CONGRUENCE REPRESENTATIONS IN ALGEBRAIC NUMBER FIELDS II. SIMULTANEOUS LINEAR AND QUADRATIC CONGRUENCES

ECKFORD COHEN

1. Introduction. Let f and λ be positive integers and p a positive odd prime. Suppose further that P is an ideal of norm p^f in a finite extension F of the rational field. In **(2)**, which will also be referred to as I in the present paper, we obtained the number of solutions $N_s(m)$ of the quadratic congruence,

$$m \equiv \alpha_1 x_1^2 + \ldots + \alpha_s x_s^2 \pmod{P^\lambda}, \tag{1.1}$$

where m is an arbitrary integer of F, and the α_i are integers of F prime to P. In this paper we consider an analogous problem in simultaneous representation involving both linear and quadratic congruences. In particular, we shall determine the number of simultaneous solutions $N_s(m, n)$ of the pair of congruences

$$\begin{aligned} m &\equiv \alpha_1 x_1^2 + \ldots + \alpha_s x_s^2 \pmod{P^\lambda} \\ n &\equiv \beta_1 x_1 + \ldots + \beta_s x_s \pmod{P^\lambda}, \end{aligned} \tag{1.2}$$

where m and n are arbitrary integers of F, and the α_i and β_i are integers of F prime to P.

As in I we make use of the theory of exponential sums in algebraic number fields. However, the method of the paper requires only the most elementary properties of the generalized Cauchy-Gauss sums (§2). The function $N_s(m, n)$ is completely and explicitly evaluated in Theorem 1 (§3), and on the basis of this result, precise solvability criteria for the congruences (1.2) are deduced in §4 (Theorem 2). In contrast with the three cases of insolvability of (1.1) obtained in I (see the Remark at the end of the present paper), there are thirteen cases in which the simultaneous congruences (1.2) may have no solutions (Theorem 2). Another striking difference between the results for the two problems lies in the fact that (1.1) is always solvable for $s \geqslant 3$, while the minimal value of s such that the pair of congruences (1.2) is always solvable is $s = 5$ (Corollary (2.1)).

In the special case $\lambda = 1$, the congruences in (1.2) may be interpreted as simultaneous equations in the Galois field $GF(p^f)$. The problem of determining $N_s(m, n)$ in this case was solved in [3], with comparatively simple results. In that paper it was shown that $N_4(m, n) > 0$ in case $\lambda = 1$. By contrast, if $\lambda > 1$, two distinct cases of insolvability may occur in (1.2) when

Received November 6, 1957.

$s = 4$ (see Theorem 2). In addition, there exist only four insolvable cases of (1.2) in case $\lambda = 1$, as compared with thirteen in the case of arbitrary λ.

Another important special case arises when $f = 1$, in which case (1.2) may be viewed as a simultaneous pair of rational congruences (mod p^λ). This problem was considered by O'Connor, using a quite different method, in connection with a more general investigation **(4)**. However, his results were fragmentary except in the case $\lambda = 1$. The results of the present paper can therefore be viewed as a completion and extension of some of O'Connor's results on rational congruences.

2. Exponential sums. Let us choose an ideal C of F, not divisible by the prime ideal P, such that $\theta = PC$ is principal. Any integer ρ of F has a representation (mod P^λ) of the form $\rho \equiv \theta^t\zeta$ where $\lambda \geqslant t \geqslant 0$ and $(\xi, P) = 1$. In this representation t is uniquely determined and, in addition, ξ is uniquely determined (mod P) if $t \neq \lambda$. (If $t = \lambda$, one may assume $\xi = 1$.) We let D denote the ideal different of F and choose an ideal B such that $\zeta = B/P^\lambda D$ is principal. Further, let $T(\rho)$ denote the trace function in F. Then we place $\zeta_k = \zeta\theta^{\lambda-k} (0 \leqslant k \leqslant \lambda)$, where $\zeta = \zeta_\lambda$, and define $e_k(\rho) = \exp(2\pi i T(\rho\zeta_k))$ with $e(\rho) = e_1(\rho)$. This is the exponential function (mod P^λ) introduced by Hecke **(4, §54)** and discussed under a different notation in I. The function $e_k(\rho)$ is an additive character (mod P^k) and has the simple properties: $e_0(\rho) = 1$, $e_k(\rho) = e_k(\rho')$ if $\rho \equiv \rho'$ (mod P^k), $e_k(\rho\theta^j) = e_{k-j}(\rho)$ for $k \geqslant j \geqslant 0$, and $e_k(a_1 + a_2) = e_k(a_1)e_k(a_2)$. In addition, if P is of norm p^f, p prime, then

$$\sum_{x (\mathrm{mod}\ P^k)} e_k(\rho x) = \begin{cases} p^{fk} & (P^k \mid \rho) \\ 0 & (P^k \mid \rho). \end{cases} \tag{2.1}$$

