CONGRUENCES IN ALGEBRAIC NUMBER FIELDS INVOLVING SUMS OF SIMILAR POWERS

BY

ECKFORD COHEN

1. Introduction. Suppose F to be a finite extension of the rational field and let P denote a prime ideal of F of norm $N(P)=p^f$ where p is a rational prime. We shall be concerned in this paper with the number of solutions $Q_s(\rho)$ of the congruence

$$\alpha_1 X_1^m + \cdots + \alpha_s X_s^m + \rho \equiv 0 \pmod{P^\lambda}, \tag{1.1}$$

where ρ is an arbitrary integer of F, λ is a positive integer, $\alpha_1, \cdots, \alpha_s$ are integers of F prime to P, and in addition the following conditions are satisfied:

$$(m, p) = 1, \qquad k = (m, p^f - 1) > 1. \tag{1.2}$$

Choose an ideal C of F such that $(P, C)=1$ and $PC=\theta$ is principal. We may suppose the integer ρ to be of the form

$$\rho = \theta^t \xi \qquad (\lambda \geqq t \geqq 0, (\xi, P) = 1), \tag{1.3}$$

where t is uniquely determined, and ξ is uniquely determined (mod P) if $t \neq \lambda$.

We discuss briefly the main results of the paper. An exact formula for $Q_s(\rho)$ involving the generalized Jacobi sum (2.9) is obtained in Theorem 1 (§3). This formula, which is rather complicated, simplifies considerably in the component cases (1) $\lambda > t \equiv 0 \pmod{m}$, (2) $\lambda > t \not\equiv 0 \pmod{m}$, and (3) $\lambda = t$. The results for $Q_s(\rho)$ in these cases are given in §4 in Theorems 2, 3, and 4 respectively. Explicit formulas for the case $s=1$ are listed in Theorem 5. In the final section (§5) estimates for $Q_s(\rho)$ are obtained (Theorems 6 and 7) and solvability criteria for the congruence (1.1) are deduced (Theorems 8 and 9). As a consequence of these results, it is proved that (1.1) is solvable in the case $s=3$ for all P of sufficiently large norm. The precise statement of this result is contained in Theorem 10.

The method employed in this paper is based on the theory of exponential sums in algebraic number fields. In this method the Hecke sums (2.5) and the generalized Gauss-Lagrange sums (2.6) are of particular importance. The most useful results involving these sums are collected in §2 in a series of preliminary lemmas.

We mention that results in the special case of binary congruences ($s=2$) have already appeared in a separate publication [2]. Since these results are corollaries of theorems proved in the present paper, we do not take the space

Presented to the Society, February 26, 1955; received by the editors February 10, 1956.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

to restate them here. The special case of quadratic congruences ($m=2$) was treated in detail in a previous paper [1]. The latter article forms the principal foundation for the method of the present paper.

The special case $\lambda=1$, that is, the case of congruences to a prime ideal modulus, may be stated equivalently as a problem concerning equations in a Galois field $GF(p^f)$. This problem has attracted considerable attention, and we cite, in particular, papers of Davenport and Hasse [3], Hua and Vandiver [4], and Weil [6]. Earlier references can be found in the bibliographies to these papers.

2. **Preliminary lemmas.** We introduce first a notation for exponentials in F which is somewhat simpler than that used in [1]. Let D represent the ideal different in F and choose B, $(B, P)=1$, so that $\zeta=B/P^{\lambda}D$ is principal. We place $\zeta_n=\zeta\theta^{\lambda-n}$ $(0\leqq n\leqq\lambda)$ so that $\zeta=\zeta_{\lambda}$, and define further

$$e_n(\rho) = e^{2\pi i \operatorname{tr}(\rho\zeta_n)}, \qquad (e(\rho)=e_1(\rho)), \tag{2.1}$$

where the symbol tr (γ) denotes the trace in F. The function $e_n(\rho)$ defines an additive character (mod P^n) and has the simple properties: $e_0(\rho)=1$, $e_n(\rho)=e_n(\rho')$ if $\rho\equiv\rho'$ (mod P^n), $e_n(\alpha+\beta)=e_n(\alpha)e_n(\beta)$. In addition, we have the fundamental relations,

$$e_n(\rho\theta^j) = e_{n-j}(\rho) \qquad (0\leqq j\leqq n), \tag{2.2}$$

$$\sum_{z(\bmod P^n)} e_n(\rho z) = \begin{cases} p^{fn} \text{ if } \rho\equiv 0 \pmod{P^n} \\ 0 \text{ otherwise.} \end{cases} \tag{2.3}$$

