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.