Suppose that $\lambda \geqslant k \geqslant 0$ and let a and b be integers of F. The notation $\psi(a)$ will be used to denote the Legendre symbol (a/P) in F. We now introduce several trigonometric sums which will be needed in our discussion:

$$G_k(a) = \sum_{x (\mathrm{mod}\ P^k)} e_k(ax^2), \qquad G(a) = G_1(a), \tag{2.2}$$

$$G_k^*(a) = \sum_{(x, P^k)=1} \psi(x) e_k(ax), \qquad G^*(a) = G_1^*(a), \tag{2.3}$$

$$c_k(a) = \sum_{(x, P^k)=1} e_k(ax), \qquad c(a) = c_1(a), \tag{2.4}$$

$$S_k(a, b) = \sum_{x (\mathrm{mod}\ P^k)} e_k(ax^2 + 2bx). \tag{2.5}$$

The functions $G_k(a)$ and $G^*{}_k(a)$ are the Hecke sums **(4, §54)**, $c_k(a)$ is Rademacher's sum **(6, §2.2)**, and $S_k(a, b)$ is the generalization to F of the Cauchy-Gauss sum **(3, (1.7))**.

Suppose that P is odd as well as prime. The Hecke and Rademacher sums possess the following useful properties. If $k > 0$ and $a \equiv \theta^t\mu$ (mod P^k) where $k \geqslant t \geqslant 0$, $(\mu, P) = 1$, then

$$G_k^*(a) = \begin{cases} p^{f(k-1)}G^*(\mu) & (t = k-1) \\ 0 & (\text{otherwise}), \end{cases} \tag{2.6}$$

$$c_k(a) = \begin{cases} p^{f(k-1)}(p^f - 1) & (k \leqslant t) \\ -p^{f(k-1)} & (t = k-1) \\ 0 & (\text{otherwise}); \end{cases} \tag{2.7}$$

if $k \geqslant 0$, then

$$G_k(1) = \begin{cases} p^j & (k = 2j) \\ p^j G(1) & (k = 2j+1), \end{cases} \tag{2.8}$$

$$G_k(\mu) = \psi^k(\mu)G_k(1); \tag{2.9}$$

moreover,

$$G^*(\mu) = G(\mu) = \psi(\mu)G(1), \tag{2.10}$$

$$G^2(1) = \psi(-1)p^f. \tag{2.11}$$

For a more detailed discussion of these sums we refer to I.

The function $S_k(a, b)$ has the following reduction property (cf. Carlitz **(1**, Lemma 3**)** in the rational case).

LEMMA 1. *If $k \geqslant 0$ and a is defined as in* (2.6) *then for P odd*

$$S_k(a, b) = p^{ft}e_{k-t}(-r^2/\mu)G_{k-t}(\mu) \quad \text{or} \quad 0 \tag{2.12}$$

according as b is or is not divisible by P^k, r being defined by $b \equiv \theta^t r \pmod{P^k}$ in case $P^t | b$.

Proof. A complete residue system (mod P^k) is given by $x = \theta^{k-t} + z$ where y and z range over complete residue systems modulo P^t and P^{k-t} respectively. Hence, by the elementary properties of $e_k(\rho)$, we have

$$S_k(a, b) = \sum_{z \pmod{P^{k-t}}} e_k(az^2 + 2bz) \sum_{y \pmod{P^t}} e_t(2by).$$

If $P^t \nmid b$, then $S_k(a, b) = 0$ by (2.1). Suppose then that $P^t | b$, so that b may be written (mod P^k) in the form $b \equiv \theta^t r$. Then by (2.1)

$$S_k(a, b) = p^{ft} \sum_{z \pmod{P^{k-t}}} e_{k-t}(\mu z^2 + 2rz)$$

$$= p^{ft}e_{k-t}\left(-\frac{r^2}{\mu}\right) \sum_{z \pmod{P^{k-t}}} e_{k-t}\left(\mu\left(z + \frac{r}{\mu}\right)^2\right).$$

But since $z + r/\mu$ and z range together over complete residue systems (mod P^{k-t}), the Lemma follows immediately.

