (166)], generalizing the ordinary Gauss sum, is discussed in the case of a prime power ideal. A related exponential sum denoted by T is also introduced and evaluated in §5.

With the exception of §2 the remainder of the paper has to do with applications of the above mentioned sums to congruence problems in algebraic number fields. The purpose of §4 is to determine the number of representations of an algebraic integer as a sum of products in the multiplicative group of the ring $R(A)$. More precisely, we find the number of solutions x_{ij}, prime to A, of the congruence

$$\rho \equiv \alpha_1 x_{11} \cdots x_{l1} + \cdots + \alpha_s x_{1s} \cdots x_{ls} \pmod{A}, \tag{1.4}$$

where ρ is an arbitrary algebraic integer and the α_i are integers, of which at least one is prime to A. The result for this problem is quite simple and follows naturally as an application of the Rademacher sum alone. This problem is a threefold generalization of one considered in [6, §5].

§§6, 7, and 8 are devoted to the question of quadratic congruences, in particular to the problem of finding the number of solutions ξ_i of

$$\rho \equiv \alpha_1 \xi_1^2 + \cdots + \alpha_s \xi_s^2 \pmod{A} \tag{1.5}$$

where A is an arbitrary *odd* ideal, ρ is an arbitrary integer of F, and $\alpha_1, \cdots, \alpha_s$ are integers of F prime to A. On the basis of the additive principle in Theorem 3, formulas involving the Hecke, Rademacher, and T sums are shown to yield the number of solutions of (1.5). The case of s even leads to a formula involving only the Rademacher function (6.12), while the corresponding formula in the odd case involves all three (7.18). The formulas in both cases are evaluated completely, the final result in the even case (6.6) being slightly simpler than that of the odd (7.10). Finally in §8 special cases of (1.5) are considered; for example, Corollary 6 gives the number of solutions of (1.5)

in case A is prime, a problem equivalent to one solved earlier by Dickson. It is also shown (Theorems 12 and 13) that the smallest s for which (1.5) is solvable for all ρ, all odd A, and all α_i prime to A is $s=3$. Explicit criteria for the solvability of (1.5) in the case $s=2$ are also obtained (Theorem 13).

We point out that the problem of representing an algebraic integer as a sum of squares relative to an ideal modulus was considered in 1913 by Klotz [16]. However, aside from a new proof of Dickson's formulas on sums of squares in a Galois field, mentioned above, Klotz's results are largely implicit in nature. His method was a partial generalization of the approach employed by Minkowski for the rational case [18]. While Minkowski based his method in part on the theory of exponential sums, Klotz considered this aspect of Minkowski's method to be "nicht übertragbar" to the case of arbitrary algebraic fields. Actually, as the present paper demonstrates, the theory of exponential sums can be applied to the algebraic case and, in fact, without the necessity of reducing the problem to one involving a prime ideal modulus, corresponding to Minkowski's treatment of the rational case. That this was possible is due to the introduction of exponential methods in algebraic number fields by Hecke [14, chap. 8]. Other applications of such methods have been made by Siegel [21; 22] in the case of sums of squares and mth powers and by Rademacher [20] and Whiteman [23] to sums of primes in algebraic fields.

2. **Some basic theorems.** The first four theorems of this section are results proved in [7]. Since they are fundamental in the applications to follow we restate them all in full. In this section, as in the rest of the paper, F will be a fixed finite extension of the rationals and A a fixed integral ideal of F. In theorems involving applications, the field of values K may be taken to be the complex field. In all other cases K may be assumed to be any field of characteristic zero containing the Nth roots of unity ($N=N(A)$), since no other restrictions on K are actually needed to guarantee the validity of the results of this section.

We introduce the following alternative notation for ϵ_ν,

$$\epsilon_{\nu,\zeta}(\beta) = \epsilon_\nu(\beta) = \epsilon_\beta(\nu), \tag{2.1}$$

for use in places where confusion might otherwise result. Note that for integral θ,

$$\epsilon_{\nu\theta,\zeta} = \epsilon_{\nu,\zeta'} \qquad (\zeta' = \zeta\theta). \tag{2.2}$$

Following Hecke [14, p. 220] we call A and B the denominator and numerator, respectively, of $\zeta = B/A\mathfrak{d}$, $(B, A)=1$. We shall refer to ζ as the associated fraction of $\epsilon_\nu = \epsilon_{\nu,\zeta}$ and unless there is explicit statement to the contrary, we shall assume B to be fixed in the definition of ζ.

We first recall the following useful lemma [14, p. 220; 21, Lemma 7].

LEMMA 1 (HECKE-SIEGEL).

$$\sum_{\beta \pmod{A}} \epsilon_\nu(\beta) = \begin{cases} 0 & (\nu \not\equiv 0 \pmod{A}), \\ N(A) & (\nu \equiv 0 \pmod{A}), \end{cases} \tag{2.3}$$

where β runs over a complete residue system (mod A).

This lemma follows directly from [14, Theorem 101] and the definition of ϵ_ν. We also note the following dual of Lemma 1:

LEMMA 1′ (HECKE-SIEGEL).

$$\sum_{\nu \pmod{A}} \epsilon_\nu(\beta) = \begin{cases} 0 & (\beta \not\equiv 0 \pmod{A}), \\ N(A) & (\beta \equiv 0 \pmod{A}). \end{cases} \tag{2.4}$$

The duality between (2.3) and (2.4) may be viewed as a special case of the duality relation arising in the general theory of characters of finite abelian groups [13, §13.3]. In the following we shall refer to Lemmas 1 and 1′ collectively as the Hecke-Siegel Lemma.

REMARK 1. Before proving the main results of this section, we observe that, if $A = A_1A_2$ and if C is chosen prime to A_1 such that $A_2C = \theta$ is principal, then the set $\alpha + \theta\beta$ ranges over a complete residue system (mod A) as α and β range over complete residue systems (mod A_2) and (mod A_1) respectively. Thus the number of residue systems (mod A_2) contained in $R(A)$ is equal to $N(A_1)$.

As a direct consequence of Lemma 1 we have

THEOREM 1. *If ρ, ν, ν' are integers of F, then*

$$\epsilon_\nu \cdot \epsilon_{\nu'} = \sum_{\rho \equiv \alpha+\beta \pmod{A}} \epsilon_\nu(\alpha)\epsilon_{\nu'}(\beta) = \begin{cases} 0 & (\nu \not\equiv \nu'), \\ N(A)\epsilon_\nu(\rho) & (\nu \equiv \nu'). \end{cases} \tag{2.5}$$

From this result it follows that the ϵ_ν are linearly independent relative to K. We may deduce then without difficulty the fundamental

THEOREM 2. *Every (A, K) arithmetic function f can be represented in one and only one way in the form*

$$f(\beta) = \sum_{\nu \pmod{A}} a_\nu \epsilon_\nu(\beta) \qquad (a_\nu \in K). \tag{2.6}$$

The coefficients a_ν are in fact given by

$$a_\nu = \frac{1}{N(A)} \sum_{\xi \pmod{A}} f(\xi)\epsilon_\nu(-\xi). \tag{2.7}$$

On the basis of Theorems 1 and 2 we can now deduce an important additive principle which will be applied in §§4, 6, 7 to obtain the solutions of the congruence problems described in the Introduction. This principle can be formulated in the following manner:

Let S be a system of representatives (mod A) and let Z_i $(i = 1, \cdots, s)$

be a finite set of integers of F, not all necessarily different, such that each $\xi \in Z_i$ is also contained in S. We place $f_i(\lambda) = c$ if λ is congruent (mod A) to an element of S which appears c times in Z_i. Thus the number $\Delta(\rho)$ of ordered sets $(\xi_1, \cdots, \xi_s)$ such that $\xi_i \in Z_i$ and $\xi_1 + \cdots + \xi_s \equiv \rho \pmod{A}$ is given by the extended Cauchy product, $f_1 \cdots f_s$, and we thus have

THEOREM 3.

$$\Delta(\rho) = \frac{1}{N(A)} \sum_{\nu \pmod{A}} \epsilon_\nu(\rho) \prod_{i=1}^{s} \Big(\sum_{\xi \in Z_i} \epsilon_\nu(-\xi) \Big), \tag{2.8}$$

the interior sum being extended over all integers of Z_i.

We note now that the set $\mathfrak{S}_A(K)$ of all (A, K) arithmetic functions forms a ring relative to the operations of Cauchy multiplication and ordinary addition of functions. Theorem 2 can be reformulated to give an algebraic characterization [10, Chapter 4] of the ring $\mathfrak{S}_A(K)$:

THEOREM 4. *The ring $\mathfrak{S}_A(K)$ of all (A, K) arithmetic functions is a commutative semisimple algebra which can be expressed as a direct sum of $N(A)$ fields $\mathfrak{K}_i$,*

$$\mathfrak{S}_A(K) = \mathfrak{K}_1 \oplus \cdots \oplus \mathfrak{K}_N, \tag{2.9}$$

where each $\mathfrak{K}_i \cong K$, $\mathfrak{K}_i^2 = \mathfrak{K}_i$, $\mathfrak{K}_i \mathfrak{K}_j = 0$ $(i \neq j)$.

The results above are all generalizations of results appearing in [6]. We now prove an additional theorem, of importance in §3, which extends [6, Lemma 4] to arbitrary algebraic fields. Before stating the theorem we introduce some notation.

