ON UNIVERSAL QUADRATIC NULL FORMS IN FIVE VARIABLES*

BY

R. S. UNDERWOOD

INTRODUCTION

1. We shall use L. E. Dickson's result:†

THEOREM 1. *Every universal quadratic null form in three or more variables is equivalent to a form*

$$F = 2^e gaxy + gby^2 + cyz + gd\psi(z, w, \cdots) \qquad (e \geqq 0), \tag{1}$$

where g and a are odd, a is prime to d, c is prime to g, and the greatest common divisor of the coefficients of ψ is 1.

We investigate the case of five variables. In (1) let

$$\psi = \alpha(hz^2 + jzw + lw^2) + Azv + Bwv + Cv^2, \tag{2}$$

where

(3) 1 is the greatest common divisor of α, A, B, C and of h, j, l, and where, by an argument which carries over from Dickson's paper, h may be taken prime to any given odd integer. We take h prime to ga.

We shall assume that one of $N, M, P \neq 0$, where $N = j^2 - 4hl$, $M = A^2 - 4\alpha hC$, $P = 2hB - jA$. For if $N = M = P = 0$, then $4\alpha h\psi = (2\alpha hz + \alpha jw + Av)^2$, where either $\alpha jw + Av$ is identically zero or it may be taken as a product of a constant by a new variable w. Hence this case reduces to the problem for three or four variables.

2. We shall need the following lemmas:

LEMMA 1. *If each of the congruences*

$$F \equiv G \pmod{2^e}, \qquad F \equiv G \pmod{gay}, \tag{4}$$

with F as in (1) *and* (2), *has a solution x, y, z, w, v such that y is odd, then $F = G$ is solvable.*

---

* Presented to the Society, June 13, 1931; received by the editors in December, 1930.

† *Universal quadratic forms*, these Transactions, vol. 31, No. 1, pp. 164–189. Subsequent references to the four-variable case refer to this paper.

LEMMA 2. *The congruence*

$$f = ax^2 + bxy + cy^2 \equiv k \pmod{p^n}, \tag{5}$$

where p is an odd prime, is solvable for every k if and only if $\Delta = b^2 - 4ac \not\equiv 0 \pmod{p}$ when $n = 1$, and $(\Delta/p) = 1$ when $n > 1$.

Proof of Lemma 1. Since gay is odd, (4) implies $F \equiv G \pmod{Py}$, where $P = 2^e ga$. But $F = Pxy + \phi$, $\phi \equiv G \pmod{Py}$, $\phi = G + PyQ$. Hence $F = G$ when $x = -Q$.

Proof of Lemma 2. Case 1. $a \equiv 0$, $b \not\equiv 0(p)$. Let $y = 1$. Then $f \equiv bx + c \equiv k(p)$, which is solvable. Assume $f = k + Hp^m$, $m \geqq 1$. Then $f \equiv k(p^{m+1})$ is solvable with x replaced by $x + Xp^m$, since $H + bX \equiv 0(p)$ has a solution X. In this case $\Delta \equiv b^2(p)$, hence $(\Delta/p) = 1$.

Case 2. $a \equiv b \equiv 0(p)$. Then $f \equiv cy^2(p)$ and $f \equiv k(p)$ is not solvable for some k. In this case $\Delta \equiv 0(p)$.

Case 3. $a \not\equiv 0(p)$. Multiplying (5) by $4a$ we get the equivalent congruence

$$Z^2 - \Delta y^2 \equiv 4ak(p^n), \tag{6}$$

where

$$Z = 2ax + by. \tag{7}$$

When $\Delta \equiv 0(p)$, (6), hence (5) also, is not solvable for some k. When $\Delta \not\equiv 0(p)$, it is well known that (6) is solvable modulo p. The solutions Z, y fix x, modulo p, by (7), so that x, y satisfy (5), modulo p.

Consider $n > 1$. If $(\Delta/p) = -1$, $k = pK$ requires $y \equiv Z \equiv 0(p)$, whence (6) is not satisfied modulo p for some K. If $(\Delta/p) = 1$, the pair Z, y which satisfy (6) modulo p may be chosen so that one of Z, y, hence one of x, $y \not\equiv 0(p)$. Let $j = k + Hp^m$, $m \geqq 1$, one of x, $y \not\equiv 0(p)$. Then $a(x + Xp^m)^2 + b(x + Xp^m)(y + Yp^m) + c(y + Yp^m)^2 \equiv k(p^{m+1})$ if

$$H + MX + NY \equiv 0(p), \tag{8}$$

where $M = 2ax + by$, $N = bx + 2cy$. Congruence (8) is satisfied unless $M \equiv N \equiv 0(p)$, i.e., unless $\Delta x \equiv \Delta y \equiv 0(p)$, which contradicts the hypotheses on Δ, x, and y.

THE CONGRUENCE $F \equiv G \pmod{gay}$

3. **Preliminary results. Discussion of y.** We may factor g and a as follows:

(9) $g = qr$, $a = st$, q and s have the same distinct prime factors; r and t are prime to each other and to both q and s.

