QUADRATIC AND LINEAR CONGRUENCE*

R. E. O'CONNOR, S.J.

The number of simultaneous solutions of a quadratic and a linear congruence does not seem to be discussed in the literature, yet a knowledge of the invariants necessary to specify this number should lead to an arithmetical classification of the form-pairs involved. This preliminary investigation is confined to congruences with modulus odd and prime to the g.c.d.'s of the two sets of coefficients. From the formulas obtained, a simple use of the Chinese Remainder Theorem will give the number of solutions for any such modulus which is either square-free or at least whose prime factors of power greater than the first are of a definite class. An interesting application, of a different type from the preceding, is given in §6. Special cases of this and of Theorem 1 have already been proven.†

1. **Hypotheses and definitions.** We shall be considering *the number* $N(p^m)$ *of simultaneous solutions of the congruences*

$$(1^m) \qquad f(x) = \sum_1^n a_{ij}x_ix_j \equiv r, \qquad g(x) = \sum_1^n c_ix_i \equiv s \pmod{p^m}$$

with f and g integral forms, $n \geqq 2$, *r and s integers, and p an odd prime dividing neither the g.c.d. of the coefficients of f nor that of g. Defining* $\phi(x, t) = f(x) + 2tg(x)$, *let a be the determinant of f,* μ *be the modulo p rank of a, b be the determinant of* ϕ, ν *be the modulo p rank of b, and* $k = s^2a + rb$.

With the above forms are to be associated three others—$F(x)$, $G(x)$ and $\Phi(x, t) = F(x) + 2tG(x)$—related to the above as follows. By a well known theorem‡ we can find a linear, integral transformation T of determinant unity that takes f into a form f' which is congruent (mod p^m) to a form

$$F(x) = a_1x_1^2 + \cdots + a_nx_n^2,$$

where $p \nmid a_1a_2 \cdots a_\mu$, $p \mid a_{\mu+1}, a_{\mu+2}, \cdots, a_n$. The transformation T', identical with T for the variables x and taking t into itself, is also unimodular and takes $\phi(x, t)$ into the form $f'(x) + 2tG(x)$, where

$$G(x) = b_1x_1 + \cdots + b_nx_n.$$

* Presented to the Society, April 14, 1939.

† G. Pall and R. E. O'Connor, American Journal of Mathematics, vol. 61 (1939), pp. 491–496.

‡ Minkowski, *Gesammelte Abhandlungen*, vol. 1, p. 14.

Let A be the determinant of F and B the determinant of Φ.

If we consider now the congruences

$$(2^m) \qquad F(x) \equiv r, \qquad G(x) \equiv s \pmod{p^m},$$

the following facts are clear. The prime p divides neither the g.c.d. of the a_i's nor that of the b_i's; $A \equiv a$, $B \equiv b \pmod{p^m}$; the modulo p ranks of the matrices of F and Φ are respectively μ and ν; and the number $N(p^m)$ of solutions of (1^m) is the number of solutions of (2^m).

A *singular solution* of (1^m) is a solution ξ such that, for some integer λ (including zero), p divides each of the n integers $\sum_i (a_{ij}\xi_j) - \lambda c_i$ for $i = 1, 2, \cdots, n$. From the fact that this expression is obtained by setting $t = -\lambda$ in the partial derivative of $\phi(x, t)/2$ with respect to x_i, it is easily seen that the transformation T defines a one-to-one correspondence between the singular solutions of (1^m) and those of (2^m). Solutions of the congruences which are not singular we shall call *ordinary*.

2. **Inhomogeneous quadratic congruence.** We shall need explicit formulas for the number Q of solutions of

$$(3) \qquad \sum_1^n \alpha_{ij} x_i x_j - 2s \sum_1^n \beta_i x_i \equiv c \pmod{p}$$

in several hypotheses.