Let A, B, ζ be defined as above and suppose A_1 and A_2 are ideals dividing A. We write

$$A_1 = A'E_1, \quad A_2 = A'E_2, \quad A^* = E_1E_2A', \quad (E_1, E_2) = 1, \tag{2.10}$$

and choose ideals C', C_1, C_2 such that

$$A'C' = \alpha', \quad E_1C_1 = \alpha_1, \quad E_2C_2 = \alpha_2, \quad (C'C_1C_2, A) = 1, \tag{2.11}$$

where α', α_1, α_2 are principal and

$$C_1 = C_2 = 1 \quad \text{if } E_1 = E_2 = 1. \tag{2.12}$$

We also take

$$\beta = BC_1C_2C'/\mathfrak{d}, \quad \zeta_1 = \beta/\alpha_1\alpha', \quad \zeta_2 = \beta/\alpha_2\alpha', \tag{2.13}$$

so that ζ_1, ζ_2 have denominators A_1, A_2 respectively. We now prove

THEOREM 5. *If μ, ν are integers of F, $(\mu, A_1) = (\nu, A_2) = 1$, where A_1 and A_2 are ideal divisors of A, then*

$$(2.14)\quad \Sigma = \sum_{\rho \equiv \xi+\eta \pmod{A}} \epsilon_{\mu,\zeta_1}(\xi)\epsilon_{\nu,\zeta_2}(\eta) = \begin{cases} N(A)\epsilon_{\mu,\zeta_1}(\rho) & (A_1 = A_2,\ \mu \equiv \nu \pmod{A_1}), \\ 0 & (\textit{otherwise}). \end{cases}$$

Proof. We place $\eta \equiv \rho - \xi$ and, using the additive property of the trace, we get by a simple calculation,

$$(2.15)\qquad \Sigma = \epsilon_{\nu,\zeta_2}(\rho) \sum_{\xi \pmod{A}} \epsilon_{\omega,\zeta^*}(\xi),$$

where

$$(2.16)\qquad \omega = \mu\alpha_2 - \nu\alpha_1, \qquad \zeta^* = \beta/\alpha_1\alpha_2\alpha' = B/\mathfrak{d}A^*.$$

We place $A = A^*\overline{A}$, so that ξ in (2.15) runs over $N(\overline{A})$ residue systems (mod A^*). Therefore

$$(2.17)\qquad \Sigma = \epsilon_{\nu,\zeta_2}(\rho) \cdot N(\overline{A}) \sum_{\xi \pmod{A^*}} \epsilon_{\omega,\zeta^*}(\xi).$$

We are now in a position to apply the Hecke-Siegel Lemma with A^*, ζ^* replacing A, ζ respectively. It thus follows that $\Sigma \neq 0$ if and only if $\omega \equiv 0 \pmod{A^*}$. This condition would imply that $\mu\alpha_2 \equiv 0 \pmod{E_1}$ and, since $(\mu, E_1) = 1$, that $\alpha_2 = E_2C_2 \equiv 0 \pmod{E_1}$. But $(E_1, C_2) = (E_1, E_2) = 1$; therefore it must follow that $E_1 = 1$. Similarly, $\omega \equiv 0 \pmod{A^*}$ implies that $E_2 = 1$, $A_1 = A_2 = A' = A^*$ and, by (2.12), $C_1 = C_2 = 1$, so that consequently $\alpha_1 = \alpha_2 = 1$. Thus the condition $\omega \equiv 0 \pmod{A^*}$ gives $\mu \equiv \nu \pmod{A_1}$, and therefore $\Sigma \neq 0$ implies that $A_1 = A_2$, $\mu \equiv \nu \pmod{A_1}$.

But the converse is also true, for if $A_1 = A_2$, then we may take $E_1 = E_2 = C_1 = C_2 = 1$, and hence $\alpha_1 = \alpha_2 = 1$. If in addition $\mu \equiv \nu \pmod{A_1}$, then $\omega \equiv 0 \pmod{A^*}$. We have thus shown that

$$(2.18)\qquad \Sigma \neq 0 \rightleftarrows A_1 = A_2, \qquad \mu \equiv \nu \pmod{A_1}.$$

In such a case we have $\zeta_1 = \zeta_2 = \zeta^*$; consequently $\epsilon_{\nu,\zeta_2}(\rho) = \epsilon_{\mu,\zeta_1}(\rho)$, and by the Hecke-Siegel Lemma, $\Sigma = \epsilon_{\nu,\zeta_2}(\rho)N(\overline{A})N(A^*) = \epsilon_{\mu,\zeta_1}(\rho)N(A)$, which proves the theorem.

It may be noted that in case F is a principal ideal field, a less involved proof along the lines of the rational case [6, Lemma 4] can be constructed for the above theorem.

3. **Subalgebras related to Rademacher's sum.** By Theorems 2 and 4 the ring $\mathfrak{S}_A(K)$ of all arithmetic functions is semisimple with orthogonal basis given by the functions $1/N(A) \cdot \epsilon_\nu(\beta)$, where ν ranges over a complete set of residues (mod A). The unit element of $\mathfrak{S}_A(K) = \mathfrak{S}$ is, by (2.4),

$$(3.1)\qquad I = \frac{1}{N(A)} \sum_{\nu \pmod{A}} \epsilon_\nu(\beta) = \begin{cases} 1 & (\beta \equiv 0 \pmod{A}), \\ 0 & (\beta \not\equiv 0 \pmod{A}). \end{cases}$$

The set of all functions of the form

$$\sum_{(\mu,A)=1} a_\mu \epsilon_\mu(\beta), \qquad a_\mu \in K, \tag{3.2}$$

where μ ranges over a reduced set of residues (mod A), is an ideal of $\mathfrak{S}$ with unit element,

$$I_1 = 1/N(A)\cdot R(\beta, A), \qquad R_A = R(\beta, A) = \sum_{(\mu,A)=1} \epsilon_\mu(\beta). \tag{3.3}$$

The function $R(\beta, A)$ is the Rademacher function [20, §2.2] and has the following important properties:

(a) $$R(\beta, A) = \sum_{E \mid (A,\beta)} N(E)\bar{\mu}\left(\frac{A}{E}\right),$$

where E ranges over the ideal divisors of (A, β) and $\bar{\mu}$ is the Möbius function in F.

(b) $$R(\beta, AA') = R(\beta, A)R(\beta, A') \qquad \text{if } (A, A') = 1.$$

(c) $R(\beta, A)$ is independent of the choice of the numerator of the fraction ζ associated with R_A.

(d) $$R(\beta, A) = R(-\beta, A).$$

An example of a subalgebra of $\mathfrak{S}$, not an ideal, is given by the set of all elements of the form $\sum a_{A_i} R(\beta, A_i)$ where the A_i range over the divisors of A. Before showing this we prove

LEMMA 2. *Let $A_i\overline{A}_i = A$ and let L_i be an integral ideal, prime to A_i, such that $\overline{A}_i L_i = \theta_i$ is principal. Then the set of numbers $\mu_i\theta_i$, where μ_i ranges over a reduced set of residues* (mod A_i) *and A_i ranges over all divisors of A, forms a complete residue system* (mod A).

Proof. The number of such elements $\mu_i\theta_i$ is given by

$$\sum_{A_i \mid A} \phi(A_i) \equiv V(A)$$

where ϕ is the Euler ϕ-function in F. Analogous to a familiar result in the rational case [12, Theorem 262] we have

$$V(A) = N(A). \tag{3.4}$$

(This result follows easily for a prime power ideal $A = P^\lambda$, and on the basis of the factorability of ϕ, V, N, it follows for arbitrary ideals A.) Moreover, no two of the elements $\mu\theta$ are congruent (mod A), for if $\mu_i\theta_i \equiv \nu_j\theta_j$ (mod A), where $(\nu_j, A_j) = 1$ and A_j, $\overline{A}_j$, L_j are as defined above, then we get $\mu_i\overline{A}_iL_i \equiv 0$ (mod $\overline{A}_j$). Multiplication by A_iA_j leads to $\mu_iA_jL_i \equiv 0$ (mod A_i). But since

$(\mu_i, A_i)=(L_i, A_i)=1$, then $A_i \mid A_j$. Similarly $A_j \mid A_i$ and $i=j$. Further, $\mu_i\theta_i \equiv \nu_i\theta_i \pmod{A}$ implies $\mu_i \equiv \nu_i \pmod{A_i}$.

We also have the related

LEMMA 3. *Following the notation of Lemma 2, the set of elements $\nu_i\theta_i$, where ν_i ranges over a complete set of residues* (mod A_i), *forms the totality of elements δ of $R(A)$ such that $\overline{A}_i \mid \delta$.*

This lemma follows from Remark 1 of the preceding section.

We now prove

THEOREM 6. *The set of all functions $\mathfrak{M}=\mathfrak{M}_A(K)$ of the form*

$$w = \sum_{A_i \mid A} a_{A_i} R(\beta, A_i), \tag{3.5}$$

A_i ranging over all ideal divisors of A and a_{A_i} over all elements of K, is a semi-simple subalgebra of $\mathfrak{S}$, with orthogonal basis given by the totality of elements $1/N(A)\cdot R(\beta, A_i)$ and with unit element identical with that of $\mathfrak{S}$.

Proof. We have simply to consider the Cauchy product of two elements R_{A_i}, say R_{A_1}, R_{A_2}. By property (c) above, R_{A_i} is independent of the choice of numerator in the associated fraction ζ_i. In performing the product $R_{A_1}\cdot R_{A_2}$ we may therefore choose ζ_1 and ζ_2 satisfying the conditions of (2.10)–(2.13). This will enable us to apply Theorem 5. We have then

$$\begin{aligned} R_{A_1}\cdot R_{A_2} &= \sum_{\rho \equiv \alpha+\beta \pmod{A}} R(\alpha, A_1)R(\beta, A_2) \\ &= \sum_{(\mu, A_1)=1,\,(\nu, A_2)=1} \sum_{\rho \equiv \alpha+\beta \pmod{A}} \epsilon_{\mu,\zeta_1}(\alpha)\epsilon_{\nu,\zeta_2}(\beta), \end{aligned}$$

where μ, ν range over reduced sets of residues modulo A_1 and A_2 respectively. Thus by Theorem 5 one obtains

$$R_{A_1}\cdot R_{A_2} = \begin{cases} N(A) \sum_{(\mu, A_1)=1} \epsilon_{\mu,\zeta_1}(\rho) = N(A)R(\rho, A_1) & (A_1 = A_2), \\ 0 & (A_1 \neq A_2). \end{cases} \tag{3.6}$$

This proves that $\mathfrak{M}$ is semisimple with orthogonal basis $1/N(A)\cdot R_{A_i}$, $A_i \mid A$.