We denote by χ a fixed, primitive kth power character (mod P) and let χ_0 represent the principal character (mod P). As a multiplicative character, χ^h has the properties, $\chi^h(\alpha\beta)=\chi^h(\alpha)\chi^h(\beta)$, and for $n\geqq 1$,

$$\sum_{(a,P^n)=1} \chi^h(a) = \begin{cases} p^{f(n-1)}(p^f-1) & (\chi^h=\chi_0), \\ 0 & (\chi^h\neq\chi_0), \end{cases} \tag{2.4}$$

where the summation is over a reduced residue system (mod P^n).

The Hecke sum (mod P^n), $\lambda\geqq n\geqq 0$, is defined by

$$S_n(\rho, m) = \sum_{z(\bmod P^n)} e_n(\rho z^m), \qquad (S(\rho, m)=S_1(\rho, m)). \tag{2.5}$$

The generalized Gauss-Lagrange sum (mod P^n) corresponding to the character χ^h is defined for $\lambda\geqq n\geqq 1$ by

$$\tau_n(\chi^h, \rho) = \sum_{(a,P^n)=1} \chi^h(a)e_n(\rho a). \tag{2.6}$$

We also use the abbreviated notation

$$\tau(\chi^h, \rho) = \tau_1(\chi^h, \rho), \qquad \tau(\chi^h) = \tau(\chi^h, 1), \tag{2.7}$$

and in the case $\chi^h=\chi_0$, the special notation [1, §3],

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

$$R_n(\rho) = \tau_n(\chi_0, \rho) = \sum_{(a,P^n)=1} e_n(\rho a). \tag{2.8}$$

The generalized Jacobi sum (mod P) is defined for $r \geqq 1$ and for characters $\chi^{h_1}, \cdots, \chi^{h_r}$ by (cf. [5, (7a)])

$$\psi(h_1, \cdots, h_r) = \sum_{v_1+\cdots+v_r+1\equiv 0 \,(\mathrm{mod}\ P)} \chi^{h_1}(v_1) \cdots \chi^{h_r}(v_r), \tag{2.9}$$

the sum being over v_i $(i=1, \cdots, r)$ in a reduced residue system (mod P) such that $v_1+\cdots+v_r+1 \equiv 0$ (mod P).

We next state a number of lemmas concerning the Hecke and generalized Gauss-Lagrange sums, most of which are familiar in one form or another. These results are listed without proof except for Lemmas 3 and 9.

LEMMA 1. *If* $n \geqq j \geqq 0$, *then*

$$S_n(\rho\theta^j, m) = p^{fj} S_{n-j}(\rho, m). \tag{2.10}$$

LEMMA 2. *If* $k = (m, p^f-1)$, *then*

$$S(\rho, m) = S(\rho, k). \tag{2.11}$$

LEMMA 3. *If* $(\nu, P)=1$, $m > i \geqq 0$, $j \geqq 0$, $m > 1$, $(m, p)=1$, *then*

$$S_{mj+i}(\nu, m) = \begin{cases} p^{fj(m-1)} & (i=0), \\ p^{fj(m-1)} S(\nu, m) & (i=1), \\ p^{f(jm-j+i-1)} & (i>1). \end{cases} \tag{2.12}$$