Then qs, r and t are relatively prime in pairs. Thus $F \equiv G$ is solvable

modulo ga if solvable modulis qs, r and t. It is solvable modulis qs and r in the four-* and hence the five-variable case. It remains to consider

$$F = G(ty). \tag{10}$$

Let t be the product of powers p^n of distinct primes. We shall use the following theorem:

THEOREM 2. *If for each factor* p^n *of* $t = p_1^{n_1} \cdots p_r^{n_r}$,

(11) $F \equiv G(p^n)$, *with* F *as in* (1) *and* (2), *has a solution* $z, w, v, y = \eta$, *with* $\eta = 1$ *or* π, *where*

(12) π *is an odd prime dividing no one of* g, a, d, α, h, *and not dividing one of* $N = j^2 - 4hl$, $M = A^2 - 4\alpha hC$, $P = 2hB - jA$, *then* (10) *is solvable with* y *odd but not necessarily the same as in the solution of* (11).

Note that by the last paragraph of §1

(13) one of $N, M, P \not\equiv 0$.

First we prove

LEMMA 2A. *The congruence*

(14) $F \equiv G(\pi)$, π *as in* (12), *is solvable with* $y = k\pi$, *where* k *is an arbitrary integer.*

For, dropping the terms of F containing y, and multiplying (14) by $4\alpha h$, we get the equivalent congruence

$$4\alpha hF \equiv gd(Z^2 - \alpha^2 N w^2 - Mv^2 + 2\alpha Pwv) \equiv 4\alpha hG(\pi), \tag{15}$$

where $Z = 2\alpha hz + \alpha jw + Av$, and N, M, P are as in (12). Since $2\alpha h$ is prime to π we may take Z, w, v as new variables in place of z, w, v. If $N = M = 0$, then $P \not\equiv 0$ by (13), and since $2gd\alpha P$ is prime to π by (12), (15) is solvable. Otherwise with $v = 0$ or $w = 0$ according as $N \not\equiv 0$ or $N = 0$, $M \not\equiv 0$, (15) is solvable by Lemma 2, and hence, since $4\alpha h$ is prime to π, (14) is solvable. This completes the proof of Lemma 2A.

Then by hypothesis (11) has a solution $z', w', v', y = \eta$, where $\eta = 1$ or π, and by Lemma 2A, if $\eta = \pi$ (and trivially if $\eta = 1$) $F \equiv G(\eta)$ has a solution $z'', w'', v'', y = \eta$.

By the Chinese Remainder Theorem there exist integers z, w, v such that $z \equiv z'$, $w \equiv w'$, $v \equiv v'$ (mod p^n), and $z \equiv z''$, $w \equiv w''$, $v \equiv v''$ (mod η). Then (11) and (14) have the same solution $z, w, v, y = \eta$, and hence, since η is prime to a and therefore to p,

$$F \equiv G(p^n\eta) \tag{16}$$

* With $v = w = 0$, change h to αh in line 9, p. 174, of the reference previously quoted.

has the same solution $z, w, v, y=\eta$.

For each factor p^n of $t=p_1^{n_1}\cdots p_r^{n_r}$ there are then solutions $z_i, w_i, v_i, y=\eta_i$ of $F\equiv G(p_i^{n_i}\eta_i)$, where $\eta_i=1$ or a prime π_i of type (12). Taking, by the Chinese Remainder Theorem,

$$(17)\qquad Y\equiv\eta_i,\ Z\equiv z_i,\ W\equiv w_i,\ V\equiv v_i \pmod{p_i^{n_i}\eta_i}\quad (i=1,\cdots,r),$$

we have that $F\equiv G(t\zeta)$ has a solution Y, Z, W, V, where $\zeta=\eta_1\eta_2\cdots\eta_r$. Since by (17) $Y=\eta_i(1+k_ip_i^{n_i})$, where $n_i\geqq 1$, $i=1,\cdots,r$, it follows that $Y=\zeta S$, where S contains no factor p of t. We select a prime $\tau=S+X_1t$ of type (12) and not dividing $t\zeta$ from the infinite number of the form $S+Xt$, where X ranges over all integers, and take $y=\zeta\tau$. Then $F\equiv G(t\zeta)$ has a solution $Z, W, V, y=\zeta\tau=\zeta S+X_1t\zeta$, and, by Lemma 2A, $F\equiv G(\tau)$ has a solution $Z', W', V', y=\zeta\tau$. Since τ is prime to $t\zeta$ it follows from the Chinese Remainder Theorem that $F\equiv G(t\zeta\tau)$ has a solution $Z'', W'', V'', y=\zeta\tau$. This completes the proof of Theorem 2.

In applying Theorem 2 we shall proceed in practice as follows. We seek a solution of (11) $F\equiv G(p^n)$, and find that various conditions on the coefficients in F require the consideration of numerous sub-cases. As a first step we consider

$$(18)\qquad F\equiv G(p).$$

When Theorem 2 is applicable we can either set $y=1$ explicitly or show that there is a solution of (18) with $y=r\not\equiv 0(p)$. From the infinite number of primes of the form $r+Xp$, where X runs through all integral values, we select a prime π of type (12) and set $y=\pi$. Then where convenient we make the induction proving (11) solvable with y fixed. When we make the induction through y we show explicitly that y remains prime to p, so that at each stage of the induction it can be chosen a prime of type (12) selected from the infinite number of primes of the form $\eta+Xp^m$, $\eta\not\equiv 0(p)$, $m\geqq 1$.