In the rest of the proof we attach to the fraction ζ_i associated with R_{A_i} the value $\zeta_i=\zeta\theta_i=BL_i/A_i\mathfrak{d}$, where θ_i and L_i are defined as in Lemma 2. Then the unit I_2 of $\mathfrak{M}$ is given by

$$\begin{aligned} \frac{1}{N(A)} \sum_{A_i \mid A} R(\beta, A_i) &= \frac{1}{N(A)} \sum_{A_i \mid A} \sum_{(\mu_i, A_i)=1} \epsilon_{\mu_i,\zeta_i}(\beta) \\ &= \frac{1}{N(A)} \sum_{A_i \mid A} \sum_{(\mu_i, A_i)=1} \epsilon_{\mu_i\theta_i,\zeta}(\beta). \end{aligned}$$

But by Lemma 2, $\mu_i\theta_i$ ranges over a complete residue system (mod A) as A_i

ranges over all divisors of A. Therefore we get, on applying the Hecke-Siegel Lemma,

$$I_2 = \frac{1}{N(A)} \sum_{\nu \pmod A} \epsilon_\nu(\beta) = \begin{cases} 1 & (\beta \equiv 0 \pmod A), \\ 0 & (\beta \not\equiv 0 \pmod A). \end{cases} \tag{3.7}$$

If we specialize in (3.6) to the case $A_1A_2=A$, $\rho=0$, we get

$$\Sigma' = \sum_{\alpha \equiv -\beta \pmod A} R(\alpha, A_1)R(\beta, A_2) = \sum_{\alpha \pmod A} R(\alpha, A_1)R(-\alpha, A_2),$$

which by (3.6) and property (d) above gives

$$\Sigma' = \sum_{\alpha \pmod{A_1A_2}} R(\alpha, A_1)R(\alpha, A_2) = 0 \qquad (A_1 \neq A_2). \tag{3.8}$$

If $A_1=A_2$ then Σ' becomes, by (3.6),

$$\Sigma' = \sum_{\alpha \pmod{A_1^2}} R(\alpha, A_1)R(\alpha, A_2) = N(A_1^2)R(0, A_1), \tag{3.9}$$

but since the sum in (3.9) runs over $N(A_1)$ residue systems (mod A_1) we have

$$\Sigma' = N(A_1) \sum_{\alpha \pmod{A_1}} (R(\alpha, A_1))^2 = (N(A_1))^2R(0, A_1),$$

$$\sum_{\alpha \pmod{A_1}} (R(\alpha, A_1))^2 = N(A_1)\phi(A_1). \tag{3.10}$$

Combining (3.8) and (3.10) one gets the following orthogonality property of R_A:

THEOREM 7. *If $A \neq C$ are integral ideals of F, then*

$$\begin{aligned} \sum_{\alpha \pmod A} (R(\alpha, A))^2 &= N(A)\phi(A), \\ \sum_{\alpha \pmod{AC}} R(\alpha, A)R(\alpha, C) &= 0. \end{aligned} \tag{3.11}$$

In the rational case this theorem reduces to a result [3, §1] which Carmichael found useful in the study of series expansions of arithmetic functions. The question of extending such applications to algebraic fields arises, but we shall not go into this question in the present paper.

4. **Sums of products.** Before proving the principal result of this section, we apply Property (a) of §3 to get

LEMMA 4. *If P is a prime ideal of degree f and k is a positive integer, then*

$$R(\beta, P^k) = \begin{cases} p^{f(k-1)}(p^f - 1) & (P^k \mid \beta), \\ -p^{f(k-1)} & (P^{k-1} \mid \beta,\ P^k \nmid \beta), \\ 0 & (P^{k-1} \nmid \beta). \end{cases} \tag{4.1}$$

We also note that if A has the factorization

$$A = P_1^{\lambda_1} \cdots P_h^{\lambda_h} \tag{4.2}$$

into powers of distinct prime ideals $P_1, \cdots, P_h$, then the ring $R(A)$ has, as in the rational case [13, p. 53], the direct decomposition,

$$R(A) = R(P_1^{\lambda_1}) \oplus \cdots \oplus R(P_h^{\lambda_h}). \tag{4.3}$$

Restated, the elements ρ of $R(A)$ are representable as vectors, $\rho \leftrightarrow(\rho_1, \cdots, \rho_h)$, where each ρ_i ranges over a complete residue system (mod $P_i^{\lambda_i}$), $\rho \equiv \rho_i \pmod{P_i^{\lambda_i}}$. On the basis of this vector representation, it is easy to prove

LEMMA 5. *If A has the factorization* (4.2) *and if $\rho, \alpha_1, \cdots, \alpha_s$ are arbitrary integers of F, then the number of solutions $\Phi(\rho, A)$ in x_{ij}, $(x_{ij}, A)=1$, of the congruence* (1.4) *is given by $\Phi(\rho, A)=\Phi(\rho, P_1^{\lambda_1}) \cdots \Phi(\rho, P_h^{\lambda_h})$.*

We next prove

THEOREM 8. *If P is a prime ideal of degree f and if $\rho, \alpha_1, \cdots, \alpha_s$ are integers of F such that $\alpha_1, \cdots, \alpha_t$ $(s \geqq t > 0)$ are prime to P and α_i $(i > t)$ are divisible by P, then the number of solutions $\Phi_{s,t,l}=\Phi(\rho, P^\lambda)=\Phi(\rho)$, $\lambda > 0$, of the congruence*

$$\rho \equiv \alpha_1 x_{11} \cdots x_{l1} + \cdots + \alpha_s x_{1s} \cdots x_{ls} \pmod{P^\lambda}, \tag{4.4}$$

in x_{ij} prime to P, is given by

$$\Phi(\rho) = p^{f(s\lambda l - s l - \lambda)}(p^f - 1)^{ls-t}\{(p^f - 1)^t + q(\rho)e_t\}, \tag{4.5}$$

where

$$q(\rho) = \begin{cases} -1 & (\rho \not\equiv 0 \pmod{P}), \\ p^f - 1 & (\rho \equiv 0 \pmod{P}), \end{cases}$$

and $e_t = +1$ or -1 according as t is even or odd.

Proof. The principle in Theorem 3 relating to additive congruence problems can be applied to (4.4) to give

$$\Phi(\rho) = p^{-\lambda f} \sum_{\nu \pmod{P^\lambda}} \epsilon_\nu(\rho) \prod_{i=1}^{s} \Bigg(\sum_{(y_j, P)=1, y_j \pmod{P^\lambda}} \epsilon_\nu(-\alpha_i y_1 \cdots y_l) \Bigg), \tag{4.6}$$

where the y_j range independently over reduced residue systems (mod P^λ). If one denotes by $\sigma_i(\nu)$ the inner sum of (4.6), it follows in case $\nu \equiv 0 \pmod{P^\lambda}$ that

$$\sigma(0) = \sigma_i(0) = (\phi(P^\lambda))^l = p^{f(\lambda-1)l}(p^f - 1)^l. \tag{4.7}$$

If $\nu \not\equiv 0 \pmod{P^\lambda}$, the hypothesis $(\alpha_1, P)=1$ and Lemma 4 show that the

product in (4.6) $=0$ unless $P^{\lambda-1}\mid\nu$, in which case we get

$$\sigma_i(\nu) = R(-\alpha_i\nu, P^\lambda)(\phi(P^\lambda))^{l-1}.$$

Thus, for $P^{\lambda-1}\mid\nu$, $P^\lambda\nmid\nu$, we have by (4.1),

$$\sigma_i(\nu) = \begin{cases} -p^{f(\lambda-1)}(p^f-1)^{l-1}p^{f(\lambda-1)(l-1)} = \sigma_1 & (1\leqq i\leqq l), \\ p^{f(\lambda-1)l}(p^f-1)^l = \sigma_2 & (i>l). \end{cases} \tag{4.8}$$

By Lemma 3, the only $\nu\not\equiv 0 \pmod{P^\lambda}$ which contribute anything to (4.6), namely all such ν which are divisible by $P^{\lambda-1}$, can be represented in the form $\nu=\gamma P^{\lambda-1}G$ where $(G, P)=1$, $\theta=GP^{\lambda-1}$ is principal, and γ ranges over a reduced residue system (mod P). Hence we have

$$\Phi(\rho) = p^{-\lambda f}\left\{(\sigma(0))^s + \sum_{\gamma \pmod P,\,(\gamma,P)=1} \epsilon_{\gamma\theta,\zeta}(\rho)\prod_{i=1}^{s}\sigma_i(\nu)\right\}, \tag{4.9}$$

where $\zeta=B/P^\lambda\mathfrak{d}$. Observing that $\zeta'=\theta\zeta=BG/P\mathfrak{d}$ is of denominator P, we see that (4.9) becomes

$$\Phi(\rho) = p^{-\lambda f}\left\{(\sigma(0))^s + \sum_{\gamma \pmod P,\,(\gamma,P)=1} \epsilon_{\gamma,\zeta'}(\rho)\cdot\sigma_1{}^t\sigma_2{}^{s-t}\right\}, \tag{4.10}$$

and evaluation of (4.10) on the basis of (4.7), (4.8) and the Hecke-Siegel Lemma leads to the theorem.