Proof. We may exclude the two cases $j=0$, $i=0$, and $j=0$, $i=1$, because in these cases the lemma is clearly true. Now the set $z = y + x\theta^{mj+i-1}, x$ (mod P), y (mod P^{mj+i-1}) furnishes a complete residue system (mod P^{mj+i}). Using this set in the summation involved in the definition of $S_{mj+i}(\nu, m)$, one obtains by (2.2) and the additive property of $e_n(\rho)$,

$$S_{mj+i}(\nu, m) = \sum_{y \,(\mathrm{mod}\ P^{mj+i-1})} e_{mj+i}(\nu y^m) \sum_{x \,(\mathrm{mod}\ P)} e(\nu m x y^{m-1}).$$

By (2.3) the inner sum $=0$ unless $P \mid y$, in which case it has the value p^f. Hence we obtain, placing $y = Y\theta$, Y (mod P^{mj+i-2}) and simplifying,

$$S_{mj+i}(\nu, m) = \begin{cases} p^{f(m-1)} S_{m(j-1)+i}(\nu, m) & (j>0), \\ p^{f(i-1)} & (j=0,\ i \geqq 2). \end{cases} \tag{2.13}$$

This proves the lemma in case $j=0$. If $j>0$, we may repeat the process j times to obtain the relation,

$$S_{mj+i}(\nu, m) = p^{fj(m-1)} S_i(\nu, m), \tag{2.14}$$

which reduces the general case to the case $j=0$. The Lemma follows from (2.13) and (2.14).

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

LEMMA 4. *If* $(\nu, P)=1$, $k>1$, *then*

$$S(\nu, k) = \sum_{i=1}^{k-1} \tau(\chi^i, \nu). \tag{2.15}$$

LEMMA 5. *If* $(\nu, P)=1$, *then*

$$\tau(\chi^h, \nu) = \bar{\chi}^h(\nu)\tau(\chi^h). \tag{2.16}$$

LEMMA 6. *If* $\chi^h \neq \chi_0$, *then*

$$\tau(\chi^h)\tau(\bar{\chi}^h) = \chi^h(-1)p^f. \tag{2.17}$$

By Lemmas 5 and 6 one may deduce easily

LEMMA 7. *If* $\chi^h \neq \chi_0$ *and* $(\nu, P)=1$, *then*

$$\left|\tau(\chi^h)\right| = p^{f/2}. \tag{2.18}$$

LEMMA 8. *If* $r>0$, $h_1+\cdots+h_{r+1}\equiv 0 \pmod{k}$, $h_i \not\equiv 0 \pmod{k}$, $i=1, \cdots, r+1$, *then*

$$\tau(\chi^{h_1})\cdots\tau(\chi^{h_{r+1}}) = p^f\psi(h_1, \cdots, h_r). \tag{2.19}$$

LEMMA 9. *If* $\chi^h \neq \chi_0$, *and if* $\rho=\theta^l\nu$, $n\geqq 1$, $n\geqq l\geqq 0$, $(\nu, P)=1$, *then*

$$\tau_n(\chi^h, \rho) = \begin{cases} p^{f(n-1)}\tau(\chi^h, \nu) & (l = n-1), \\ 0 & (\textit{otherwise}). \end{cases} \tag{2.20}$$

Proof. If $l=n$, we have by (2.4)

$$\tau_n(\chi^h, \rho) = \sum_{(a, P^n)=1} \chi^h(a) = 0, \qquad (l = n).$$

In the rest of the proof we may suppose then that $l\leqq n-1$. Since there are p^{fl} reduced residue systems (mod P^{n-l}) contained in a reduced residue system (mod P^n), one obtains by (2.2),

$$\tau_n(\chi^h, \rho) = p^{fl}\tau_{n-l}(\chi^h, \nu), \qquad (l \leqq n-1). \tag{2.21}$$

The relation (2.21) yields the lemma immediately in the case $l=n-1$. Suppose therefore that $l<n-1$. In this case a reduced residue system (mod P^{n-l}) is given by the set $a=a'+\theta u$, $(a', P)=1$, $u \pmod{P^{n-l-1}}$. Summing over this set in the definition of $\tau_{n-1}(\chi^h, \nu)$, (2.21) becomes

$$\tau_n(\chi^h, \rho) = p^{fl} \sum_{(a', P)=1} \chi^h(a')e_{n-l}(a'\nu) \sum_{u \,(\mathrm{mod}\, P^{n-l-1})} e_{n-l-1}(u\nu),$$

but the inner sum $=0$ by (2.3).