There remain, besides the certainly non-universal cases, those for which we can prove (18) solvable but find it not convenient, and in some cases not possible, to hold $y\not\equiv 0(p)$ in the solution. In such cases, as in 12123 below, we use the following theorem:

THEOREM 2A. *Let p^n be a typical factor of $t=p_1^{n_1}\cdots p_r^{n_r}$. If, for F as in* (1) *and* (2), *$F\equiv G(p^\sigma)$ has for every $\sigma\geqq n$ a solution $z, w, v, y=p^\delta\eta$, where $\eta=1$ or a prime of type* (12) *and $\delta\geqq 0$ depends upon G, p, n, and F, but not upon σ, then* (10) *$F\equiv G(ty)$ is solvable.*

Let $s=n+\delta$. By hypothesis $F\equiv G(p^s)$ has a solution $z, w, v, y=p^\delta\eta$, where $\eta=1$ or a prime of type (12). Also, by Lemma 2A, $F\equiv G(\eta)$ has a solution

z', w', v', $y=p^{\delta}\eta$. Hence, applying the Chinese Remainder Theorem, $F\equiv G(p^{s}\eta=p^{n}y)$ has a solution Z, W, V, $y=p^{\delta}\eta$. That is, $F\equiv G(p_i^{n_i}y_i)$ has a solution z_i, w_i, v_i, $y_i=p_i^{\delta_i}\eta_i$, where $i=1, \cdots, r$ and each of the η_i is 1 or a prime of type (12).

From this point the part of the proof of Theorem 2 below (16) applies exactly if we delete the now unnecessary statement "where $\eta_i=1$ or a prime π_i of type (12)" and elsewhere replace η_i by y_i. Note that $\zeta=\eta_1\eta_2\cdots\eta_r$ becomes $\zeta=y_1y_2\cdots y_r$.

In view of Theorem 2A it will suffice in practice to prove that, excluding the (here) provably non-universal cases, congruence (11) $F\equiv G(p^{n})$ has a solution z, w, v, $y=p^{\delta}r$, $r\not\equiv 0(p)$, where δ is unchanged in the induction from modulus p^{m} to modulus p^{m+1}. This will be true when y remains fixed in the induction, and will be shown explicitly when the induction is through y.

4. **The congruence $F\equiv G \pmod t$.** Since t is prime to g, d, and h, but divides a, the congruence

$$F \equiv G(p^{n}), \tag{19}$$

where p is a prime factor of t, is equivalent to

$$F = gby^2 + cyz + gd[\alpha(hz^2 + jzw + lw^2) + Azv + Bwv + Cv^2] \equiv G(p^{n}). \tag{20}$$

We may assume without loss of generality that

$$G \not\equiv 0(p^2). \tag{21}$$

For suppose $G=p^{2s}G_1$, where $G_1\not\equiv 0(p^2)$. If $n\leqq 2s$, (20) is solvable with $y=p^{n}$, $z=w=v=0$. If $n>2s$, take $y=p^{s}y'$, $z=p^{s}z'$, $w=p^{s}w'$, $v=p^{s}v'$. Division by p^{2s} yields the equivalent congruence $F(y', z', w', v')\equiv G_1(p^{n-2s})$, which justifies the assumption.

In the following scheme of subdivision, **121** and **122** are subheads of **12**, etc.

1. $C\not\equiv 0(p)$.

11. $b\equiv c\equiv D\equiv E\equiv K\equiv 0(p)$,

where $D=4\alpha hC-A^2$, $E=2\alpha jC-AB$, $K=4\alpha lC-B^2$. Then F is not universal.

Multiplying both sides of (20) by $4C$, we have

$$F_1 = 4CF = gd[V^2 + Dz^2 + 2Ezw + Kw^2] + 4C(gby^2 + cyz) \equiv 4CG(p^{n}), \tag{22}$$

where $V=2Cv+Az+Bw$. Since our moduli are powers of p we may take V, z, w, y as new variables in place of v, z, w, y, and (22) is equivalent to (20). By the conditions of **11**, $F_1\equiv gdV^2\equiv 4CG(p)$, which is not solvable for some G.

12. One of b, c, D, E, $K\not\equiv 0(p)$.

121. $b\not\equiv 0(p)$. By (22)

(23) $F_2 = gbF_1 = CY^2 - Lz^2 + g^2db[V^2 + 2Ezw + Kw^2] \equiv k(p^n)$,

where

$$Y = 2gby + cz,\ L = RC + g^2dbA^2,\ R = c^2 - 4g^2dba h,\ k = 4gbCG.$$

1211. $(-4g^2dbC/p) = (-dbC/p) = 1$. By Lemma 2, (23) is solvable with $z = w = 0$.

1212. $(-dbC/p) = -1$.