If at least one α_i is prime to A, it follows that the number of solutions of (1.4) in x_{ij} prime to A is completely determined by Lemma 5 and Theorem 8.

One notes by (4.5) that $\Phi(\rho)=0$ if and only if

$$(p^f-1)^t + q(\rho)e_t = 0. \tag{4.11}$$

Thus, if P is an odd ideal, that is, if $p>2$, (4.11) can occur if and only if $t=1$, $P\mid\rho$. If P is even, so that $p=2$, then (4.11) occurs if and only if either $f=1$, $(\rho, P)=1$, t even, or $f=1$, $P\mid\rho$, t odd, or $f>1$, $t=1$, $P\mid\rho$.

COROLLARY 1. *If P is even of degree >1 or if P is odd, then* (4.4) *is solvable for all ρ, l, and λ if and only if $s\geqq t\geqq 2$.*

Specializing Theorem 8 to the case $l=1$ we get

COROLLARY 2. *If ρ, α_i, and P satisfy the conditions of Theorem* 8, *the number of solutions x_i prime to P of*

$$\rho \equiv \alpha_1x_1 + \cdots + \alpha_sx_s \pmod{P^\lambda} \tag{4.12}$$

is given by

$$\Phi_1(\rho) = p^{f(s\lambda-\lambda-s)}(p^f-1)^{s-t}\{(p^f-1)^t + q(\rho)e_t\} \tag{4.13}$$

where q and δ are defined as in the theorem.

Further specialization to the case of F rational leads to [6, Theorem 6] which is important in the solution of the finite Goldbach problem for the rational field [8]. Corollary 2 bears the same importance to the analogous problem for algebraic numbers fields.

We mention finally four reduction formulas as corollaries of Theorem 8. By Corollary 2 we verify easily

COROLLARY 3.

$$\Phi(\rho) = p^{fs(\lambda-1)(l-1)}(p^f - 1)^{s(l-1)}\Phi_1(\rho). \tag{4.14}$$

This result may also be deduced from (4.13), observing that for each solution of (4.12) there are $(\phi(P^\lambda))^{s(l-1)}$ solutions of (4.4) and that all solutions of (4.4) arise in such a manner.

COROLLARY 4.

$$\Phi(\rho, P^\lambda) = p^{f(\lambda-1)(ls-1)}\Phi(\rho, P). \tag{4.15}$$

COROLLARY 5. *If* $s, s' \geqq t$, *and* $ls = l's'$, *then*

$$\Phi_{s,t,l} = \Phi_{s',t,l'}; \tag{4.16}$$

in particular,

$$\Phi_{s,t,l} = \Phi_{ls,t,1}, \tag{4.17}$$

$$\Phi_{s,t,l} = \Phi_{l,t,s} \qquad (l \geqq t). \tag{4.18}$$

COROLLARY 6. *If* $s' = s + n$ $(s \geqq t,\ n \geqq 0)$, *then*

$$\Phi_{s',t,l} = p^{fln(\lambda-1)}(p^f - 1)^{ln}\Phi_{s,t,l}. \tag{4.19}$$

5. **The Hecke sum and the related T sum.** Hecke's sum [14, (166)] is a generalization to algebraic number fields of the well known Gauss sum, and is defined by

$$S(\beta) = \sum_{\xi \pmod A} \epsilon\xi^2(\beta). \tag{5.1}$$

In order to avoid ambiguities of sign we redefine the Hecke function in a more precise manner.

Let us consider first the case of a prime ideal, $A = P$, $N(P) = p^f$. In this case, the residue class ring $R(P)$ is a field isomorphic with the Galois field $GF(p^f)$, [19, §5]. We conceive of the elements of $GF(p^f)$ as polynomials

$$U = a_f + a_{f-1}\Theta + \cdots + a_1\Theta^{f-1} \tag{5.2}$$

with coefficients (mod p) and reduced modulo a fixed (primary) irreducible polynomial $E(\Theta)$ of degree f.

With this representation of $R(P)$ in mind, we define, for $U \in GF(p^f)$, a function [1, §2],

$$\omega_U(M) = \omega(MU, E) = e^{2\pi ic/p}, \tag{5.3}$$

where c is the coefficient of Θ^{f-1} in MU, reduced (mod E), M being an arbitrary element of $GF(p^f)$. The function ω defines an additive function, or character, on the additive group of $GF(p^f)$: $\omega_U(M+M') = \omega_U(M)\omega_U(M')$. Thus the isomorphism, $R(P) \cong GF(p^f)$, defines a similar character on $R(P)$, and it follows that each ω_U is equivalent to some ϵ_ν. With ζ of denominator P, we choose the numerator of ζ such that

$$\epsilon_1(\alpha) = \epsilon_{1,\zeta}(\alpha) = \omega_1(M, E) \qquad (M \leftrightarrow \alpha), \tag{5.4}$$

where M corresponds to α under a fixed isomorphism of $R(P)$ and $GF(p^f)$. We refer to $\epsilon_1(\alpha)$ as the unity function of $R(P)$, relative to the isomorphism in (5.4). With this choice of ζ we now define

$$S(1, P) = \sum_{\xi \pmod P} \epsilon_1(\xi^2), \tag{5.5}$$

$$S(\mu, P) = \sum_{\xi \pmod P} \epsilon_\mu(\xi^2). \tag{5.6}$$

In order to define $S(1, P^\lambda)$ for *fixed* $\lambda \geqq 1$, we choose C such that

$$PC = \theta, \qquad (C, P) = 1, \qquad (\theta \text{ principal}). \tag{5.7}$$

Next we may choose $B = B_\lambda$ in

$$\zeta_1 = \zeta_\lambda \theta^{\lambda-1}, \qquad \zeta = \zeta_\lambda = B_\lambda / P^\lambda \mathfrak{d}, \tag{5.8}$$

so that ϵ_1, ζ_1 is the unity function of $R(P)$ as defined in (5.4). With this notation we now define

$$S(1, P^\lambda) = \sum_{\xi \pmod{P^\lambda}} \epsilon_{1,\zeta}(\xi^2), \tag{5.9}$$

$$S(\mu, P^\lambda) = \sum_{\xi \pmod{P^\lambda}} \epsilon_{\mu,\zeta}(\xi^2). \tag{5.10}$$

In the rest of the paper we assume P to be *odd* ($p > 2$). On the basis of the above notation, Hecke's Hilfssatz [14, p. 222] becomes

LEMMA 6.

$$S(1, P^\lambda) = \begin{cases} (N(P))^{\lambda/2} & (\lambda \textit{ even}), \\ (N(P))^{(\lambda-1)/2} S(1, P) & (\lambda \textit{ odd}). \end{cases} \tag{5.11}$$

We are thus led to an evaluation of $S(1, P^\lambda)$:

LEMMA 7. $S(1, P^\lambda) = (N(P))^{\lambda/2} J(\lambda f)$, $J(b) = i^{(p^b-1)^2/4}$.

Proof. In the case $\lambda = 1$, the value of $S(1, P)$ can be computed by passing to the corresponding sum Σ in $GF(p^f)$, obtained on the basis of the isomorphism in (5.4),

$$S(1, P) = \sum_{X \pmod{E}} \omega_1(X^2, E) \equiv \Sigma,$$

where X is the isomorphic image of ξ in (5.5). Here E is, as defined above, an irreducible polynomial (mod p) of degree f. But by [1, Theorem 2], $\Sigma = S(1, P)$ has the value $p^{f/2}J(f)$. Moreover

$$J(\lambda f) = \begin{cases} 1 & (\lambda \text{ even}), \\ J(f) & (\lambda \text{ odd}), \end{cases} \tag{5.12}$$

which proves the lemma, on applying (5.11).

As a consequence one finds that

LEMMA 8.

$$S^2(1, P^\lambda) = \left(\frac{-1}{P}\right)^\lambda p^{f\lambda}, \tag{5.13}$$

where $(-1/P)$ *is the Legendre symbol in* F.

Proof. It suffices, by Lemma 7, to show that $J^2(\lambda f) = (-1/P)^\lambda$. That this is true for λ even is evident. If λ is odd, f even, then $J^2(\lambda f) = 1$ by (5.12). But for f even, since $x^2 \equiv -1$ is solvable (mod P), that is, since $x^2 = -1$ is solvable in $GF(p^f)$ [9, §62], it is clear that $(-1/P) = 1$.

If λ is odd, f odd, then by (5.12),

$$J^2(\lambda f) = J^2(1) = \begin{cases} 1 & (p \equiv 1 \pmod 4), \\ -1 & (p \equiv 3 \pmod 4). \end{cases}$$

But in case f is odd, it is also true [9, §62; 17, Theorem 83] that

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p}\right) = \begin{cases} 1 & (p \equiv 1 \pmod 4), \\ -1 & (p \equiv 3 \pmod 4), \end{cases}$$

so that the lemma follows in all cases.

One may also reformulate Hecke's Theorem [14, Theorem 155] for the case $A = P^\lambda$ in the following manner.

LEMMA 9.

$$S(\mu, P^\lambda) = \left(\frac{\mu}{P^\lambda}\right) S(1, P^\lambda), \qquad (\mu, P) = 1, \tag{5.14}$$

(μ/P^λ) *being the Jacobi symbol in* F.