The analogue of Lemma 9 in the case $\chi^h=\chi_0$ is given by

LEMMA 10. *If* $n\geqq 1$ *and if* ρ *and* l *are defined as in Lemma* 9, *then*

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

$$R_n(\rho) = \begin{cases} p^{f(n-1)}(p^f - 1) & (l = n), \\ -p^{f(n-1)} & (l = n-1), \\ 0 & (l < n-1). \end{cases} \tag{2.22}$$

3. **The principal theorem.** In addition to the notation contained in (1.2) and (1.3) we require the notation given below. We shall also use the convention that a vacuous sum has the value 0.

If $h \geqq 0$, place

$$g(h) = \sum_{i=0}^{h-1} p^{f(m-s)i} = \begin{cases} \dfrac{p^{fh(m-s)} - 1}{p^{f(m-s)} - 1} & (m \neq s), \\ h & (m = s). \end{cases} \tag{3.1}$$

It is noted that $g(0) = 0$, $g(1) = 1$. With $i = 0, \cdots, m-1$, we define further

$$\delta_i = 0 \text{ or } 1 \text{ according as } i = 0 \text{ or } i \neq 0; \tag{3.2}$$

$$q_i = \left[\frac{\lambda - i}{m}\right], \qquad r_i = \left[\frac{t - i}{m}\right], \tag{3.3}$$

where the symbol $[x]$ denotes the largest integer $\leqq x$;

$$L_i(t) = \begin{cases} 1 & (\lambda > t \equiv i \pmod m), \\ 0 & (\text{otherwise}); \end{cases} \tag{3.4}$$

$$\phi(r_i) = (p^f - 1)g(r_i + \delta_i) - p^{f(m-s)(r_i+\delta_i)}L_{i-1}(t); \tag{3.5}$$

$$Z = p^{f(s-1)} + p^{f(m-2)}\phi(r_0) + \sum_{i=2}^{m-1} p^{f(i-2)}\phi(r_i). \tag{3.6}$$

We shall also need the following function defined for integers γ_i of F, $(\gamma_i, P) = 1$ $(i = 1, \cdots, r)$:

$$J(\gamma_1, \cdots, \gamma_r) = \sum_{h_i;(i=1,\cdots,r)} \chi(\gamma_1^{h_1} \cdots \gamma_r^{h_r})\psi(h_1, \cdots, h_r), \tag{3.7}$$

where the summation is over h_i satisfying $h_1 + \cdots + h_r \not\equiv 0 \pmod k$, $h_i \not\equiv 0 \pmod k$, $i = 1, \cdots, r$ $(r > 0)$. If $\alpha_1, \cdots, \alpha_s$ are integers of F prime to P, we define for γ, $(\gamma, P) = 1$,

$$J_r(\gamma) = \begin{cases} J\left(\dfrac{\gamma}{\alpha_1}, \cdots, \dfrac{\gamma}{\alpha_r}\right) & (s \geqq r \geqq 1), \\ 0 & (r = 0); \end{cases} \tag{3.8}$$

$$\eta_s = J_{s-1}(\alpha) \qquad (\alpha = \alpha_s). \tag{3.9}$$

Note that $\eta_1 = 0$.