LEMMA.* *Let p be an odd prime; let s, c, α_{ij} $(=\alpha_{ji})$, and β_i, $(i, j = 1, 2, \cdots, n)$, be assigned integers; let δ be the determinant $|\alpha_{ij}|$ and δ' the integer $-\sum_1^n A_{ij}\beta_i\beta_j$, where A_{ij} is the cofactor of α_{ij} in δ.*

(4_1) If $p \nmid s\delta'$, $p \mid \delta$, then $Q = p^{n-1}$.

(4_2) If $p \nmid \delta'$, $p \mid \delta$, s, then, according as n is even or odd, $Q - p^{n-1} = p^{(n)}((-1)^{(n)}\delta' c \mid p)$ or $p^{(n)} p[c]((-1)^{(n)+1}\delta' \mid p)$.

(4_3) If $p \nmid \delta$, $\cdots$, then, according as n is even or odd, $Q - p^{n-1} = p^{(n)-1} p[\sigma]((-1)^{(n)}\delta \mid p)$ or $p^{(n)}((-1)^{(n)}\sigma \mid p)$.

Here (n) in the indices stands for $n/2$ or $(n-1)/2$ according as n is even or odd; σ for $\delta c - \delta' s^2$; and $p[z]$ for $p - 1 - p(z^2 \mid p)$ and hence for $p-1$ or -1 according as $p \mid z$ or $p \nmid z$. These formulas are valid for $n \geqq 1$, as is evident from the proof except in the case (4_2) with $n = 1$; but for this case (4_2) is easily verified directly.

By the process used to replace ϕ by Φ in §1, we can replace (3) by

* Formulae (4_1) and (4_3) for the case $n = 2$ are given by R. LeVavasseur (Mémoires de l'Académie des Sciences de Toulouse, (10), vol. 3 (1903), p. 39). A confusion of sign in summary on p. 46 has led to a similar confusion in Dickson, *History of the Theory of Numbers*, vol. 2, p. 327.

$$\sum_1^n \alpha_i y_i^2 - 2s\sum_1^n \gamma_i y_i \equiv c \pmod{p}, \tag{5}$$

which has the same number of solutions as (3) and where

$$\alpha_1\alpha_2 \cdots \alpha_n \equiv \delta, \qquad \gamma_1^2\alpha_2\alpha_3 \cdots \alpha_n + \gamma_2^2\alpha_3\alpha_4 \cdots \alpha_n\alpha_1 + \cdots + \gamma_n^2\alpha_1\alpha_2 \cdots \alpha_{n-1} \equiv -\delta' \pmod{p}. \tag{6}$$

From (6) it is clear that the hypothesis $p \mid \delta$ and $p \nmid \delta'$ implies that p divides exactly one of the α_i's, say α_n, and that p does not divide the corresponding γ_i, that is γ_n, and consequently that $\delta' \equiv -\gamma_n^2\alpha_1\alpha_2 \cdots \alpha_{n-1} \pmod{p}$. Thus in the hypothesis of (4_1) the left side of (5) contains a nonzero linear term, say $2s\gamma_n y_n$, such that the corresponding quadratic coefficient vanishes (mod p). The numbers $y_1, y_2, \cdots, y_{n-1}$ may be chosen arbitrarily and y_n is uniquely determined to satisfy (5).

In the hypothesis of (4_2), one quadratic and all linear coefficients of (5) vanish (mod p). Let $p \mid \alpha_n$. The number of solutions of (5) is then p times that of $\sum_1^{n-1}\alpha_i y_i^2 \equiv c \pmod{p}$. This gives* (4_2) in view of the remark immediately following (6).

To establish (4_3) we can transform (5)—since no α_i vanishes—into $\sum_1^n \alpha_i z_i^2 \equiv c + Rs^2 \pmod{p}$ by the transformation $y_i = z_i + s\mathfrak{a}_i\gamma_i$, $(i = 1, 2, \cdots, n)$, where $\mathfrak{a}_i$ is some integer satisfying $\mathfrak{a}_i\alpha_i \equiv 1 \pmod{p}$. Here R will be $\sum \mathfrak{a}_i\gamma_i^2$, so by (6) $R\delta \equiv -\delta' \pmod{p}$. The number of solutions z is then given by (4_3).