Before introducing the T sum we add to our notation. As in (5.8) we define generally

$$\zeta_k = \zeta\theta^{\lambda-k} = B_k/P^k\mathfrak{d}, \qquad B_k = BC^{\lambda-k} \qquad (0 \leqq k \leqq \lambda), \tag{5.15}$$

θ, B, ζ being defined by (5.7) and (5.8). It can be seen that ζ_k $(k \geqq 1)$ is admissible as the associated fraction in the sum $S(1, P^k)$, since $\zeta_1 = \zeta_k \theta^{k-1} = \zeta_\lambda \theta^{\lambda-1}$, and we place

$$S(\rho, P^k) = \sum_{\xi \pmod{P^k}} \epsilon_{\rho,\zeta_k}(\xi^2) \qquad (0 \leqq k \leqq \lambda). \tag{5.16}$$

We now define for integral ρ,

$$T(\rho, P^k) = \sum_{\xi \pmod{P^k},\,(P,\xi)=1} \epsilon_{\rho,\zeta_k}(\xi^2), \tag{5.17}$$

where the summation is over a reduced residue system (mod P^k). We now evaluate (5.17) in the case of odd prime ideals P. By definition of T and Lemma 3, we get for $k > 1$,

$$T(\rho, P^k) = \sum_{\xi \pmod{P^k}} \epsilon_{\rho,\zeta_k}(\xi^2) - \sum_{\xi' \pmod{P^{k-1}}} \epsilon_{\rho,\zeta_k}((\xi'\theta)^2) \tag{5.18}$$

where θ is defined by (5.7). But since $\zeta_k \theta^2 = \zeta_{k-2}$ and since ξ' ranges over $N(P) = p^f$ residue systems (mod P^{k-2}), (5.18) gives

$$\begin{aligned} T(\rho, P^k) &= S(\rho, P^k) - p^f \sum_{\xi' \pmod{P^{k-2}}} \epsilon_{\rho,\zeta_{k-2}}(\xi'^2) \\ &= S(\rho, P^k) - p^f S(\rho, P^{k-2}), \qquad k > 1. \end{aligned} \tag{5.19}$$

If $k = 1$, then we have from (5.17)

$$T(\rho, P) = S(\rho, P) - 1. \tag{5.20}$$

We now introduce the convention

$$S(\rho, P^{-1}) = p^{-f}, \tag{5.21}$$

so that (5.19) and (5.20) can be combined to give

LEMMA 10.

$$T(\rho, P^k) = S(\rho, P^k) - p^f S(\rho, P^{k-2}), \qquad k \geqq 1. \tag{5.22}$$

Now let us suppose that t is the largest non-negative integer $\leqq k$ such that $P^t \mid \rho$. By Lemma 2, we may then assume ρ (mod P^k) to be of the form

$$\rho = \begin{cases} \theta^t \mu, & (\mu, P) = 1 \qquad (0 \leqq t < k), \\ \theta^t \equiv 0, & \mu = 1 \qquad (t = k), \end{cases} \tag{5.23}$$

where θ is defined by (5.7). Noting that

$$\theta^t \zeta_k = \zeta_{k-t} \qquad (k \geqq t) \tag{5.24}$$

we get, on substituting (5.23) and (5.24) in (5.16),

$$S(\rho, P^k) = (N(P))^t S(\mu, P^{k-t}), \qquad k \geqq t. \tag{5.25}$$

We also find, on applying Lemmas 6 and 9, that

LEMMA 11.

$$S(\mu, P^k) = N(P) \cdot S(\mu, P^{k-2}), \qquad (\mu, P^k) = 1, \qquad k > 1. \tag{5.26}$$

This leads to an evaluation of $T(\rho, P^k)$:

LEMMA 12. *If* t, μ *are defined by* (5.23) *and* $k \geqq 1$, *then*

$$T(\rho, P^k) = \begin{cases} 0 & (t \leqq k-2), \\ p^{f(k-1)}(S(\mu, P) - 1) & (t = k-1), \\ p^{f(k-1)}(p^f - 1) & (t = k). \end{cases} \tag{5.27}$$

Proof. Case 1 ($k>1$). If $t \leqq k-2$, then application of (5.25) and (5.26) to $T(\rho, P^k)$ in Lemma 10 gives $T=0$. If $t=k-1$, one obtains, by (5.25) and (5.22), $T(\rho, P^k) = p^{f(k-1)}S(\mu, P) - p^f S(0, P^{k-2})$, and noting that

$$S(0, P^l) = (N(P))^l = p^{fl} \qquad (l \geqq 0), \tag{5.28}$$

the theorem follows in this case. If $t=k$, then application of (5.28) leads to the result.

Case 2 ($k=1$). Two subcases arise: $t=0$ and $t=1$. If $t=0$, $(\rho, P)=1$, $\rho=\mu$, then (5.20) gives the result for this case. If $t=1$, it suffices to apply (5.25) to (5.20), using the fact that $S(\mu, 1)=1$.

We remark that $T(\rho, P^k)$ has properties similar to those of the sum $R(\rho, P^k)$; a rather detailed discussion of these properties for the rational case will be given in a paper to be published elsewhere.

6. **Sums of an even number of squares.** We point out first that the quantities λ, C, $B=B_\lambda$, $\zeta=\zeta_\lambda$, t, B_k, ζ_k, ρ, μ will be assumed fixed for the rest of the paper. Each will have the same significance as in §5; note, in particular, (5.7), (5.8), (5.15), and (5.23) for the defining relations.

Before stating Theorem 9 we introduce the following new notation:

$$\sigma = \left(\frac{(-1)^l \alpha_1 \cdots \alpha_s}{P}\right), \qquad l = \begin{cases} m & (s = 2m), \\ m+1 & (s = 2m+1), \end{cases} \tag{6.1}$$

$$\nu = \sigma p^{f(2m\lambda - \lambda - m)}, \tag{6.2}$$

$$\Gamma(t) = (1 - p^f)\frac{1 - \sigma^t p^{ft(1-m)}}{1 - \sigma p^{f(1-m)}}, \tag{6.3}$$

$$\eta(t) = \begin{cases} \sigma^t & (0 \leqq t < \lambda), \\ 0 & (t = \lambda). \end{cases} \tag{6.4}$$

The quantities α_i will be defined in the statement of the main theorem. On the basis of properties (a), (b) of the direct decomposition (4.3), we have

LEMMA 13. *If* A *is an arbitrary odd ideal of* F *with the factorization* (4.2),

$A = P_1^{\lambda_1} \cdots P_h^{\lambda_h}$, if $\rho, \alpha_1, \cdots, \alpha_s$ are integers of F, then the number of incongruent solutions $\psi_s(\rho, A)$ of (1.5) is given by $\psi_s(\rho, P_1^{\lambda_1}) \cdots \psi_s(\rho, P_h^{\lambda_h})$.

This lemma makes it unnecessary to consider any but powers of prime ideals. We now state

THEOREM 9. *If P is an arbitrary odd prime ideal, if $\alpha_1, \cdots, \alpha_s$ are integers of F prime to P, if ρ is an arbitrary integer of F and t is the largest rational integer $\leqq \lambda$ such that $\rho \equiv 0 \pmod{P^t}$, then the number of distinct solutions $\pmod{P^\lambda}$, $\lambda \geqq 1$, of*

$$\rho \equiv \alpha_1 \xi_1^2 + \cdots + \alpha_s \xi_s^2 \pmod{P^\lambda} \tag{6.5}$$

is given, in case $s = 2m$, $m > 1$, by

$$\psi_{2m}(\rho) = p^{f\lambda(2m-1)} - \nu\{\Gamma(t) + \eta(t) p^{ft(1-m)}\}. \tag{6.6}$$

Proof. We first apply Theorem 3 to get the following exponential formula for the number of solutions of (6.5) for *arbitrary* s:

$$\psi_s(\rho) = p^{-f\lambda} \sum_{\gamma \pmod{P^\lambda}} \epsilon_\gamma(\rho) \prod_{i=1}^{s} S(-\alpha_i\gamma, P^\lambda) \qquad (\epsilon_\gamma = \epsilon_{\gamma,\xi}). \tag{6.7}$$

We next observe, by Lemma 2, that a complete residue system $\pmod{P^\lambda}$ is given by $\gamma_k \theta^{\lambda-k}$, $k = 0, 1, \cdots, \lambda$, where each γ_k ranges over a reduced set of residues $\pmod{P^k}$. Thus (6.7) may be written, on isolating $\gamma = 0$,

$$\psi_s(\rho) = p^{-f\lambda}\left\{p^{\lambda f s} + \sum_{k=1}^{\lambda} \sum_{\gamma \pmod{P^k}, (\gamma,P)=1} \epsilon_{\gamma\theta^{\lambda-k},\xi}(\rho) \prod_{i=1}^{s} S(-\alpha_i\gamma\theta^{\lambda-k}, P)^\lambda\right\}. \tag{6.8}$$

But by the definition of ζ_k, (5.15), and relation (5.25), (6.8) becomes

$$p^{-f\lambda}\left\{p^{\lambda f s} + \sum_{k=1}^{\lambda} \sum_{\gamma \pmod{P^k}, (\gamma,P)=1} \epsilon_{\gamma,\zeta_k}(\rho) \prod_{i=1}^{s} \sum_{\xi \pmod{P^\lambda}} \epsilon_{\alpha_i\gamma,\zeta_k}(-\xi^2)\right\}.$$

But ξ runs over $N(P^{\lambda-k}) = p^{f(\lambda-k)}$ residue systems $\pmod{P^k}$, so by the definition of $S(\mu, P^k)$, (5.16), we get

$$\psi_s(\rho) = p^{f\lambda(s-1)}\left\{1 + \sum_{k=1}^{\lambda} p^{-fks} \sum_{\gamma \pmod{P^k}, (\gamma,P)=1} \epsilon_{\gamma,\zeta_k}(\rho) \prod_{i=1}^{s} S(-\alpha_i\gamma, P^k)\right\}. \tag{6.9}$$

Applying (5.14), one obtains

$$\psi_s(\rho) = p^{f\lambda(s-1)}\left\{1 + \sum_{k=1}^{\lambda} p^{-fks}\left(\frac{(-1)^s \alpha_1 \cdots \alpha_s}{P^k}\right)(S(1, P^k))^s \cdot \sum_{\gamma \pmod{P^k}, (\gamma,P)=1} \left(\frac{\gamma}{P^k}\right)^s \epsilon_{\gamma,\zeta_k}(\rho)\right\}. \tag{6.10}$$

Formula (6.10) holds for s either even or odd. If we now suppose $s=2m$ in (6.10), ψ_s becomes

$$\psi_{2m}(\rho) = p^{f\lambda(2m-1)}\left\{1 + \sum_{k=1}^{\lambda} p^{-2fkm}\left(\frac{\alpha_1 \cdots \alpha_s}{P^k}\right)(S^2(1, P^k))^m \cdot \sum_{\gamma(\mathrm{mod}\ P^k),(\gamma,P)=1} \epsilon_{\gamma,\zeta_k}(\rho)\right\}. \tag{6.11}$$

Applying now (5.13) to (6.11) we get

$$\psi_{2m}(\rho) = p^{f\lambda(2m-1)}\left\{1 + \sum_{k=1}^{\lambda} \sigma^k p^{-fkm} R(\rho, P^k)\right\}, \tag{6.12}$$

where σ is defined by (6.1) and $R(\rho, P^k)$ by (3.3).