3. Evaluation of $N_s(m, n)$. In the remainder of the paper f, λ, and s will denote positive integers. As in the Introduction, P will represent an odd prime ideal of F with norm p^f, p being a rational odd prime. The letters α_i, β_i $(i = 1, \ldots, s)$ will denote integers of F prime to P, while m and n will represent arbitrary integers of F. In addition, we define

$$\alpha = \alpha_1 \dots \alpha_s, \qquad \beta = \frac{\beta_1^2}{\alpha_1} + \dots + \frac{\beta_s^2}{\alpha_s},$$

and write

$$m \equiv \theta^a M, \qquad n \equiv \theta^b N, \qquad \beta \equiv \theta^d \beta' \pmod{P^\lambda}$$

where a, b, d are non-negative integers $\leqslant \lambda$, and M, N, β' are integers of F not divisible by P. We also define for $b \geqslant d$,

$$\gamma = N^2\theta^{2b-d} - m\beta' \qquad \gamma \equiv \theta^h \gamma' \pmod{P^\lambda},$$

where $\lambda \geqslant h \geqslant 0$ and $(\gamma', P) = 1$. We place

$$\delta = \min(b, d) \qquad \eta = \min(b, h),$$

it being understood that $\eta = b$ if h is undefined. Also we put

$$s = \begin{cases} 2r & (s \text{ even}) \\ 2r+1 & (s \text{ odd}) \end{cases} \qquad d = \begin{cases} 2D & (d \text{ even}) \\ 2D+1 & (d \text{ odd}). \end{cases}$$

Let l denote any one of the integers a, δ, h, λ. Then we place

$$l_0 = \left[\frac{l+1}{2}\right], \qquad l_1 = \left[\frac{l}{2}\right], \qquad l_2 = \left[\frac{l-1}{2}\right],$$

where $[x]$ denotes the greatest integer $\leqslant x$, and $l_i = a_i$, δ_i, h_i or λ_i according as $l = a$, δ, h, or λ $(i = 0, 1, 2)$. We also write

$$t_1 = \min(a_1, \delta_1), \qquad t_2 = \min(a_2, \delta_2)$$

and define for integers u, v,

$$L(u, v) = \begin{cases} 1 & (u \text{ odd}, u < v) \\ 0 & (\text{otherwise}), \end{cases}$$

$$L'(u, v) = \begin{cases} 1 & (u \text{ even}, u < v) \\ 0 & (\text{otherwise}). \end{cases}$$

If $\sigma \geqslant -1$, we define further

$$P_r(\sigma) = \sum_{j=0}^{\sigma} p^{fj(4-2r)} = \begin{cases} \dfrac{p^{f(\sigma+1)(4-2r)} - 1}{p^{f(4-2r)} - 1} & (r \neq 2) \\ \sigma + 1 & (r = 2), \end{cases}$$

$$Q_r(\sigma) = \sum_{j=0}^{\sigma} p^{fj(3-2r)} = \frac{p^{f(\sigma+1)(3-2r)} - 1}{p^{f(3-2r)} - 1},$$

$$W_r(\sigma) = \sum_{j=0}^{\sigma} p^{2fj(1-r)} = \begin{cases} \dfrac{p^{2f(\sigma+1)(1-r)} - 1}{p^{2f(1-r)} - 1} & (r \neq 1) \\ \sigma + 1 & (r = 1). \end{cases}$$

The final formulas for $N_s(m, n)$ will be expressed in terms of the following functions:

https://doi.org/10.4153/CJM-1958-056-x Published online by Cambridge University Press

$$A_1 = (p^f - 1)\{p^{f(2-r)}P_r(t_1 - 1) + \psi((-1)^r\alpha)P_r(t_2)\} - p^{af(2-r)}\{L(a, \delta) + \psi((-1)^r\alpha)L'(a, \delta)\} + p^{f(r-1)}, \tag{3.1}$$

$$A_2 = p^f(p^f - 1)Q_r(t_1 - 1) - p^{f(a+a_2(1-2r))}L(a, \delta) + p^{f(r+a_1(3-2r))}\psi((-1)^r\alpha M)L'(a, \delta) + p^{f(2r-1)}, \tag{3.2}$$

$$B_1 = p^{f((D+1)(3-2r)-1)}(p^f - 1)Q_r(h_1 - D - 1) - p^{f(h_0(3-2r)-1)}L(h, \lambda) + p^{f(1-r+h_1(3-2r))}\psi((-1)^r\alpha\gamma')L'(h, \lambda), \tag{3.3}$$

$$B_2 = p^{f((D+1)(3-2r)-r+1)}(p^f - 1)\psi((-1)^r\alpha)Q_r(h_2 - D - 1) + p^{fh_0(3-2r)}\psi(\gamma')L(h, \lambda) - p^{f(h_1(3-2r)-r+1)}\psi((-1)^r\alpha)L'(h, \lambda), \tag{3.4}$$