On the basis of the above notation we now state the main theorem concerning $Q_s(\rho)$.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

THEOREM 1. *The number of solutions $Q_s(\rho)$ of the congruence* (1.1) *is given by*

$$Q_s(\rho) = p^{f(\lambda-1)(s-1)}\{p^{fr_0(m-s)}J_s(\xi)L_0(t) + \eta_s\phi(r_1) + Z\}. \tag{3.10}$$

Proof. The Fourier expansion [1, Theorem 2] of $Q_s(\rho)$ is given by

$$Q_s(\rho) = p^{-f\lambda}\sum_{u \pmod{P^\lambda}} e_\lambda(\rho u)S_\lambda(\alpha_1 u, m)\cdots S_\lambda(\alpha_s u, m).$$

In the summation $u \pmod{P^\lambda}$ we may place [1, Lemma 2] $u = v\theta^{\lambda-n}$, $0 \leqq n \leqq \lambda$, $(v, P^n) = 1$, to get on the basis of Lemma 1,

$$Q_s(\rho) = p^{f\lambda(s-1)}\sum_{m=0}^{\lambda} p^{-fns}\sum_{(v,P^n)=1} e_n(\rho v)S_n(\alpha_1 v, m)\cdots S_n(\alpha_s v, m).$$

We rewrite this summation in the form,

$$Q_s(\rho) = U_1 + U_2 + U_3, \tag{3.11}$$

where the outer summation in U_1 is over $n = mj+1$, in U_2 over $n = mj$, and in U_3 over $n = mj+i$ $(1 < i < m)$.

Applying Lemmas 2 and 3 and using the notation $w = p^{f(\lambda(s-1)-s)}$, one obtains

$$U_1 = w\sum_{j=0}^{q_1} p^{-fjs}\sum_{(v,P^{mj+1})=1} e_{mj+1}(\rho v)S(\alpha_1 v, k)\cdots S(\alpha_s v, k).$$

By Lemmas 4 and 5, it follows that

$$U_1 = w\sum_{j=0}^{q_1} p^{-fjs}\sum_{(v,P^{mj+1})=1} e_{mj+1}(\rho v)\prod_{i=1}^{s}\Big(\sum_{h_i=1}^{k-1}\bar{\chi}^{h_i}(\alpha_i v)\tau(\chi^{h_i})\Big).$$

This becomes, on rearranging and using the definition of τ_n,

$$U_1 = w\sum_{h_i=1;\,(i=1,\cdots,s)}^{k-1}\bar{\chi}(\alpha_1^{h_1}\cdots\alpha_s^{h_s})\tau(\chi^{h_1})\cdots\tau(\chi^{h_s})\sum_{j=0}^{q_1} p^{-fjs}\tau_{mj+1}(\bar{\chi}^h, \rho),$$

where $h = h_1 + \cdots h_s$. The h_i summations in U_1 will now be divided into two types according as

$$h \equiv 0 \pmod{k}, \qquad k > h_i \geqq 1, \tag{3.12}$$

or

$$h \not\equiv 0 \pmod{k}, \qquad k > h_i \geqq 1, \tag{3.13}$$

$i = 1, \cdots, s$. Summations of the first type will be indicated by the symbol $\sum'$ while summations of the second type will be denoted by $\sum''$. We may write therefore

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

$$U_1 = U_{11} + U_{12} \tag{3.14}$$

where U_{11} corresponds to summations satisfying (3.12) and U_{12} to those satisfying (3.13).

Application of Lemma 8 yields then, with $\alpha=\alpha_s$,

$$U_{11} = wp^f \sum_{h_1,\cdots,h_s}{}' \chi\left(\left(\frac{\alpha}{\alpha_1}\right)^{h_1}\cdots\left(\frac{\alpha}{\alpha_{s-1}}\right)^{h_{s-1}}\right)\psi(h_1,\cdots,h_{s-1})\sum_{j=0}^{q_1} p^{-fjs}R_{mj+1}(\rho)$$

if $s>1$, and $U_{11}=0$ if $s=1$. Applying Lemma 10 and the definitions of η_s and $\phi(r_1)$, we obtain for $s\geqq 1$,

$$U_{11} = p^{f(\lambda-1)(s-1)}\eta_s\phi(r_1). \tag{3.15}$$

By Lemma 9 we have for U_{12},

$$U_{12} = wp^{fr_0(m-s)} \sum_{h_1,\cdots,h_s}{}'' \bar{\chi}(\alpha_1^{h_1}\cdots\alpha_s^{h_s})\tau(\chi^{h_1})\cdots\tau(\chi^{h_s})\tau(\bar{\chi}^{h}, \xi)L_0(t).$$