12121. One of $L, E, K \not\equiv 0(p)$. Then (23) is solvable.

Take $V = 1$. Then (23) has a solution Y, z, w, modulo p, with (1) $w = 0$, (2) $z = 0$, (3) $z = 1$ according as (1) $L \not\equiv 0$, (2) $L \equiv 0$, $K \not\equiv 0$, (3) $L \equiv K \equiv 0$, $E \not\equiv 0(p)$. Assume $F_2 = k + Hp^m$, $m \geqq 1$, $V \not\equiv 0(p)$. Then $F_2 \equiv k(p^{m+1})$ with Y, z, w (and hence y) unchanged and with V replaced by $V + p^m X \not\equiv 0(p)$, since $2g^2dbV \not\equiv 0(p)$.

12122. $L = pL_1$, $E = pE_1$, $K = pK_1$, $T = g^2dbE_1^2 + L_1K_1 \equiv 0(p)$. Then F is not universal.

Since $(-dbC/p) = -1$, the solution of (23) modulo p with $k = pk_1$ requires $Y \equiv V \equiv 0(p)$, so that, dividing out p, $F \equiv pk_1(p^2)$ reduces to $-L_1z^2 + g^2db(2E_1zw + K_1w^2) \equiv k_1(p)$, which by Lemma 2 is not solvable for some k_1.

12123. $L = pL_1$, $E = pE_1$, $K = pK_1$, $T \not\equiv 0(p)$. Then (23) is solvable.

By Lemma 2 we may fix Y and V modulo p so that

$$CY^2 + g^2dbV^2 \equiv k(p), \tag{24}$$

hence $k - CY^2 - g^2dbV^2 = pQ$. Then (23) modulo p^2 reduces to

$$-L_1z^2 + g^2db(2E_1zw + K_1w^2) \equiv Q(p), \tag{25}$$

which is solvable by Lemma 2. This fixes z and w, modulo p, and hence also y and v through Y and V. Assume $F_2 = k + Hp^m$, $m \geqq 2$, and assume first $V \not\equiv 0(p)$. Then $F_2 \equiv k(p^{m+1})$ with Y, z, w unchanged and with v replaced by $v + p^m v'$ (so that V is replaced by $V + 2Cp^m v'$), since $2g^2dbV \not\equiv 0(p)$.

It remains to complete the induction on (23) from $m \geqq 2$ to $m+1$ when $V \equiv 0(p)$. First assume $k \not\equiv 0(p)$, so that $Y \not\equiv 0(p)$ by (24). If $y \not\equiv 0(p)$ we complete the induction by replacing y by $y + p^m y' \not\equiv 0(p)$, so that $Y = 2gby + cz$ is replaced by $Y + 2gbp^m Y' \not\equiv 0(p)$. If $y \equiv 0(p)$ then $cz \not\equiv 0(p)$. We set $y = p$ and replace z by $z + p^m Z$, hence Y by $Y + cp^m Y' \not\equiv 0(p)$ and $V = 2Cv + Az + Bw$ by $V + Ap^m Z \equiv 0(p)$. The induction is complete since $2(g^2dbAV + cCY) \equiv 2cCY \not\equiv 0(p)$.

Next assume $k=pk_1$, where $k_1\not\equiv 0(p)$ by (21). Then since $(-dbC/p)=-1$, $Y\equiv V\equiv 0(p)$ is required. Note that $c\equiv 0(p)$ then *requires* that $y\equiv 0(p)$. Since $k_1\not\equiv 0(p)$, $Q\not\equiv 0(p)$ by the equation just below (24), hence one of z, $w\not\equiv 0(p)$ in the solution of (25). Assume $F_2=k+Hp^m$, $m\geqq 2$, one of z, $w\not\equiv 0(p)$. Then $F_2\equiv k(p^{m+1})$ with z and w replaced respectively by $z+p^{m-1}Z$, $w+p^{m-1}W$ if $C(Y+cp^{m-1}Z)^2+g^2db(V+Ap^{m-1}Z+Bp^{m-1}W)^2\equiv CY^2+g^2dbV^2(p^{m+1})$ and $H+2\theta_1Z+2g^2db\theta_2W\equiv 0(p)$, where $\theta_1=-L_1z+g^2dbE_1w$, $\theta_2=E_1z+K_1w$. The latter congruence is solvable, since $\theta_1\equiv\theta_2\equiv 0(p)$ requires that $Tz\equiv Tw\equiv 0(p)$, contradicting the conditions on T, z, and w. The former congruence is also solvable if $Y\equiv V\equiv 0(p^2)$, $m\geqq 3$. For the case $m=2$, with z and w fixed by (25) we hold $Y\equiv V\equiv 0(p^2)$ by adjustment of y and v. The latter need not be changed thereafter, since if $Y\equiv V\equiv 0(p^2)$ then $Y+p^{m-1}cZ\equiv V+p^{m-1}(AZ+BW)\equiv 0(p^2)$ for $m\geqq 3$.

122. $b\equiv 0$, $c\not\equiv 0(p)$. By Lemma 2, (20) is solvable with $w=v=0$, since the Δ of Lemma $2=c^2-4g^2dbh\equiv c^2(p)$, hence $(\Delta/p)=1$.