To evaluate (6.12) we place

$$\chi(t) = \begin{cases} 0 & (t = \lambda), \\ 1 & (t \neq \lambda), \end{cases} \tag{6.13}$$

so that by (6.4),

$$\eta(t) = \chi(t)\sigma^t. \tag{6.14}$$

On the basis of this notation and Lemma 4, (6.12) may be written

$$\psi_{2m}(\rho) = p^{f\lambda(2m-1)}\left\{1 + \sum_{k=1}^{t} \sigma^k p^{-fkm} R(\rho, P^k) + \chi(t)\sigma^{t+1} p^{-fm(t+1)} R(\rho, P^{t+1})\right\}, \tag{6.15}$$

where the k-sum is taken to be zero in the vacuous case $t=0$. Applying now (4.1) and (6.14) we get

$$\psi_{2m}(\rho) = p^{f\lambda(2m-1)}\left\{1 + (1 - p^{-f})\sum_{k=1}^{t} (\sigma p^{f(1-m)})^k - \sigma\eta(t) p^{f(t-mt-m)}\right\}. \tag{6.16}$$

If we now assume $m>1$, the value of the geometric sum in (6.16) is given by

$$\sum_{k=1}^{t} (\sigma p^{f(1-m)})^k = \sigma p^{f(1-m)}(1 - p^f)^{-1}\Gamma(t) \qquad (t \geqq 0), \tag{6.17}$$

the formula holding in case $t=0$ by virtue of the fact that $\Gamma(0)=0$. Substitution in (6.16) leads to the theorem.

In the excluded case, $m=1$, (6.16) yields

$$\psi_2(\rho) = p^{f\lambda}\left\{1 + (1 - p^{-f})\sum_{k=1}^{t} \sigma^k - \sigma\eta(t) p^{-f}\right\}. \tag{6.18}$$

We have

$$\chi(\sigma, t) \equiv \sum_{k=1}^{t} \sigma^k = \begin{cases} t & (\sigma = 1), \\ 0 & (\sigma = -1, t \text{ even}), \\ -1 & (\sigma = -1, t \text{ odd}). \end{cases} \tag{6.19}$$

(6.19) holds also in case $t=0$ since $\chi(\sigma, 0)=0$ for either $\sigma=1$ or $\sigma=-1$. Substituting in (6.18) and simplifying, we obtain

THEOREM 10. *If ρ, α_1, α_2, t are as defined in Theorem 9, then the number of solutions $\psi_2(\rho)$ of*

$$\rho \equiv \alpha_1\xi_1^2 + \alpha_2\xi_2^2 \pmod{P^\lambda} \tag{6.20}$$

is given by

$$\psi_2(\rho) = p^{f\lambda} + p^{f(\lambda-1)}\{(p^f - 1)\chi(\sigma, t) - \sigma\eta(t)\}, \tag{6.21}$$

where σ and η have the same meaning as in Theorem 9 and $\chi(\sigma, t)$ is defined by (6.19).

We point out finally the close analogy between Theorem 9 and the corresponding result [6, Theorem 8] for $GF[p^n, x]$.

7. **Sums of an odd number of squares.** Suppose $(\alpha, P)=1$. Then we have:

LEMMA 14. *If P is an odd prime ideal, then α is a quadratic residue* (mod P^λ), $\lambda \geqq 1$, *if and only if α is a quadratic residue* (mod P). *The number of solutions of*

$$\xi^2 \equiv \alpha \pmod{P^\lambda} \tag{7.1}$$

is

$$1 + \left(\frac{\alpha}{P}\right).$$

This is an extension of a familiar result in rational number theory [12, (8.4.2)], and is contained in a result of Klotz (§8, Corollary 8). It implies that the number of quadratic residues (mod P^λ) is equal to the number of non-residues.

A second lemma, of importance in this section, is concerned with the function

$$T'(\rho, P^k) = T(\rho, P^k) - R(\rho, P^k) \tag{7.2}$$

where R and T were defined by (3.3) and (5.7) respectively. Recalling the definition of ρ, μ, t in (5.23), we have

LEMMA 15. *If $k \geqq 1$,*

$$T'(\rho, P^k) = \begin{cases} p^{f(k-1)}S(\mu, P) & (t = k-1), \\ 0 & (t \neq k-1). \end{cases} \tag{7.3}$$

Proof. This result follows immediately from (4.1) and (5.27).

Before stating Theorem 11 let us introduce some more notation:

$$L(t) = \begin{cases} 1 & (t \text{ odd}, \lambda > t), \\ 0 & (\text{otherwise}); \end{cases} \tag{7.4}$$

$$L'(t) = \begin{cases} 1 & (t \text{ even}, \lambda > t), \\ 0 & (\text{otherwise}); \end{cases} \tag{7.5}$$

$$t = \begin{cases} 2r & (t \text{ even}), \\ 2r+1 & (t \text{ odd}); \end{cases} \tag{7.6}$$

$$\tau = \left(\frac{(-1)^m \mu \alpha_1 \cdots \alpha_{2m+1}}{P}\right) \tag{7.7}$$

where μ is defined by (5.23);

$$\Lambda(r) = (1 - p^f)\left(\frac{1 - p^{fr(2m-1)}}{1 - p^{f(2m-1)}}\right), \quad \omega = t^{f(2\lambda m - 2rm + r)}. \tag{7.8}$$

We now prove

THEOREM 11. *If P, ρ, $\alpha_1, \cdots, \alpha_{2m+1}$, t are as defined in Theorem 9, then the number of incongruent solutions* (mod P^λ) *of*

$$\rho \equiv \alpha_1 \xi_1^2 + \cdots + \alpha_{2m+1}\xi_{2m+1}^2 \pmod{P^\lambda} \tag{7.9}$$

is given, for all $m \geqq 0$, by

$$\psi_{2m+1}(\rho) = p^{2m\lambda f} - \omega\{p^{-f}\Lambda(r) + p^{-2mf}L(t) - p^{-mf}\tau L'(t)\}. \tag{7.10}$$

Proof. Formula (6.10) with $s = 2m+1$ gives the number of solutions of (7.9). Making this substitution in (6.10) we get

$$\psi_{2m+1}(\rho) = p^{2mf\lambda}\left\{1 + \sum_{k=1}^{\lambda} p^{-fk(2m+1)}\left(\frac{-\alpha_1 \cdots \alpha_s}{P^k}\right)(S(1, P^k))^{2m+1} \cdot \sum_{\gamma \pmod{P^k}, (\gamma, P)=1} \left(\frac{\gamma}{P^k}\right)\epsilon_{\gamma,\zeta_k}(\rho)\right\}. \tag{7.11}$$

Applying (5.13), (7.11) becomes

$$\psi_{2m+1}(\rho) = p^{2mf\lambda}\left\{1 + \sum_{k=1}^{\lambda} \sigma^k p^{-fk(m+1)}S(1, P^k) \cdot \sum_{\gamma \pmod{P^k}, (\gamma, P)=1} \left(\frac{\gamma}{P^k}\right)\epsilon_{\gamma,\zeta_k}(\rho)\right\}, \tag{7.12}$$

where σ is defined by (6.1).