$$B_3 = p^{2fD(1-r)}(p^f - 1)\{p^{f(1-2r)}W_r(h_1 - D - 1) + \psi((-1)^r\beta'\alpha)p^{-fr}W_r(h_2 - D)\} - p^{f(h(1-r)-r)}\{L(h, \lambda) + \psi((-1)^r\alpha\beta')L'(h, \lambda)\}, \tag{3.5}$$

$$B_4 = p^{f(1-r)(h+1)}\{\psi(\gamma')L(h, \lambda) + \psi((-1)^{r+1}\alpha\beta'\gamma')L'(h, \lambda)\}. \tag{3.6}$$

We are now in a position to state and prove our first main result.

THEOREM 1. *The number of solutions $N_s(m, n)$ of the pair of congruences* (1.2) *is given by the following formulas:*

If $d > \eta$, then

$$N_s(m, n) = \begin{cases} p^{f(2\lambda-1)(r-1)}A_1 & (s = 2r) \\ p^{f(\lambda-1)(2r-1)}A_2 & (s = 2r + 1). \end{cases} \tag{3.7}$$

If $d \leqslant \eta$, then

$$N_s(m, n) = \begin{cases} p^{f(2\lambda-1)(r-1)}A_1 + p^{f(2\lambda(r-1)+D)}B_1, \\ p^{f(2\lambda-1)(r-1)}A_1 + p^{f(2\lambda(r-1)+D)}B_2, \\ p^{f(\lambda-1)(2r-1)}A_2 + p^{f(\lambda(2r-1)+D)}B_3, \\ p^{f(\lambda-1)(2r-1)}A_2 + p^{f(\lambda(2r-1)+D)}B_4, \end{cases} \quad \text{or} \tag{3.8}$$

according as (i) $s = 2r$, $d = 2D$, (ii) $s = 2r$, $d = 2D + 1$, (iii) $s = 2r + 1$, $d = 2D$, *or* (iv) $s = 2r + 1$, $d = 2D + 1$.

Proof. The proof will be divided into four parts.

Part I. Our method is based on the Fourier representation **(3)** of $N_s(m, n)$ as a function of m and n (mod P^λ). In particular

$$N_s(m, n) = p^{-2f\lambda} \sum_{u(\mathrm{mod}\ P^\lambda)} \sum_{v(\mathrm{mod}\ P^\lambda)} \phi(u, v)e_\lambda(-mu)\, e_\lambda(-2nv), \tag{3.9}$$

where

$$\phi(u, v) = \sum_{\substack{x_i(\mathrm{mod}\ P^\lambda) \\ (i=1, \ldots, s)}} e_\lambda(u(\alpha_1x_1^2 + \ldots + \alpha_sx_s^2))\, e_\lambda(2v(\beta_1x_1 + \ldots + \beta_sx_s)) = \prod_{i=1}^{s} S_\lambda(\alpha_iu, \beta_iv).$$

Placing $u = U\theta^{\lambda-k}$ $(k = 0, 1, \ldots, \lambda)$ and summing over $U \pmod{P^k}$, $(U, P^k) = 1$, we have

$$N_s(m,n) = p^{-2f\lambda} \sum_{k=0}^{\lambda} \sum_{(U,P^k)=1} \sum_{v \pmod{P^\lambda}} e_k(-mU)\, e_\lambda(-2nv). \left(\sum_{i=1}^{s} S_\lambda(\alpha_i U\theta^{\lambda-k}, \beta_i v) \right). \tag{3.10}$$

By Lemma 1 it follows that $S_\lambda(\alpha_i U\theta^{\lambda-k}, \beta_i v) = 0$, unless v can be expressed (mod P^k) in the form $v \equiv \theta^{\lambda-k}y$, in which case, using (2.9),

$$S_\lambda(\alpha_i U\theta^{\lambda-k}, \beta_i v) = p^{f(\lambda-k)}\psi^k(\alpha_i U) e_k(-\beta_i^2 y^2/\alpha_i U) G_k(1).$$

Substituting in (3.10) and summing over $y \pmod{P^k}$, one obtains, on the basis of the definitions of α, β, and S_k,

$$N_s(m,n) = p^{f\lambda(s-2)} \sum_{k=0}^{\lambda} p^{-fks} \psi^k(\alpha) G_k^s(1) \cdot \sum_{(U,P^k)=1} \psi^{ks}(U)\, e_k(-mU)\, S_k\left(-\frac{\beta}{U}, -n\right). \tag{3.11}$$