123. $b=pb_1$, $c=pc_1$, $D\not\equiv 0(p)$. By (22)

$$F_3 = gdDF_1 = g^2d^2DV^2 + Z^2 + g^2d^2\theta w^2 + 4p\delta_1Cy^2 - 4p\gamma_1yw \equiv k(p^n), \tag{26}$$

where

$$Z = gdDz + gdEw + 2cCy,\quad \theta = DK - E^2,\quad \delta = g^2bdD - c^2C = p\delta_1,$$

$$\gamma = gdcCE = p\gamma_1,\quad k = 4gdCDG.$$

Applying to (26) the arguments of **121** as applied to (23), we find (26) solvable unless $\theta=p\theta_1$, $(-D/p)=-1$, and $\gamma_1^2-g^2d^2C\theta_1\delta_1\equiv 0(p)$, in which case F is not universal. To make sure that the power of p in y is not indefinitely increased in the induction we note that by the argument of **121** as obviously modified to fit the new lettering the induction is through V and Z (i.e., v and z) unless $k=pk_1$, $k_1\not\equiv 0(p)$, $V\equiv Z\equiv 0(p)$, with one of y, $w\not\equiv 0(p)$. Then if $y\equiv 0(p)$, $\theta_1w\not\equiv 0(p)$, and the induction can be made through w alone; otherwise y remains $\not\equiv 0(p)$ in the required replacement of y by $y+p^{m-1}Y$.

124. $b=pb_1$, $c=pc_1$, $D=pD_1$, $K\not\equiv 0(p)$. By (22)

$$F_4 = KF_1 = gd[W^2 + KV^2 + \theta z^2] + 4pCK(gb_1y^2 + c_1yz) \equiv 4CKG(p^n), \tag{27}$$

where

$$W = Kw + Ez,\quad \theta = DK - E^2.$$

As in **123**, (27) is solvable unless $\theta=p\theta_1$, $(-K/p)=-1$, and $c_1^2CK-g^2db_1\theta_1\equiv 0(p)$, in which case F is not universal.

125. $b=pb_1$, $c=pc_1$, $D=pD_1$, $K=pK_1$, $E\not\equiv 0(p)$.

In this case (22) is solvable by Lemma 2 with $V=0$, $y=p^n\eta$, since the Δ of Lemma $2\equiv 4E^2(p)$, hence $(\Delta/p)=1$.

2. $C\equiv 0(p)$, and one of A, $B\not\equiv 0(p)$. Then (20) is solvable.

Fix z and w so that $Az+Bw=M\not\equiv 0(p)$, and take $y=1$. Then (20) yields

$$L(v) = gd(Mv + Cv^2) \equiv k(p^n), \tag{28}$$

where k is a constant. This is solvable, modulo p. Assume $L(v)=k+Hp^m$, $m\geqq 1$, and take $v'=v+Xp^m$. Then

$$\begin{aligned} L(v') &\equiv k + p^m[H + gdMX](p^{m+1}) \\ &\equiv k(p^{m+1}) \end{aligned}$$

by choice of X, completing the induction.

3. $A=pA_1$, $B=pB_1$, $C=pC_1$. Then $\alpha\not\equiv 0(p)$ by (3).

31. $N=j^2-4hl\not\equiv 0(p)$.

Since p is odd and does not divide $gd\alpha h$, multiplication of (20) by $4gd\alpha h$ yields the equivalent congruence

$$4gd\alpha h(gby^2 + cyz) + g^2d^2\alpha^2[(2hz + jw)^2 - Nw^2] + \xi \equiv 4gd\alpha hG(p^n), \tag{29}$$

where

$$\xi = 4pg^2d^2\alpha h(A_1z + B_1w + C_1v)v. \tag{30}$$

The product of (29) by N gives

$$S(U, V, y, z, w, v) = NU^2 - V^2 + Jy^2 + 4pD(A_1zv + B_1wv + C_1v^2) \equiv k(p^n), \tag{31}$$

where

$$U = gd\alpha(2hz + jw) + cy, \tag{32}$$

$$V = Ngd\alpha w + cjy, \tag{33}$$

$$J = c^2j^2 - NR,\ R = c^2 - 4g^2db\alpha h,\ k = 4gd\alpha hNG,\ D = Ng^2d^2\alpha h \not\equiv 0(p). \tag{34}$$

311. $J\not\equiv 0(p)$.

312. $(N/p)=1$.

In cases 311 and 312, (20) is solvable with $v=0$, as shown in the four-variable case.

313. $(N/p)=-1$ and $J=pJ_1$.

The result is given in

(35) $\begin{cases} \text{when } Q \equiv 0(p), F \text{ is not universal;} \\ \text{when } Q \not\equiv 0(p), (31) \text{ is solvable, where } Q = \alpha C_1 J_1 N - c^2 h(jB_1 - 2A_1 l)^2. \end{cases}$

Since $N \not\equiv 0(p)$,

(36) one of $j, l \not\equiv 0(p)$.