Now let us consider the γ sum appearing in (7.12):

$$Q(\rho, P^k) \equiv \sum_{\gamma \pmod{P^k},(\gamma,P)=1} \left(\frac{\gamma}{P^k}\right) \epsilon_{\gamma,\zeta_k}(\rho). \tag{7.13}$$

By the definition of R_A, (3.3), we have

$$Q(\rho, P^k) = R(\rho, P^k), \qquad (k \text{ even}). \tag{7.14}$$

Further, by Lemma 14,

$$Q(\rho, P^k) = \sum_{\gamma_1} \epsilon_{\gamma_1,\zeta_k}(\rho) - \sum_{\gamma_2} \epsilon_{\gamma_2,\zeta_k}(\rho), \qquad (k \text{ odd}), \tag{7.15}$$

where the first summation is over a complete set of quadratic residues (mod P^k), γ_1, and the second summation is over a complete set of quadratic nonresidues, γ_2. Adding and subtracting $\sum \epsilon_{\gamma_1}$ simultaneously in (7.15), we have

$$Q(\rho, P^k) = 2\sum_{\gamma_1} \epsilon_{\gamma_1,\zeta_k}(\rho) - \sum_{\gamma \pmod{P^k},(\gamma,P)=1} \epsilon_{\gamma,\zeta_k}(\rho), \tag{7.16}$$

and applying Lemma 14 to (7.16), it follows that

$$Q(\rho, P^k) = T(\rho, P^k) - R(\rho, P^k) = T'(\rho, P^k), \qquad (k \text{ odd}). \tag{7.17}$$

Substituting (7.13), (7.14), (7.17) in (7.12) one finds

$$\begin{aligned}\psi_{2m+1}(\rho) = p^{2mf\lambda}\Bigg\{1 &+ \sum_{k=1(k \text{ even})}^{\lambda} p^{-fk(m+1)} S(1, P^k) R(\rho, P^k) \\ &+ \sum_{k=1(k \text{ odd})}^{\lambda} \sigma p^{-fk(m+1)} S(1, P^k) T'(\rho, P^k)\Bigg\},\end{aligned} \tag{7.18}$$

$$\psi_{2m+1}(\rho) = p^{2mf\lambda}(1 + \textstyle\sum_1 + \sum_2), \tag{7.19}$$

where $\sum_1$ and $\sum_2$ represent the first and second sums respectively in (7.18). We rewrite $\sum_1$, adopting, as usual, the convention that a vacuous sum is zero:

$$\sum_1 = \sum_{j=1}^{[\lambda/2]} p^{-2fj(m+1)} S(1, P^{2j}) R(\rho, P^{2j}), \tag{7.20}$$

where $[\lambda/2]$ denotes the greatest integer $\leqq \lambda/2$, and by (4.1),

$$\begin{aligned}\sum_1 = \sum_{j=1}^{r} p^{-2fj(m+1)} S(1, P^{2j}) R(\rho, P^{2j}) + L(l) p^{-2f(r+1)(m+1)} \\ \cdot S(1, P^{2r+2}) R(\rho, P^{2r+2}).\end{aligned} \tag{7.21}$$

We may evaluate (7.21), using (4.1) and (5.11):

$$\sum_1 = (1 - p^{-f}) \sum_{j=1}^{r} p^{jf(1-2m)} - L(t)p^{f(r-2rm-2m)},$$

and summing the progression,

$$\sum_1 = - p^{f(r-2rm)} \{ p^{-f}\Lambda(r) + p^{-2mf}L(t) \}. \tag{7.22}$$

(Observe that (7.22) still holds for the vacuous case in (7.21), namely the case $r=0$, since $\Lambda(0)=0$.)

We note by Lemma 15 and (7.18) that the only case which need be considered in the sum $\sum_2$ is the case $k=t+1$, $t<\lambda$, $t=2r$. One thus obtains by (7.5),

$$\sum_2 = L'(t)\sigma p^{-f(t+1)(m+1)}S(1, P^{t+1})T'(\rho, P^{t+1}), \tag{7.23}$$

which gives, on applying (5.11) and (7.3),

$$\begin{aligned} \sum_2 &= L'(t)\sigma p^{-f(t+1)(m+1)} p^{ft/2} S(1, P) \cdot p^{ft} S(\mu, P) \\ &= L'(t)\sigma \left(\frac{\mu}{P}\right) p^{-f(tm-t/2+m+1)} S^2(1, P). \end{aligned}$$

With $t=2r$, we apply (5.13), (6.1), and (7.7) to get

$$\sum_2 = L'(t)\tau p^{f(r-2rm-m)}. \tag{7.24}$$

Substitution of (7.22) and (7.24) in (7.19) leads immediately to the theorem.

REMARK 2. In the definition of ρ as a representative element in the ring $R(P^k)$, (5.23), we note that the exponent t of θ is uniquely determined. The unit multiple μ, $\mu \in R(P^k)$, $(\mu, P)=1$, is not, however, in general unique. If we have two such representations of ρ,

$$\rho \equiv \theta^t \mu_1 \equiv \theta^t \mu_2 \pmod{P^k},$$

then it follows, for $t<k$, that $\mu_1 \equiv \mu_2 \pmod{P}$. Thus the quadratic character of $\mu \pmod{P}$ is independent of the choice of μ in the representation (5.23) of ρ. Hence the character τ in (7.7) is well-defined in spite of the lack of uniqueness in the choice of μ. (For a discussion of the multiplicative representations of elements in more general rings, including $R(P^k)$ as a special case, see [11].)

8. **Special cases and sums of two and three squares.** This section consists of three parts. First we make a few brief remarks on quadratic congruences in the rational case. Second we derive, as special cases of Theorems 10 and 11, some Waring type results for sums of squares modulo an ideal (Theorems 12 and 13). Third, we derive certain results which serve to verify the main results in §§6, 7. These special cases are contained in Corollaries 5 ($s=1$, $m=0$), 6 ($\lambda=1$), 7, and 8 ($t=0$, $(\rho, P)=1$).

The problem of finding the number of representations of a rational integer n in the form

$$n \equiv a_1x_1^2 + \cdots + a_sx_s^2 \pmod{p^\lambda} \qquad (a_i \text{ rational}) \tag{8.1}$$

where $(a_i, p)=1$, p an odd prime, was discussed by Minkowski [18, §§4, 5] who gave exact formulas in case $(n, p)=1$ (Corollary 8). We may find explicit formulas for (8.1) simply by specializing F to the rational case in formulas (6.6), (6.21), (7.10). This is accomplished by taking $f=1$ in each formula and specifying μ in the following manner: Choose n positive, $n \leqq p^\lambda$, and place $n=p^tg$, $g=\mu$ ($(g, p)=1$ if $t<\lambda$, and $g=1$ if $t=\lambda$). The case $\lambda=1$ was treated by Jordan (see Corollary 6).

The cases of two and three squares yield quite simple results. Specialization to the case $s=3$, $m=1$, in Theorem 11 gives

COROLLARY 1. *The number of solutions of*

$$\rho \equiv \alpha_1\xi_1^2 + \alpha_2\xi_2^2 + \alpha_3\xi_3^2 \pmod{P^\lambda} \tag{8.2}$$

is given by

$$\psi_3(\rho) = p^{2\lambda f}\{1 + p^{-f} + p^{-f(r+1)}(\tau L'(t) - 1) - L(t)p^{-f(r+2)}\}, \tag{8.3}$$

where the quantities t, r, τ, L, L' are defined as in Theorem 11.

The result in (8.3) may be stated explicitly by considering the subcases arising from different values of t and τ:

COROLLARY 2. *The number of solutions of* (8.2) *is given by*

$$\psi_3(\rho) = \begin{cases} p^{2\lambda f}(1 + p^{-f})(1 - p^{-f(r+1)}) & (\lambda > t,\ t \text{ odd}), \\ p^{2\lambda f}(1 + p^{-f}) & (\lambda > t,\ t \text{ even},\ \tau = 1), \\ p^{2\lambda f}(1 + p^{-f} - 2p^{-f(r+1)}) & (\lambda > t,\ t \text{ even},\ \tau = -1), \\ p^{2\lambda f}(1 + p^{-f} - p^{-f(r+1)}) & (\lambda = t \text{ or } \rho = 0). \end{cases} \tag{8.4}$$

Specializing in the same way in Theorem 10, we obtain a corresponding result for sums of two squares:

COROLLARY 3. *The number of solutions of* (6.20) *is given by*

$$\psi_2(\rho) = \begin{cases} p^{f\lambda}(1 + \lambda - \lambda p^{-f}) & (t = \lambda,\ \sigma = 1), \\ p^{f\lambda} & (t = \lambda,\ \sigma = -1,\ \lambda \text{ even}), \\ p^{f(\lambda-1)} & (t = \lambda,\ \sigma = -1,\ \lambda \text{ odd}), \\ p^{f\lambda}(1 - p^{-f})(t + 1) & (t < \lambda,\ \sigma = 1), \\ p^{f\lambda}(1 + p^{-f}) & (t < \lambda,\ \sigma = -1,\ t \text{ even}), \\ 0 & (t < \lambda,\ \sigma = -1,\ t \text{ odd}), \end{cases} \tag{8.5}$$

σ being defined by (6.1).

Inspection of (8.4) reveals immediately that $\psi_3 > 0$ in all cases. Thus we have, on the basis of Lemma 13:

THEOREM 12. *If A is an arbitrary odd ideal, and if α_1, α_2, α_3 are algebraic integers prime to A, then every integer ρ is expressible as a sum of three squares,*

$$\rho \equiv \alpha_1\xi_1^2 + \alpha_2\xi_2^2 + \alpha_3\xi_3^2 \pmod{A}.$$

That every integer ρ is *not* necessarily expressible as a sum of two squares (mod A) follows by inspection of (8.5). In this case we may deduce the following explicit criterion:

THEOREM 13. *If A is an ideal with the prime power factorization $A = P_1^{\lambda_1} \cdots P_h^{\lambda_h}$, and if α_1, α_2 are integers prime to A, then an integer ρ is not representable as a sum of two squares,*

$$\rho \equiv \alpha_1\xi_1^2 + \alpha_2\xi_2^2 \pmod{A}, \qquad (A \text{ odd}), \tag{8.6}$$

if and only if, for at least one P_i, $\rho \equiv 0 \pmod{P_i}$, with the additional restrictions that the maximum exponent t_i to which P_i divides ρ is odd and $< \lambda_i$, and $-\alpha_1\alpha_2$ is a quadratic nonresidue (mod P_i).

As a consequence of this theorem we obtain

COROLLARY 4. *A necessary and sufficient condition that* (8.6) *be solvable for arbitrary ρ and for all α_1, α_2 prime to A is that A should be a product of distinct prime ideals.*

As a means of checking Theorem 11 in the case $m = 0$, we prove independently

LEMMA 16. *The number of solutions of*

$$\rho \equiv \xi^2 \pmod{P^\lambda} \tag{8.7}$$

is given by

$$\psi_1(\rho) = \begin{cases} p^{t}r & (t = \lambda), \\ 2p^{t}r & (t < \lambda,\ t \text{ even},\ \tau = 1), \\ 0 & (\text{otherwise}), \end{cases} \tag{8.8}$$

the quantities t, r, τ being defined as in Theorem 11.