If $k \leqslant d$, then by Lemma 1

$$S_k\left(-\frac{\beta}{U}, -n\right) = \begin{cases} p^{fk} & (k \leqslant b) \\ 0 & (k > b) \end{cases}, \tag{3.12}$$

while if $k > d$, we obtain by (2.9),

$$S_k\left(-\frac{\beta}{U}, -n\right) = \begin{cases} p^{fd}\psi^{k-d}\left(-\frac{\beta'}{U}\right) e_k\left(\frac{N^2\theta^{2b-d}U}{\beta'}\right) G_{k-d}(1) & (b \geqslant d) \\ 0 & (b < d). \end{cases} \tag{3.13}$$

We now separate the k summation in (3.11) into three parts to obtain

$$N_s(m,n) = \sum_1 + \sum_2 + \sum_3, \tag{3.14}$$

where $k = 0$ in $\sum_1$, $d \geqslant k \geqslant 1$ in $\sum_2$, and $k > d$ in $\sum_3$, it being agreed that vacuous sums shall have the value 0. It follows immediately that

$$\sum_1 = p^{f\lambda(s-2)}, \tag{3.15}$$

and by (3.12) that

$$\sum_2 = p^{f\lambda(s-2)} \sum_{k=1}^{\delta} p^{fk(1-s)} \psi^k(\alpha) G_k^s(1) \sum_{(U,P^k)=1} \psi^{ks}(U) e_k(-mU). \tag{3.16}$$

Also, by (3.13) and the definition of γ, one obtains

$$\sum_3 = \begin{cases} 0 & \text{or} \\ p^{f(\lambda(s-2)+d)}\psi^d(-\beta') \sum_{k=d+1}^{\lambda} p^{-fks}\psi^k(-\alpha\beta') G_k^s(1) G_{k-d}(1). \\ \qquad \sum_{(U,P^k)=1} (\psi(U))^{k(s+1)-d} e_k\left(\frac{\gamma U}{\beta'}\right), \end{cases} \tag{3.17}$$

https://doi.org/10.4153/CJM-1958-056-x Published online by Cambridge University Press

according as $d > \eta$ or $d \leqslant \eta$, because the inner U sum reduces in every case either to $c_k(\gamma/\beta')$ or to $G^*{}_k(\gamma/\beta')$, and these functions vanish when $h < k - 1$, by (2.7) and (2.6) respectively.

Part II. With reference to (3.16) we write

$$\sum_{2} = \sum_{21} + \sum_{22}, \tag{3.18}$$

where $k = 2j$ in $\sum_{21}$ and $k = 2j + 1$ in $\sum_{22}$.

Case $1(s = 2r)$. Applying (2.8) one obtains

$$\sum_{21} = p^{2f\lambda(r-1)} \sum_{j=1}^{\delta_1} p^{2fj(1-r)} c_{2j}(-m),$$

which becomes by (2.7)

$$\sum_{21} = p^{f(2\lambda-1)(r-1)}\{(p^f - 1)p^{f(2-r)}P_r(t_1 - 1) - p^{af(2-r)}L(a, \delta)\}. \tag{3.19}$$

By (2.8) and (2.11),

$$\sum_{22} = p^{f(2\lambda-1)(r-1)}\psi((-1)^r\alpha) \sum_{j=0}^{\delta_2} p^{2fj(1-r)} c_{2j+1}(-m),$$

so that by (2.7)

$$\sum_{22} = p^{f(2\lambda-1)(r-1)}\psi((-1)^r\alpha)\{(p^f - 1)P_r(t_2) - p^{af(2-r)}L'(a, \delta)\}. \tag{3.20}$$

Case $2(s = 2r + 1)$. In this case we have by (2.8)

$$\sum_{21} = p^{f\lambda(2r-1)} \sum_{j=1}^{\delta_1} p^{fj(1-2r)} c_{2j}(-m),$$

which becomes, on applying (2.7),

$$\sum_{21} = p^{f(\lambda-1)(2r-1)}\{p^f(p^f - 1)Q_r(t_1 - 1) - p^{f(a_2(1-2r)+a)}L(a, \delta)\}. \tag{3.21}$$

By (2.8) and (2.11) we have

$$\sum_{22} = p^{f(\lambda(2r-1)-r)}\psi((-1)^r\alpha)G(1) \sum_{j=0}^{\delta_2} p^{fj(1-2r)} G^*_{2j+1}(-m),$$

and hence on the basis of (2.6), (2.10), and (2.11),

$$\sum_{22} = p^{f((\lambda-1)(2r-1)+a_1(3-2r)+r)}\psi((-1)^r\alpha M)L'(a, \delta). \tag{3.22}$$

This completes the evaluation of $\sum_2$.