3. $N(p)$ **for simple invariants.** The following theorem is required for the proof of the more general Theorem 2 but in certain applications is more useful than the latter.

THEOREM 1. *With the hypotheses and definitions of* §1,

(7_1) *if* $p \nmid a$, $p \mid b$, *then* $N(p) = p^{n-2}$;

(7_2) *if* $p \nmid a$, $p \mid b$, s, *then, according as* n *is even or odd,* $N(p) - p^{n-2} = p^{(n)-1}p[r]((-1)^{(n)}a \mid p)$ *or* $p^{(n)}((-1)^{(n)}ar \mid p)$;

(7_3) *if* $p \nmid b, \cdots$ *then, according as* n *is even or odd,* $N(p) - p^{n-2} = p^{(n)-1}((-1)^{(n)}k \mid p)$ *or* $p^{(n)-1}p[k]((-1)^{(n)+1}b \mid p)$.

The superior symbol (n) *and the symbol* $p[\ ]$ *are defined in the lemma.*

* Here and later we make use of the following theorem: *The number of solutions of the quadratic congruence* $u_1x_1^2 + u_2x_2^2 + \cdots + u_nx_n^2 \equiv h \pmod{p}$, *where* p *is an odd prime,* $p \nmid u = u_1u_2 \cdots u_n$, h *an arbitrary integer and* $n \geqq 1$, *is given by the formula,* $p^{n-1} + p^{(n-2)/2}p[h]((-1)^{n/2}u \mid p)$ *or* $p^{n-1} + p^{(n-1)/2}((-1)^{(n-1)/2}uh \mid p)$ *according as* n *is even or odd.* Here we have written $p[h]$ for $p - 1 - p(h^2 \mid p)$ and $(z \mid p)$ is a Legendre symbol. These formulae were first given by C. Jordan in Comptes Rendus de l'Académie des Sciences, Paris, vol. 62 (1866), p. 687.

Replacing (1^1) by (2^1), we may suppose $p \nmid b_\tau$. Solving the linear congruence of (2^1) for x_τ and substituting this in the quadratic, we obtain, on multiplying the resulting eliminant by b_τ^2,

$$(8)\qquad \sum{}'(b_\tau^2 a_i + b_i^2 a_\tau)x_i^2 + a_\tau \sum_{i\neq j}{}' b_i b_j x_i x_j - 2sa_\tau \sum{}' b_i x_i \equiv b_\tau^2 r - a_\tau s^2 \pmod{p},$$

where $\sum'$ indicates that i, j are to be summed over the first n positive integers excluding τ. The number of solutions of (8) will coincide with $N(p)$. The determinant of the quadratic coefficients of (8) is identically $-b_\tau^{2(n-2)}B$, as may be seen for example by considering this determinant algebraically, subtracting b_i/b_1 times the first column from the column corresponding to the variable x_i for each $i \neq 1$ or τ, then multiplying every column except the first by b_1 and finally dividing every row except the first by $b_1 b_\tau^2$. The determinant of the whole left side of (8) considered as a form in variables x, s, which is the determinant corresponding to δ' of lemma, is easily seen to be identically $b_\tau^{2(n-2)}(b_\tau^2 A + a_\tau B)$. The formulas (7) are then obtained directly from the lemma, recalling only that $A \equiv a$, $B \equiv b \pmod{p}$.

4. $N(p)$ **for unrestricted invariants.** We shall write $\chi_i(x)$, $(i = 1, \cdots, n)$, for the ith concomitant* of a quadratic form $\chi(x) = \chi_1(x)$ and $(\chi_i \mid p)$ for the quadratic character (mod p) of any integer prime to p represented by $\chi_i(x)$, implying that the character is definitely 1 or -1. If $p \nmid r$, we also define $\psi(x, t) = f(x) + 2tg(x) + ct^2$ where c is an integer satisfying $rc \equiv s^2 \pmod{p}$. We can then prove

THEOREM 2. *The number $N(p)$ of solutions of (1^1) is given in all cases by the following table*:

	Hypothesis	Value of $N(p) - p^{n-2}$ (μ even)	Value of $N(p) - p^{n-2}$ (μ odd)
(9_1)	$\nu = \mu + 2$	$p^{n-2-(\mu)} p[r]((-1)^{(\mu)} a(\mu) \mid p)$	$p^{n-2-(\mu)}((-1)^{(\mu)} r a(\mu) \mid p)$
(9_2)	$\nu = \mu + 1$	$p^{n-1-(\mu)}((-1)^{(\mu)} k(\mu) \mid p)$	$p^{n-2-(\mu)} p[k(\mu)]((-1)^{(\mu)+1} b(\mu) \mid p)$
(9_3)	$\nu = \mu$, $p \nmid s$	0	0
(9_4)	$\nu = \mu$, $p \mid s$	$p^{n-1-(\mu)} p[r]((-1)^{(\mu)} a(\mu) \mid p)$	$p^{n-1-(\mu)}((-1)^{(\mu)} r a(\mu) \mid p)$

Here (μ) in indices is written for $\mu/2$ or $(\mu-1)/2$, according as μ is even or odd; $p[z]$ is written for $p - 1 - p(z^2 \mid p)$ and hence for $p - 1$ or -1, according as $p \mid z$ or $p \nmid z$; $a(\mu)$ is defined below, but $(a(\mu) \mid p) = (f_\mu \mid p)$; $b(\mu)$ is defined below, but $(b(\mu) \mid p) = (\phi_{\mu+1} \mid p)$, if $\nu = \mu + 1$; $k(\mu)$ is defined below, but $(k(\mu) \mid p)$ has the following invariant meaning if $\nu = \mu + 1$: if $p \mid r$, $(k(\mu) \mid p) = (s^2 a(\mu) \mid p)$, if $p \nmid r$, $(k(\mu) \mid p) = 0$ or $(r\psi_{\mu+1} \mid p)$, according as $p \mid \psi_{\mu+1}(x)$ or $p \nmid \psi_{\mu+1}(x)$. The other symbols are defined in §1.

* Cf. H. J. S. Smith, *Collected Mathematical Papers*, vol. 1, p. 412.

We may replace (1^1) by (2^1) and define $a(\mu)=a_1a_2\cdots a_\mu$, $b(\mu)=-(b_1^2a_2a_3\cdots a_\mu+b_2^2a_3a_4\cdots a_\mu a_1+\cdots+b_\mu^2a_1a_2\cdots a_{\mu-1})$, $k(\mu)=s^2a(\mu)+rb(\mu)$. Recalling that $p\nmid a(\mu)$, $p\mid a_{\mu+1}, a_{\mu+2}, \cdots, a_n$, a moment's consideration of the matrix of Φ shows that $\mu\leqq\nu\leqq\mu+2$ and that the condition $\nu=\mu+2$ is necessary and sufficient for there to be an index $\tau>\mu$ such that $p\nmid b_\tau$. Hence, if $\nu=\mu+2$, $N(p)$ is $p^{n-\mu-1}$ times the number of solutions of

$$a_1x_1^2+a_2x_2^2+\cdots+a_\mu x_\mu^2\equiv r \pmod p,$$

and taking this number from the note under §2, we have (9_1) valid for $\mu\geqq 1$; if $\nu<\mu+2$, $N(p)$ is $p^{n-\mu}$ times the number of solutions of

$$\begin{aligned} a_1x_1^2+a_2x_2^2+\cdots+a_\mu x_\mu^2&\equiv r,\\ b_1x_1+b_2x_2+\cdots+b_\mu x_\mu&\equiv s \pmod p, \end{aligned}\tag{10}$$

and we can take this number directly from Theorem 1 since the subcases $\nu=\mu+1$, $\nu=\mu$ coincide with the conditions $p\nmid b(\mu)$, $p\mid b(\mu)$, respectively. This gives (9_2), (9_3) and (9_4) for $\mu\geqq 2$. If $\mu=1$ with $\nu=\mu$, every b_i is divisible by p. To prove (9_2) for $\mu=1$, note that $N(p)$ is p^{n-1} times the number of solutions x_1 of $a_1x_1^2\equiv r$, $b_1x_1\equiv s \pmod p$ where $p\nmid a_1b_1$; hence, $N(p)=p^{n-1}\{1-(v^2\mid p)\}$ where $v=a_1s^2-b_1^2r$, a formula to which (9_2) reduces for $\mu=1$.