Since $J \equiv 0(p)$, (31) gives

$$NU^2 - V^2 \equiv k(p). \tag{37}$$

This is solvable by Lemma 2, fixing U and V modulo p. It remains to test (31) modulo p^m, $m \geqq 2$.

3131. $C \equiv 0(p)^2$.

31311. $c \equiv 0(p)$. Then F is not universal.

For, by (37), (33), and (32), $k = pK$ requires $U \equiv V \equiv w \equiv z \equiv 0(p)$. By (31), $S \equiv Jy^2(p^2) \not\equiv pK(p^2)$ for some K.

31312. $\mu = 2A_1 l - jB_1 \equiv 0(p)$. Then F is not universal.

Eliminating y from (32) and (33) and replacing $j^2 - N$ by $4hl$, we get

$$jU - V \equiv 2gd\alpha h(jz + 2lw)(p). \tag{38}$$

Multiplying (38) by B_1 and replacing jB_1 by $2A_1 l$, we get

$$(jU - V)B_1 \equiv 4gd\alpha hlM(p), \tag{39}$$

where

$$M = A_1 z + B_1 w. \tag{40}$$

By (37) and (39) $k = pK$ requires $U \equiv V \equiv lM \equiv 0(p)$. The condition $l \equiv 0(p)$ requires $j \not\equiv 0(p)$ by (36), whence by (38) and the condition that $\mu \equiv 0(p)$, $z \equiv B_1 \equiv 0(p)$. Hence $k = pK$ requires $M \equiv 0(p)$. By (31) $S \equiv Jy^2(p^2) \not\equiv pK(p^2)$ for some K.

31313. $c\mu \not\equiv 0(p)$. Then (31) is solvable.

Since $\mu = 2A_1 l - jB_1 \not\equiv 0(p)$,

$$jB_1 = 2A_1 l + r, \text{ where } r \not\equiv 0(p). \tag{41}$$

Multiplying (38) by B_1 and replacing jB_1 by $2A_1 l + r$, we get

$$(jU - V)B_1 - 2gd\alpha hrz \equiv 4gd\alpha hlM(p^n), \text{ with } M \text{ as in (40)}. \tag{42}$$

Noting (36) and the fact that U and V are fixed, modulo p, by (37), we have three subcases:

When $i \equiv 0(p)$, $jB_1 \equiv r \not\equiv 0(p)$ by (41), and z is fixed modulo p by (38). Choose w so that, by (40), $M \not\equiv 0(p)$. Then y is fixed modulo p by (32) or (33) (consistent through (38)).

When $j \equiv 0(p)$, $2A_1 l \equiv -r \not\equiv 0(p)$ by (41), and w is fixed modulo p by (33). Choose z so that, by (40), $M \not\equiv 0(p)$, fixing y modulo p by (32).

When $jl \not\equiv 0(p)$, choose z so that the left side of (42) $\not\equiv 0(p)$.

In all cases we have $M = A_1 z + B_1 w \not\equiv 0(p)$. By (31), taking $C = p^2 C_2$,

$$L(v) = 4Dp(Mv + pC_2 v^2) \equiv K(p^n), \tag{43}$$

where

$$K = k - NU^2 + V^2 - Jy^2 = pK_1,$$

with K_1 independent of v. Dividing out p we find (43), hence (31), solvable by the method used for (28).

Note that (35) is satisfied in our results for **3131**.

3132. $C = pC_1$, $C_1 \not\equiv 0(p)$.

31321. $c \equiv J_1 \equiv 0(p)$. Then F is not universal.

By (37), (33) and (32), $k = pK$ requires $U \equiv V \equiv w \equiv z \equiv 0(p)$. By (31), noting $J = pJ_1$, $S \equiv 4pDC_1 v^2 (p^2) \not\equiv pK(p^2)$ for some K.

31322. $c \equiv 0$, $J_1 \not\equiv 0(p)$. Then (31) is solvable.

U, V, w and z are fixed, modulo p, by (37), (33), and (32). Multiplying both sides of (31) by C_1, we get

$$pC_1 J_1 y^2 + pD\Delta^2 \equiv K(p^2), \tag{44}$$

where

$$\Delta = 2C_1 v + A_1 z + B_1 w, \tag{45}$$

$$K = C_1(k - NU^2 + V^2) + pD(A_1 z + B_1 w)^2 = pK_1. \tag{46}$$

Dividing out p, we find (44) solvable by Lemma 2, fixing y, Δ, and v, modulo p, by (44) and (45). Thus (31) is solvable modulo p^2. The induction will be completed in **313234**.

31323. $c \not\equiv 0(p)$.

313231. $j \equiv P \equiv 0(p)$, $P = \alpha C_1 J_1 + c^2 l A_1^2$. Then F is not universal.