Part III. Referring to (3.17) in the case $d \leqslant \eta$, we place

$$\sum_{3} = \sum_{31} + \sum_{32} \tag{3.23}$$

where $k = 2j$ in $\sum_{31}$ and $k = 2j + 1$ in $\sum_{32}$.

Case $1(s = 2r, d = 2D)$. In this case by (2.8)

https://doi.org/10.4153/CJM-1958-056-x Published online by Cambridge University Press

$$\sum_{31} = p^{f(2\lambda(r-1)+D)} \sum_{j=D+1}^{\lambda_1} p^{fj(1-2r)} c_{2j}\left(\frac{\gamma}{\beta'}\right),$$

and hence on the basis of (2.7)

$$\sum_{31} = p^{f(2\lambda(r-1)+D)}\{p^{f((D+1)(3-2r)-1)}(p^f - 1)Q_r(h_1 - D - 1) - p^{f(h_0(3-2r)-1)}L(h, \lambda)\}. \tag{3.24}$$

By (2.8) and (2.11)

$$\sum_{32} = p^{f(2\lambda(r-1)+D-r)}\psi((-1)^{r+1}\alpha\beta')G(1) \sum_{j=D}^{\lambda_2} p^{fj(1-2r)} G^*_{2j+1}\left(\frac{\gamma}{\beta'}\right),$$

which by (2.6), (2.10), and (2.11) gives

$$\sum_{32} = p^{f(2\lambda(r-1)+h_1(3-2r)+D-r+1)}\psi((-1)^r\alpha\gamma')L'(h, \lambda). \tag{3.25}$$

Case 2($s = 2r$, $d = 2D + 1$). By (2.8)

$$\sum_{31} = p^{f(2\lambda(r-1)+D)}\psi(-\beta')G(1) \sum_{j=D+1}^{\lambda_1} p^{fj(1-2r)} G^*_{2j}\left(\frac{\gamma}{\beta'}\right),$$

so that by (2.6), (2.10), and (2.11)

$$\sum_{31} = p^{f(2\lambda(r-1)+h_0(3-2r)+D)}\psi(\gamma')L(h, \lambda). \tag{3.26}$$

Applying (2.8) and (2.11), we have

$$\sum_{32} = p^{f(2\lambda(r-1)+D-r+1)}\psi((-1)^r\alpha) \sum_{j=D+1}^{\lambda_2} p^{fj(1-2r)} c_{2j+1}\left(\frac{\gamma}{\beta'}\right),$$

which becomes by (2.7)

$$\sum_{32} = p^{f(2\lambda(r-1)+D-r+1)}\psi((-1)^r\alpha)\{(p^f - 1)p^{f(D+1)(3-2r)}Q_r(h_2 - D - 1) - p^{fh_1(3-2r)}L'(h, \lambda)\}. \tag{3.27}$$

Case 3($s = 2r + 1$, $d = 2D$). By (2.8)

$$\sum_{31} = p^{f(\lambda(2r-1)+D)} \sum_{j=D+1}^{\lambda_1} p^{-2frj} c_{2j}\left(\frac{\gamma}{\beta'}\right),$$

and hence on the basis of (2.7)

$$\sum_{31} = p^{f(\lambda(2r-1)+D)}\{p^{f(2(D+1)(1-r)-1)}(p^f - 1)W_r(h_1 - D - 1) - p^{f(h(1-r)-r)}L(h, \lambda)\}. \tag{3.28}$$

Applying (2.8) and (2.11), one obtains

$$\sum_{32} = p^{f(\lambda(2r-1)+D-r)}\psi((-1)^r\alpha\beta') \sum_{j=D}^{\lambda_2} p^{-2frj} c_{2j+1}\left(\frac{\gamma}{\beta'}\right),$$

and thus by (2.7)

$$\sum_{32} = p^{f(\lambda(2r-1)+D-r)}\psi((-1)^r\alpha\beta')\{(p^f - 1)p^{2fD(1-r)}W_r(h_2 - D) - p^{fh(1-r)}L'(h, \lambda)\}. \tag{3.29}$$