The statements regarding the invariant values of $(a(\mu)\mid p)$, $(b(\mu)\mid p)$ and $(k(\mu)\mid p)$ may be justified as follows. By definition, $a(\mu)$ is the only nonzero (mod p) determinant of order μ in the matrix of F; $b(\mu)$, in the case $\nu=\mu+1$, is the only nonzero (mod p) determinant of order $\mu+1$ in the matrix of Φ; $k(\mu)/r$, in the case $\nu=\mu+1$, $p\nmid r$, is a determinant of order $\mu+1$ in the matrix of $\Psi(x,t)=F(x)+2tG(x)+ct^2$ while all the other determinants of like order certainly vanish (mod p). Also each of these three determinants is principal. These statements remain true if f' is substituted for F in each of the three forms; but the three forms resulting are equivalent respectively to f, ϕ and ψ. Recalling then that corresponding concomitants of two equivalent forms are likewise equivalent, the statements of the theorem are seen to be correct.

5. **Modulus p^m.** With $m>1$ it seems we have to distinguish between ordinary and singular solutions (cf. §1).

THEOREM 3. *With $m\geqq 1$, the number $M(p^m)$ of ordinary solutions of (1^m) is $p^{(n-2)(m-1)}M(p)$, where $M(p)$ is the number of ordinary solutions of (1^1).*

We may replace (1^m) by (2^m). The theorem being clearly true for

$m=1$, let $m>1$. Every ordinary solution of (2^m) is an ordinary solution of (2^{m-1}) and hence each of the former is represented just once by $z_i=x_i+p^{m-1}y_i$, $(i=1, 2, \cdots, n)$, as x ranges through a complete set of ordinary solutions of (2^{m-1}) and, with each such x, y ranges through a complete (mod p) set of solutions of the congruences for y obtained by substituting z for the variables in (2^m). These congruences are

$$\sum_1^n a_i x_i y_i \equiv \rho, \qquad \sum_1^n b_i y_i \equiv \sigma \pmod{p}, \tag{11}$$

where ρ, σ are integers dependent on x. The condition that x be not singular implies that the matrix of the coefficients of y in (11) has modulo p rank equal to 2; hence, (11) has precisely p^{n-2} solutions y. The theorem follows immediately.

In cases where singular solutions occur, formulas for the total number $N(p^m)$ of solutions of (1^m) are not yet available except for $m=1$. The following theorem, taken with the two preceding, gives explicit formulae for $M(p^m)$ in all cases and for $N(p^m)$ in the cases where no singular solutions occur.

THEOREM 4. *The number of singular solutions of* (1^1) *is* $p^{n+1-\nu}$ *in each of the three cases*: (i) $\nu=\mu+2$, $p\,|\,r$; (ii) $\nu=\mu+1$, $(k(\mu)\,|\,p)=0$; (iii) $\nu=\mu$, $p\,|\,r$, $p\,|\,s$. *In no other cases have the congruences singular solutions.* (Cf. Theorem 2 for definition of $k(\mu)$ and invariant interpretation of $(k(\mu)\,|\,p)$.)

We consider congruences (2^1). The existence of a singular solution x implies that of an integer λ satisfying

$$a_i x_i \equiv \lambda b_i, \qquad i = 1, 2, \cdots, n, \tag{12^n}$$

$$r \equiv \lambda s \pmod{p}, \tag{13}$$

where (13) is obtained by substituting λb_i for each $a_i x_i$ in (2^1) which gives $\lambda\sum b_i x_i \equiv r$, $\sum b_i x_i \equiv s \pmod{p}$.