By (32) we have, with $j \equiv 0(p)$,

$$c^2 y^2 \equiv (U - 2gd\alpha hz)^2 (p). \tag{47}$$

Multiplying (44) by c^2, replacing K and $c^2 y^2$ by their values in (46) and (47) respectively, and then D in the coefficient of z by its value in (34), and noting that $N = j^2 - 4hl \equiv -4hl(p)$, we have

$$pDc^2\Delta^2 + 4p\alpha h^2g^2d^2Pz^2 - pTz \equiv K_2(p^2), \tag{48}$$

where

$$T = 4C_1J_1gd\alpha hU + 2c^2DA_1B_1w, \tag{49}$$

$$K_2 = c^2C_1(k - NU^2 + V^2) + p(Dc^2B_1^2w^2 - C_1J_1U^2) = pK_3. \tag{50}$$

By (37), (33), and (49), $k = pK$ requires $U \equiv V \equiv w \equiv T \equiv 0(p)$, whence by (50) $K_2 \equiv pc^2C_1K(p^2)$. We then have by (48) and the fact that $P \equiv 0(p)$

$$pDc^2\Delta^2 \equiv pc^2C_1K(p^2),$$

which is not solvable for some K.

Note that $j \equiv P \equiv 0(p)$ is equivalent to $Q \equiv 0(p)$, with Q as in (35).

313232. $j \equiv 0, P \not\equiv 0(p)$. Then (31) is solvable.

U, V, and T are fixed, modulo p, by (37), (33), and (49). Completing the square in z in (48) we have

$$p\delta\Delta^2 + pZ^2 \equiv K_4(p^2), \tag{51}$$

where

$$Z = 8\alpha h^2g^2d^2Pz - T, \tag{52}$$

$$K_4 = 16\alpha h^2g^2d^2PK_2 + pT^2 = pK_5, \quad \delta = 16\alpha h^2g^2d^2PDc^2 \not\equiv 0(p). \tag{53}$$

Dividing out p we find (51) solvable by Lemma 2, fixing Δ and Z, modulo p, and hence also z, v, and y by (52), (45), and (32) respectively. Thus (31) is solvable modulo p^2. The induction will be completed in **313234**.

313233. $j \not\equiv 0$, $Q \equiv 0(p)$, with Q as in (35). F is not universal.

Eliminating y and z from (44) (with K replaced as in (46)) by means of (33) and (38), we get

$$p(E\Delta^2 + Lw^2 - Mw) \equiv K_6(p^2), \tag{54}$$

where

$$E = D(2cjgd\alpha h)^2 \not\equiv 0(p), \tag{55}$$

$$L = Dh(2gd\alpha)^2Q, \tag{56}$$

$$M = 4gd\alpha hD[2\alpha C_1J_1V + c^2A_1(jU - V)(jB_1 - 2A_1l)], \tag{57}$$

$$K_6 = (2gd\alpha hcj)^2C_1(k - NU^2 + V^2) + p[c^2DA_1^2(jU - V)^2 - C_1J_1(2gd\alpha hV)^2] = pK_7. \tag{58}$$

By (37) and (57), $k = pK$ requires $U \equiv V \equiv M \equiv 0(p)$. Since Q and hence $L \equiv 0(p)$, we get, from (54) and (58), $pE\Delta^2 \equiv p(2gd\alpha hcj)^2C_1K(p^2)$, which is not solvable for some K.

313234. $jQ \not\equiv 0(p)$, with Q as in (35). Then (31) is solvable.

U, V, and M are fixed, modulo p, by (37) and (57). Completing the square in (54), we get

$$4pLE\Delta^2 + pW^2 \equiv K_8(p^2), \tag{59}$$

where

$$W = 2Lw - M, \tag{60}$$

$$K_8 = 4LK_6 + pM^2 = pK_9. \tag{61}$$

Dividing out p we find (59) solvable by Lemma 2, fixing Δ and W, modulo p, and hence also w, y, z and v by (60), (33), (32) and (45) respectively. Thus (31) is solvable modulo p^2.

It remains to complete the induction in cases **31322**, **313232**, and **313234**. This will be done in subdivisions of **313234**. For convenience we may rewrite (31) as follows:

$$S = NU^2 - V^2 + pJ_1y^2 + 4pDZv + 4pDC_1v^2 \equiv k(p^n), \tag{62}$$

where

$$Z = A_1z + B_1w, \quad Dgd\alpha hNC_1 \not\equiv 0(p),$$

and y, z, w, v are fixed, modulo p. Since (62) is solvable modulo p^2 with the exceptions noted, we may have $m \geqq 2$ in the induction.

3132341. $U \not\equiv 0(p)$.

Assume $S(z) = k + Hp^m$. Take $z' = z + Xp^m$. Then, by (32), $U' = U + 2hgd\alpha Xp^m \not\equiv 0(p)$. By (62) $S(z') \equiv k + p^m[H + 4gd\alpha hNX]$ (p^{m+1}), etc., completing the induction.

3132342. $U \equiv 0$, $V \not\equiv 0(p)$.

Assume $S(w) = k + Hp^m$. Take $w' = w + Xp^m$. Then by (32) and (33), $U' = U + gd\alpha jXp^m \equiv 0(p)$, $V' = V + gd\alpha NXp^m \not\equiv 0(p)$. By (62) $S(w') \equiv k + p^m[H - 2gd\alpha NV'X]$ (p^{m+1}), etc., completing the induction.

3132343. $U \equiv V \equiv 0(p)$.