Case 4 ($s = 2r + 1$, $d = 2D + 1$). In this case by (2.8)

$$\sum_{31} = p^{f(\lambda(2r-1)+D)}\psi(-\beta')G(1)\sum_{j=D+1}^{\lambda_1} p^{-2frj}G^*_{2j}\left(\frac{\gamma}{\beta'}\right),$$

which by (2.6), (2.10), and (2.11) gives

$$\sum_{31} = p^{f(\lambda(2r-1)+(h+1)(1-r)+D)}\psi(\gamma')L(h, \lambda). \tag{3.30}$$

Applying (2.8) and (2.11), one obtains

$$\sum_{32} = p^{f(\lambda(2r-1)-r+D)}\psi((-1)^r\alpha)G(1)\sum_{k=D+1}^{\lambda_2} p^{-2frj}G^*_{2j+1}\left(\frac{\gamma}{\beta'}\right),$$

and hence by (2.6), (2.10), and (2.11),

$$\sum_{32} = p^{f(\lambda(2r-1)+(h+1)(1-r)+D)}\psi((-1)^{r+1}\alpha\beta'\gamma')L'(h, \lambda). \tag{3.31}$$

This completes the evaluation of $\sum_3$ in case $d \leqslant \eta$.

Part IV. We now combine the results of the preceding parts. By (3.1), (3.15), (3.18), (3.19), and (3.20),

$$\sum_1 + \sum_2 = p^{f(2\lambda-1)(r-1)}A_1 \qquad (s = 2r), \tag{3.32}$$

and by (3.2), (3.15), (3.18), (3.21), and (3.22)

$$\sum_1 + \sum_2 = p^{f(\lambda-1)(2r-1)}A_2 \qquad (s = 2r + 1). \tag{3.33}$$

By (3.3), (3.23), (3.24), and (3.25)

$$\sum_3 = p^{f(2\lambda(r-1)+D)}B_1 \qquad (\text{Case } 1, d \leqslant \eta); \tag{3.34}$$

by (3.4), (3.23), (3.26), and (3.27)

$$\sum_3 = p^{f(2\lambda(r-1)+D)}B_2 \qquad (\text{Case } 2, d \leqslant \eta); \tag{3.35}$$

by (3.5), (3.23), (3.28), and (3.29)

$$\sum_3 = p^{f(\lambda(2r-1)+D)}B_3 \qquad (\text{Case } 3, d \leqslant \eta); \tag{3.36}$$

by (3.6), (3.23), (3.30), and (3.31)

$$\sum_3 = p^{f(\lambda(2r-1)+D)}B_4 \qquad (\text{Case } 4, d \leqslant \eta). \tag{3.37}$$

We also have by (3.17)

$$\sum_3 = 0 \qquad (d > \eta). \tag{3.38}$$

The theorem follows on combining the following formulas: (3.14), (3.32), (3.38) in case $d > \eta$, s even; (3.14), (3.33), (3.38) in case $d > \eta$, s odd; (3.14), (3.32), (3.34) in case $d \leqslant \eta$, s even, d even; (3.14), (3.32), (3.35) in case $d \leqslant \eta$, s even, d odd; (3.14), (3.33), (3.36) in case $d \leqslant \eta$, s odd, d even; and (3.14), (3.33), (3.37) in case $d \leqslant \eta$, s odd, d odd.

Although the formulas for $N_s(m, n)$ are quite complicated in the general case, they simplify remarkably in certain special cases. For example, by taking $\lambda = 1$ in Theorem 1, one obtains the compact results already proved in **(3)**. We also note the following simple corollaries which result easily from the theorem.

COROLLARY 1.1. *If* $b = 0$, $d > 0$ $(P \nmid n, P|\beta)$, *then*

$$N_s(m, n) = p^{f\lambda(s-2)}. \tag{3.39}$$

COROLLARY 1.2. *If* $d = h = 0$ $(P \nmid \beta, P \nmid \gamma)$, *then*

$$N_s(m, n) = \begin{cases} p^{f(2\lambda-1)(r-1)}(p^{f(r-1)} + \psi((-1)^r\alpha\gamma')) \\ p^{f(\lambda(2r-1)-r)}(p^{fr} - \psi((-1)^r\alpha\beta')), \end{cases} \quad \text{or} \tag{3.40}$$

according as $s = 2r$ *or* $2r + 1$.

COROLLARY 1.3. *If* $a = 0$, $b \geqslant d > h$, *then*

$$N_s(m, n) = \begin{cases} p^{f(2\lambda-1)(r-1)}(p^{f(r-1)} - \psi((-1)^r\alpha)) \\ p^{f((\lambda-1)(2r-1)+r)}(p^{f(r-1)} + \psi((-1)^r\alpha m)), \end{cases} \quad \text{or} \tag{3.41}$$

according as $s = 2r$ *or* $2r + 1$.