Now let $\nu=\mu+2$. There is a subscript $\tau>\mu$ such that $p\nmid b_\tau$, $p\,|\,a_\tau$. Formulas (12) and (13) then imply that $\lambda\equiv r\equiv 0 \pmod{p}$. Conversely, if $r\equiv 0$, choosing $\lambda\equiv 0$ determines $x_1\equiv x_2\equiv \cdots \equiv x_\mu\equiv 0$ and leaves x_i arbitrary for $i>\mu$; to be a singular solution of (2^1), this set must also satisfy $\sum_{\mu+1}^n b_i x_i\equiv s \pmod{p}$ and these conditions suffice. Thus there are $p^{n-\mu-1}$ singular solutions.

Let $\nu<\mu+2$. There is no such subscript τ and (2^1) admits precisely $p^{n-\mu}$ times as many singular solutions as (10). But if $(x_1, x_2, \cdots, x_\mu)$ is a singular solution of (10), (12^μ) and (13) must be satisfied and

substitution from (12^{μ}) in the linear congruence of (10) yields $\lambda b(\mu)+sa(\mu)\equiv 0$; this, multiplied by s, gives $p \mid k(\mu)$ in view of (13). If $\nu=\mu$ (that is, if $p \mid b(\mu)$), this further implies $p \mid s$, $p \mid r$. Conversely let $p \mid k(\mu)$. If $p \nmid s$, the singular solution of (10) is uniquely determined by (12^{μ}) and (13); if $p \mid s$, then by (13) $p \mid r$. Taking $(x_1, x_2, \cdots, x_{\mu})$ from (12^{μ}), the left members of (10) are congruent respectively to $\lambda^2 b(\mu)/a(\mu)$ and $\lambda b(\mu)/a(\mu)$. Thus (10) is satisfied by singular solutions in p ways (λ arbitrary) if $p \mid b(\mu)$ and uniquely ($\lambda \equiv 0$) if $p \nmid b(\mu)$.

6. **Simple applications.** It follows simply from this theorem that, *if* $p \nmid k=s^2a+rb$, *then* (1^1) *admits no singular solution.* (For if $p \nmid a$, then $\mu=n$, $\nu \leqq \mu+1$, and $k=k(\mu)$; while if $p \mid a$ the condition implies $p \nmid rb$ and hence $\nu=\mu+2$, $p \nmid r$.) Thus Theorems 1 and 3 give very simple formulas for $N(p^m)$ in this case. Other similar conclusions can easily be drawn.

Theorem 1 has the following interesting application, pointed out by Dr. Gordon Pall. *Let* a_{ij} *be a symmetric matrix of integers, of order* 3 *and with determinant prime to the odd, square-free integer* m. *Then a necessary and sufficient condition that two solutions* x, y *of the congruence*

$$\sum a_{ij}\xi_i\xi_j \equiv 0 \pmod{m} \tag{14}$$

should satisfy

$$\sum a_{ij}x_iy_j \equiv 0 \pmod{m} \tag{15}$$

is that x, y *be linearly dependent* (mod m).

For, taking m equal to a prime p, the number of simultaneous solutions y of the quadratic congruence (14), with y in place of ξ, and the linear congruence (15), for $x \not\equiv 0$, is easily calculated by the formula (7_2) to be p; and this number is exhausted by the solutions $y \equiv (\lambda x_1, \lambda x_2, \lambda x_3) \pmod{p}$, $\lambda = 1, 2, \cdots, p$. This is easily extended to m as specified by the Chinese Remainder Theorem.

If we relate integral vectors to the quadratic form with matrix (a_{ij}) and adjoint (A_{ij}) by defining norm of $x=\sum A_{ij}x_ix_j$, inner product of x, $y=\sum A_{ij}x_iy_j$, it follows (since $|A_{ij}|$ with $|a_{ij}|$ is prime to m) that *a necessary and sufficient condition that two vectors of norm zero* (mod m) *be linearly dependent* (mod m) *is that their inner product be zero* (mod m).

WESTON COLLEGE