Hence by Lemmas 5 and 8 and the definition of $J_s(\xi)$ it follows that

$$U_{12} = p^{f[(\lambda-1)(s-1)+r_0(m-s)]}J_s(\xi)L_0(t). \tag{3.16}$$

Returning to U_2 and using Lemma 3, one obtains

$$U_2 = p^{f\lambda(s-1)}\sum_{j=0}^{q_0} p^{-fjs}R_{mj}(\rho),$$

which becomes, on applying Lemma 10 and simplifying,

$$U_2 = p^{f(\lambda-1)(s-1)}(p^{f(m-2)}\phi(r_0) + p^{f(s-1)}). \tag{3.17}$$

In the case of U_3, we have again by Lemma 3,

$$U_3 = w\sum_{i=2}^{m-1}\sum_{j=0}^{q_i} p^{-fjs}R_{mj+i}(\rho),$$

and by Lemma 10 and simplification, it follows that

$$U_3 = p^{f(\lambda-1)(s-1)}\sum_{i=2}^{m-1} p^{f(i-2)}\phi(r_i). \tag{3.18}$$

Collecting (3.11), (3.14), (3.15), (3.16), (3.17), and (3.18), the theorem results.

4. **Component cases.** In this section we obtain simplifications of Theorem 1, by considering separately the three cases mentioned in the Introduction. The results obtained in these cases are direct corollaries of Theorem 1, and numerical details will therefore be omitted. We mention, however, the identity, $g(e+1)=g(e)+p^{fs(m-s)}$, which is useful in simplifying the calculations.

We need the additional notation

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

$$T(\eta_s) = (p^f - 1)\eta_s + p^{f(s-1)} - 1. \tag{4.1}$$

In the first case, $\lambda > t \equiv 0 \pmod{m}$, one obtains from Theorem 1, on simplifying,

THEOREM 2. *If* $\lambda > t = em$, *then*

$$Q_s(\rho) = p^{f(\lambda-1)(s-1)}\left\{p^{fe(m-s)}(J_s(\xi) + p^{f(s-1)} - \eta_s) + g(e)T(\eta_s)\right\}. \tag{4.2}$$

COROLLARY 2.1. *If* $t = 0$, *then*

$$Q_s(\rho) = p^{f(\lambda-1)(s-1)}(J_s(\xi) + p^{f(s-1)} - \eta_s). \tag{4.3}$$

In the second case, $\lambda > t \not\equiv 0 \pmod{m}$, Theorem 1 simplifies to give

THEOREM 3. *If* $\lambda > t = em + j$, $m > j > 0$, *then*

$$Q_s(\rho) = p^{f(\lambda-1)(s-1)}g(e+1)T(\eta_s). \tag{4.4}$$

COROLLARY 3.1 ($e = 0$). *If* $\lambda > t = j$, $m > j > 0$, *then*

$$Q_s(\rho) = p^{f(\lambda-1)(s-1)}T(\eta_s). \tag{4.5}$$

In the third case, $\lambda = t$, Theorem 1 reduces, on simplification, to

THEOREM 4 ($\rho = 0$). *If* $\lambda = t = em + j$, $m > j \geqq 0$, *then*

$$Q_s(\rho) = \begin{cases} p^{f(\lambda-1)(s-1)}(p^{f(em-es+j-1)} + g(e+1)T(\eta_s)) & \text{if } j > 0, \\ p^{f(\lambda-1)(s-1)}(p^{f(em-es+s-1)} + g(e)T(\eta_s)) & \text{if } j = 0. \end{cases} \tag{4.6}$$

As a final result in this section, we state explicit formulas for the case $s = 1$. In this connection, we note that $T(\eta_1) = 0$ and that ($\alpha = \alpha_1$)

$$J_1(\xi) = \begin{cases} k - 1 & \text{if } \chi(-\xi) = \chi(\alpha), \\ -1 & \text{if } \chi(-\xi) \neq \chi(\alpha). \end{cases} \tag{4.7}$$