COROLLARY 1.4. *If* $a = 0$, $d > b > 0$, *then* $N_s(m, n)$ *is given by* (3.41).

4. Solvability criteria. Theorem 1 presents a means for determining directly all cases for which (2.1) is insolvable. To accomplish this, one must first simplify the formulas for $N_s(m, n)$ for small values of $s (s \leqslant 5)$. In obtaining these simplifications, it is useful to observe that $\psi(-\alpha) = 1$ in case $s = 2$, $d > 0$, and that the condition $d \leqslant \eta$ always implies that $d \leqslant a$. However, we omit the simplified formulas, since they involve numerous subcases and, moreover, are of little interest beyond the verification of our second main result, which we now state.

THEOREM 2. *The function* $N_s(m, n)$ *vanishes* (*that is*, (1.2) *is insolvable*) *if and only if one of the following sets of conditions is satisfied:*

(1) $s = 1$, $h < \lambda$
(2) $s = 2$, $d > \eta$, $a < \delta$
(3) $s = 2$, $d \leqslant \eta$, d *even*, h *even*, $h < \lambda$, $\psi(-a\gamma') = -1$
(4) $s = 2$, $d \leqslant \eta$, d *even*, h *odd*, $h < \lambda$
(5) $s = 2$, $d \leqslant \eta$, d *odd*, h *even*, $h < \lambda$
(6) $s = 2$, $d \leqslant \eta$, d *odd*, h *odd*, $h < \lambda$, $\psi(\gamma') = -1$
(7) $s = 3$, $d > \eta$, a *even*, $a < \delta$, $\psi(-\alpha M) = -1$
(8) $s = 3$, $d > \eta$, a *odd*, $a < \delta$
(9) $s = 3$, $d \leqslant \eta$, d *even*, h *odd*, $h < \lambda$, $\psi(-\alpha\beta') = -1$
(10) $s = 3$, $d \leqslant \eta$, d *odd*, h *odd*, $h < \lambda$, $\psi(\gamma') = -1$
(11) $s = 3$, $d \leqslant \eta$, d *odd*, h *even*, $h < \lambda$, $\psi(\alpha\beta'\gamma') = -1$
(12) $s = 4$, $d > \eta$, a *odd*, $a < \delta$, $\psi(\alpha) = -1$
(13) $s = 4$, $d \leqslant \eta$, d *odd*, h *odd*, $h < \lambda$, $\psi(\alpha) = \psi(\gamma') = -1$.

On the basis of Theorem 2 one obtains

COROLLARY 2.1. *The minimal value of s such that $N_s(m, n) > 0$ for all odd, prime-power ideals P^λ, for all coefficients, α_i, β_i prime to P, and for arbitrary m, n is given by $s = 5$.*

It will be observed that conditions (12) and (13), under which $N_4(m, n) = 0$, fail to arise in case $\lambda = 1$. We therefore have a result proved previously **(3**, §3**)**.

COROLLARY 2.2. *If $\lambda = 1$, then $N_4(m, n) > 0$.*

We also note

COROLLARY 2.3. *If $\psi(\alpha) = 1$, then $N_4(m, n) > 0$.*

Finally, it will be observed that the only cases of insolvability which can occur when $\lambda = 1$ arise from cases (1), (2), (3), and (7) of Theorem 2 **(3**, Theorem 2**)**.

Remark. By I, in contrast with Theorem 2, the congruence (1.1) is insolvable ($N_s(m) = 0$), if and only if one of these three sets of conditions is satisfied: (1) $s = 1$, $a < \lambda$, a *odd*; (2) $s = 1$, $a < \lambda$, a even, $\psi(\alpha M) = -1$; (3) $s = 2$, $a < \lambda$, a odd, $\psi(-\alpha) = -1$. This result is not stated explicitly in I but follows immediately from **(2**; (8.4), (8.5), (8.8)**)**.

REFERENCES

1. Leonard Carlitz, *Weighted quadratic partitions* (mod p^r), Math. Z., *59* (1953), 40–46.
2. Eckford Cohen, *Congruence representations in algebraic number fields*, Trans. Amer. Math. Soc., *75* (1953), 444–470.
3. Eckford Cohen, *Simultaneous pairs of linear and quadratic equations in a Galois field*, Can. J. Math., *9* (1957), 74-78.
4. Erich Hecke, *Vorlesungen ueber die Theorie der algebraischen Zahlen* (Leipzig, 1923).
5. R. E. O'Connor, *Quadratic and linear congruence*, Bull. Amer. Math. Soc., *45* (1939), 792–798.

University of Tennessee