Proof. Case 1 ($t = \lambda$). Here we consider

$$\xi^2 \equiv 0 \pmod{P^\lambda}; \tag{8.9}$$

by (5.23) any ξ satisfying (8.9) is of the form $\xi = \nu\theta^i$, $(\nu, P) = 1$, $g \leqq i \leqq \lambda$, $g = r$ or $r+1$ according as $\lambda = 2r$ or $2r+1$. By the remark at the end of §7, if we let ν range over all $\nu \in R(P^\lambda)$ such that $(\nu, P) = 1$, then repetitions may arise. However, by Lemma 2, if ν ranges over a reduced residue system

(mod $P^{\lambda-i}$) in $\nu\theta^i$ ($i=g, \cdots, \lambda$), then all elements obtained are distinct and exhaust the possibilities for ξ. Thus the number of ξ satisfying (8.9) is given by $\Lambda(P^{\lambda-g}) = p^{f(\lambda-g)} = p^{rf}$, using (3.4).

Case 2 ($t<\lambda$, t even, $\tau=1$). In this case, by (5.23), one may take $\rho=\theta^{2r}\mu$, $t=2r$, $(\mu, P)=1$, $\tau=(\mu/P)=1$. We consider then

$$\rho = \theta^{2r}\mu \equiv \xi^2 \pmod{P^\lambda}. \tag{8.10}$$

But ξ is necessarily of the form $\theta^r\nu$, $(\nu, P)=1$, so that (8.10) gives $\theta^{2r}(\mu-\nu^2) \equiv 0 \pmod{P^\lambda}$ or

$$\nu^2 \equiv \mu \pmod{P^{\lambda-2r}}. \tag{8.11}$$

Now (8.11) has two solutions (mod $P^{\lambda-2r}$) by Lemma 14. We want the number of solutions $\xi_i=\theta^r\nu_i$ of (8.10), incongruent (mod P^λ). But

$$\theta^r\nu_1 \equiv \theta^r\nu_2 \pmod{P^\lambda} \rightleftarrows \nu_1 \equiv \nu_2 \pmod{P^{\lambda-r}};$$

thus there is a 1-1 correspondence between the ξ_i satisfying (8.10) and the ν_i (mod $P^{\lambda-r}$) satisfying (8.11). Since there are $N(P^r)=p^{fr}$ residue systems (mod $P^{\lambda-2r}$) contained in a complete residue system (mod $P^{\lambda-r}$), it follows that each solution ν of (8.11) gives rise to p^{fr} distinct ν_i (mod $P^{\lambda-r}$). This proves Case 2.

Case 3($t<\lambda$ and t odd or $\tau=-1$). These cases are obviously insolvable.

One may specialize Theorem 11 to the case $m=0$ to get

COROLLARY 5. *The number of solutions $\psi_1(\rho)$ of* (8.7) *is given by*

$$\psi_1(\rho) = p^{fr}\left\{1 - L(t) + \left(\frac{\mu}{P}\right)L'(t)\right\}, \tag{8.12}$$

where r, L, L', μ have the usual meaning of §7.

This result checks with (8.8).

As a second verification of the results in the two previous sections, we consider the case of sums of squares in a Galois field $GF(p^n)$. This problem was solved, in the case $n=1$, by Jordan [15, Nos. 197–200] and later for arbitrary n by Dickson [9, §§64–66]. We put $\lambda=1$ in Theorems 9, 10, 11, to get

COROLLARY 6. (JORDAN-DICKSON). *If $GF(p^f)$ is a Galois field isomorphic with $R(P)$, if $\alpha_1, \cdots, \alpha_s$ are nonzero elements of $GF(p^f)$, and if $\rho \in GF(p^f)$ is arbitrary, then the number of solutions $\Phi_s(\rho)$ of*

$$\rho = \alpha_1\xi_1^2 + \cdots + \alpha_s\xi_s^2 \tag{8.13}$$

in $GF(p^f)$ is given, in case $s=2m$, by

$$\Phi_{2m}(\rho) = \begin{cases} p^{f(2m-1)} - \sigma p^{f(m-1)} & (\rho \neq 0), \\ p^{f(2m-1)} + \sigma(p^{fm} - p^{f(m-1)}) & (\rho = 0), \end{cases} \tag{8.14}$$

where $\sigma = 1$ *or* -1 *according as* $(-1)^m\alpha_1 \cdots \alpha_{2m}$ *is or is not a square of the field; in case* $s = 2m+1$,

$$\Phi_{2m+1}(\rho) = \begin{cases} p^{2mf} + \tau p^{mf} & (\rho \neq 0), \\ p^{2mf} & (\rho = 0), \end{cases} \tag{8.15}$$

where $\tau = +1$ *or* -1 *according as* $(-1)^{m-1}\rho\alpha_1 \cdots \alpha_{2m+1}$ *is or is not a square of the field.*

For a generalization of this corollary to the case of polynomials in a Galois field see [4, Theorem 10; 5, Theorem 2] and for a second generalization in case $s = 2m$ [6, Theorem 8].

By taking $t = 0$ in (6.6) and (7.10) we get formulas for the case $(\rho, P) = 1$:

COROLLARY 7. *If* $\alpha_1, \cdots, \alpha_s$ *are integers prime to* P, *then the number of solutions* $\psi_s^\lambda(\rho)$ *of*

$$\rho \equiv \alpha_1\xi_1^2 + \cdots + \alpha_s\xi_s^2 \pmod{P^\lambda}, \qquad (\rho, P) = 1, \tag{8.16}$$

is given by

$$\psi_s^\lambda(\rho) = \begin{cases} p^{f\lambda(2m-1)} - \sigma p^{f(2m\lambda-\lambda-m)} & (s = 2m), \\ p^{2m\lambda f} + \tau p^{mf(2\lambda-1)} & (s = 2m+1), \end{cases} \tag{8.17}$$

where σ *and* τ *are defined by* (6.1) *and* (7.7) *respectively.*

The solution of the problem in (8.16) was given by Minkowski [18, §4] in the rational case, while a generalization to algebraic fields was carried out by Klotz [16, p. 255]. Their formulas were given in the implicit form of the following corollary, which one may verify with no trouble by (8.14), (8.15), and (8.17):

COROLLARY 8 (MINKOWSKI-KLOTZ). *If* $\psi_s^\lambda(\rho)$ *represents the number of solutions of* (8.16), *then*

$$\psi_s^\lambda(\rho) = p^{f(\lambda-1)(s-1)}\psi_s^1(\rho). \tag{8.18}$$

BIBLIOGRAPHY

1. L. Carlitz, *The singular series for sums of squares of polynomials*, Duke Math. J. vol. 14 (1947) pp. 1105–1120.

2. ———, *Representations of arithmetic functions in* $GF[p^n, x]$, Duke Math. J. vol. 14 (1947) pp. 1121–1137.

3. R. D. Carmichael, *Expansions of arithmetical functions in infinite series*, Proc. London Math. Soc. (2) vol. 34 (1932) pp. 1–26.

4. Eckford Cohen, *Sums of an even number of squares in* $GF[p^n, x]$, II, Duke Math. J. vol. 14 (1947) pp. 543–557.

5. ———, *Sums of an odd number of squares in* $GF[p^n, x]$, Duke Math. J. vol. 15 (1948) pp. 501–511.

6. ———, *Rings of arithmetic functions*, Duke Math. J. vol. 19 (1952) pp. 115–129.

7. ———, *Sur les fonctions arithmétiques relatives aux corps algébriques*, C. R. Acad. Sci. Paris vol. 234 (1952) pp. 787–788.

8. ———, *A finite analog of the Goldbach problem*, not yet published.

9. Leonard Eugene Dickson, *Linear groups*, Leipzig, 1901.

10. ———, *Algebras and their arithmetics*, Chicago, 1923.

11. A. A. Fraenkel, *Über die Teiler der Null und die Zerlegung von Ringen*, J. Reine Angew. Math. vol. 145 (1914) pp. 139–176.

12. G. H. Hardy and E. M. Wright, *Introduction to the theory of numbers*, Oxford, 1938.

13. Helmut Hasse, *Vorlesungen über Zahlentheorie*, Berlin, 1950.

14. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, 1923.

15. Camille Jordan, *Traité des substitutions*, Paris, 1870.

16. Jakob Klotz, *Anzahl der Lösungen einer quadratischen Kongruenz in einem beliebigen endlichen algebraischen Zahlkörper*, Vierteljahrschrift der Naturforschende Gesellschaft in Zürich vol. 58 (1913) pp. 239–268.

17. Edmund Landau, *Vorlesungen über Zahlentheorie*, vol. I, Leipzig, 1927.

18. Hermann Minkowski, *Untersuchungen über quadratische Formen*, Acta Math. vol. 7 (1885) pp. 201–258.

19. Oystein Ore, *Les corps algébriques et la théorie des idéaux*, Paris, 1934.

20. Hans Rademacher, *Zur additive Primzahltheorie algebraischer Zahlkörper*, III, Math. Zeit. vol. 27 (1928) pp. 319–426.

21. Carl Ludwig Siegel, *Additive Theorie der Zahlkörper*, II, Math. Ann. vol. 88 (1923) pp. 184–210.

22. ———, *Sums of mth powers of algebraic integers*, Ann. of Math. vol. 46 (1945) pp. 313–339.

23. Albert Leon Whiteman, *Additive prime number theory in real quadratic fields*, Duke Math. J. vol. 7 (1940) pp. 208–232.

The Institute for Advanced Study,
Princeton, N. J.