Place $\beta = -\rho = \theta^t\zeta$, $(\zeta, P) = 1$, and let $H(\beta)$ denote the number of solutions of the congruence

$$X^m \equiv \beta \pmod{P^\lambda}, \tag{4.8}$$

under the restrictions $(m, p) = 1$, $(m, p^f - 1) = k > 1$. Then specializing to the case $s = 1$ in Theorems 2, 3, and 4 and using (4.7) with $\zeta = -\xi$, $\alpha = 1$, it follows that

THEOREM 5. *If* $H(\beta)$ *denotes the number of solutions of the congruence* (4.8), *then*

$$H(\beta) = \begin{cases} kp^{fe(m-1)} & (\lambda > t = em,\ \chi(\zeta) = 1), \\ p^{fe(m-1)+f(j-1)} & (\lambda = t = em + j, m > j > 0), \\ p^{fe(m-1)} & (\lambda = t = em), \\ 0 & (\textit{otherwise}). \end{cases} \tag{4.9}$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

5. **Estimates and solvability criteria.** To obtain estimates for $Q_s(\rho)$ we need first a bound on $|J_r(\gamma)|$, $(\gamma, P)=1$. Place $N_0=0$ and define N_r for $r\geqq 1$ to be the number of sets $(h_1, \cdots, h_r)$ such that $k>h_i>0$ $(r\geqq i\geqq 1)$ with $h_1+\cdots+h_r\not\equiv 0 \pmod{k}$. We note the identity, $N_r+N_{r-1}=(k-1)^r$, in case $r\geqq 1$. On the basis of this notation and Lemmas 7 and 8, one obtains

LEMMA 11. *If* $r\geqq 0$ *and* $(\gamma, P)=1$, *then*

$$|J_r(\gamma)| \leqq N_r p^{f(r-1)/2}. \tag{5.1}$$

In particular, we have the estimates $(s\geqq 1)$,

$$|J_s(\xi)| \leqq N_s p^{f(s-1)/2}, \qquad |\eta_s| \leqq N_{s-1} p^{f(s-2)/2}. \tag{5.2}$$

By Corollary 2.1 and (5.2) we obtain the following estimate for $Q_s(\rho)$ in case $t=0$.

THEOREM 6. *If* $\lambda>t=0$, *then*

$$|Q_s(\rho) - p^{f\lambda(s-1)}| \leqq p^{f[(\lambda-1)(s-1)+(s-2)/2]}(p^{f/2}N_s + N_{s-1}). \tag{5.3}$$

A second estimate is obtained on applying the bound for $|\eta_s|$ in (5.2) to the result in Corollary 3.1.

THEOREM 7. *If* $\lambda>t=j$, $m>j>0$, *then*

$$|Q_s(\rho) - p^{f(\lambda-1)(s-1)}(p^{f(s-1)} - 1)| \leqq p^{f[(\lambda-1)(s-1)+(s-2)/2]}(p^f - 1)N_{s-1}. \tag{5.4}$$

We use these two estimates to obtain solvability criteria for the congruence (1.1) in case $\lambda>t$.

REMARK. To show that $Q_s(\rho)>0$ where $\rho=\theta^{em+i}\xi$, $(\xi, P)=1$, $(m>j\geqq 0)$, it is sufficient to consider the case $e=0$.

THEOREM 8. *If* $\lambda>t\equiv 0 \pmod{m}$, *then* $Q_s(\rho)>0$ *provided*

$$f_1(\sigma) = \sigma^s - N_s\sigma - N_{s-1} > 0 \qquad (\sigma = p^{f/2}). \tag{5.5}$$

Proof. By the above remark we may suppose that $t=0$. In this case we obtain from (5.3) the lower bound,

$$Q_s(\rho) \geqq p^{f(\lambda-1)(s-1)+f(s-2)/2} f_1(\sigma),$$

and hence, $Q_s(\rho)>0$ if $f_1(\sigma)>0$.

THEOREM 9. *If* $\lambda>t\not\equiv 0 \pmod{m}$, *then* $Q_s(\rho)>0$ *provided*

$$f_2(\sigma) = \sigma^{2(s-1)} - N_{s-1}\sigma^s + N_{s-1}\sigma^{s-2} - 1 > 0 \qquad (\sigma = p^{f/2}). \tag{5.6}$$

Proof. Again by the remark preceding Theorem 8, it is sufficient to consider the case $\lambda>t$, $m>t>0$. We obtain in this case by (5.4) the lower bound,

$$Q_s(\rho) \geqq p^{f(\lambda-1)(s-1)} f_2(\sigma).$$

It follows that $Q_s(\rho)>0$ if $f_2(\sigma)>0$.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

We are now in a position to prove the following solvability criterion in the case $s=3$.

THEOREM 10. *If* $(\alpha_1\alpha_2\alpha_3, P)=1$, *then subject to the conditions* (1.2), *the congruence,*

$$\alpha_1 X_1^m + \alpha_2 X_2^m + \alpha_3 X_3^m + \rho \equiv 0 \pmod{P^\lambda}, \tag{5.7}$$

is solvable for all prime ideals P *of norm* $N(P)=p^f > (k-1)^2(k-2)^2$.

Proof. We consider three cases.

Case 1 ($\lambda > t \equiv 0 \pmod m$). In this case $Q_3(\rho)>0$ by Theorem 8, provided $f_1(\sigma)>0$, where

$$f_1(x) = x^3 - (k-1)(k^2-3k+3)x - (k-1)(k-2).$$

If $k=2$, then $f_1(\sigma)=\sigma^3-\sigma>0$ for all σ. Hence we may suppose $k\geqq 3$. It is easily verified in case $k\geqq 3$ that $f_1(x)=0$ has a single simple, positive root. Thus with $k=3$, we have $f_1(7^{1/2})>0$, so that $Q_3(\rho)>0$ except possibly when $p=2, f=2$. If $k>3$, we have

$$f_1((k-1)(k-2)) = (k-1)^2(k-2)\left[k^2(k-6)+11k-7\right] - (k-1)(k-2).$$

Since the bracketed expression >0 for $k>3$, it follows in this subcase that $f_1(\sigma)>0$ for all $\sigma > (k-1)(k-2)$. This proves the Theorem in Case 1.

Case 2 ($\lambda > t \not\equiv 0 \pmod m$). In this case $Q_3(\rho)>0$ by Theorem 9, provided $f_2(\sigma)>0$, where

$$f_2(x) = (x^2-1)(x^2-(k-1)(k-2)x+1).$$

For all $k\geqq 2$, it is clear that $f_2(\sigma)>0$ if $\sigma > (k-1)(k-2)$, and the theorem follows in Case 2.

Case 3 ($\lambda = t$). Since in this case $\rho=0$, there is always the trivial solution.

BIBLIOGRAPHY

1. Eckford Cohen, *Congruence representations in algebraic n umber fields*, Trans. Amer. Math. Soc. vol. 75 (1953) pp. 444–470.

2. ———, *Binary congruences in algebraic number fields*, Proc. Nat. Acad. Sci. U.S.A. vol. 42 (1956) pp. 120–122.

3. H. Davenport and H. Hasse, *Die Nullstellen der Kong ruenzzetafunktionen in gewissen Zyklischen Fällen*, J. Reine Angew. Math. vol. 172 (1935) pp. 151–182.

4. L. K. Hua and H. S. Vandiver, *Characters over certain types of rings with applications to theory of equations in a finite field.* Proc. Nat. Acad. Sci. U.S.A. vol. 35 (1949) pp. 94–99.

5. H. S. Vandiver, *On a generalization of a Jacobi exponential sum associated with cyclotomy*, Proc. Nat. Acad. Sci. U.S.A. vol. 36 (1950) pp. 144–151.

6. André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 497–508.

UNIVERSITY OF TENNESSEE
KNOXVILLE, TENN.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use