31323431. $v \not\equiv 0(p)$.

Assume $S(y, z, w, v) = k + Hp^m$. Take $z' = z + Xp^{m-1}$. Then by (32) and the definition of Z below (62), $U' = U + 2hgd\alpha Xp^{m-1} \equiv 0(p)$, $Z' = Z + A_1p^{m-1}$, and $S(z') \equiv k + p^{m-1}[Hp + 4L_1X]$ (p^{m+1}), where $L_1 = NUhgd\alpha + pDA_1v$. The induction will be complete unless $L_1 \equiv 0(p^2)$. Similarly, taking in succession

$y'=y+Xp^{m-1}$ (except when $y\equiv 0(p)$) and $w'=w+Xp^{m-1}$, we get in succession the two following coefficients of X:

$$L_2 = 2(NcU - cjV + pJ_1y),$$
$$L_3 = 2(gd\alpha jNU - gd\alpha NV + 2pDB_1v).$$

Hence with the proper substitution the induction is complete unless $y\equiv 0(p)$ or

$$L_1 \equiv L_2 \equiv L_3 \equiv 0(p). \tag{63}$$

Eliminating U and V from (63) and dividing out p, we get

$$2cDv(2A_1l - jB_1) + Ngd\alpha J_1y \equiv 0(p). \tag{64}$$

This will be considered in conjunction with (67) below.

Again, take $z'=z(1+Xp^{m-1})$, $y'=y(1+Xp^{m-1})$, $w'=w(1+Xp^{m-1})$. Then since $U\equiv V\equiv 0(p)$, we have $U'=U(1+Xp^{m-1})\equiv 0(p)$, $V'=V(1+Xp^{m-1})\equiv 0(p)$, $Z'=Z(1+Xp^{m-1})$. Finally, take $v'=v(1+Xp^{m-1})\not\equiv 0(p)$. The induction will be valid in one of these last two cases unless

$$L_4 \equiv L_5 \equiv 0(p), \tag{65}$$

where

$$L_4 = 2(J_1y^2 + 2DZv),\quad L_5 = 4Dv(Z + 2C_1v); \tag{66}$$

Z is as defined below (62). Eliminating Z from (65), we get

$$4C_1Dv^2 - J_1y^2 \equiv 0(p). \tag{67}$$

Since $4C_1Dv\not\equiv 0(p)$, (67) is impossible if $y\equiv 0(p)$; hence in that case one of L_4, $L_5\not\equiv 0(p)$, and the induction is complete with the power of p in y unaltered.

Finally, eliminating y from (64) and (67), replacing D by $Ng^2d^2\alpha h$, and dropping common factors which we know to be prime to p (as g, d, α, h, N, C), we get $v^2Q\equiv 0(p)$, with Q as in (35), which contradicts the hypotheses on Q and v. Hence at least one of the five induction substitutions above succeeds, and the induction is complete.

31323432. $v\equiv 0(p)$.

By (21) we may assume that $G\not\equiv 0(p^2)$, hence in (62) $k=4gd\alpha hGN\not\equiv 0(p^2)$. Then by (62) $J_1y\not\equiv 0(p)$. Assume $S(y, z, w, v)=k+Hp^m$, where $U\equiv V\equiv 0$, $J_1y\not\equiv 0(p)$. Take $y'=y(1+Xp^{m-1})\not\equiv 0(p)$, $z'=z(1+Xp^{m-1})$, $w'=w(1+Xp^{m-1})$. Then $U'=U(1+Xp^{m-1})\equiv 0(p)$, $V'=V(1+Xp^{m-1})\equiv 0(p)$, $Z'=Z(1+Xp^{m-1})$.

By (62) $S(y', z', w', v') \equiv k + p^m[H + 2J_1y^2X](p^{m+1})$, etc., completing the induction. This completes 313. Examination of the subcases reveals that (35) is a complete statement of the results.

32. $N = pN_1$. Then, since $N \equiv 0$, $h \not\equiv 0(p)$,

$$\text{either } j \equiv l \equiv 0, \text{ or } jl \not\equiv 0(p). \tag{68}$$

321. $jl \not\equiv 0(p)$. Then (31) is solvable, as shown in the four-variable case (§14, I).

322. $j \equiv l \equiv 0(p)$.

By (29),

$$\begin{aligned}\phi &= Z^2 - Ry^2 + g^2d^2\alpha[\alpha j(4hzw + jw^2) - \alpha pN_1w^2 + 4ph(A_1zv + B_1wv + C_1v^2)] \\ &\equiv k(p^n),\end{aligned} \tag{69}$$

where

$$Z = 2gd\alpha hz + cy, \tag{70}$$

$$R = c^2 - 4g^2d\alpha hb. \tag{71}$$

By (69) and 322 we have

$$Z^2 - Ry^2 \equiv k(p). \tag{72}$$

3221. $(R/p) = 1$. Then by Lemma 2, (69), hence (19), is solvable with $w = v = 0$.

3222. $R \equiv 0(p)$. Then F is not universal.

For then (72) has no solution Z for some k.

3223. $(R/p) = -1$. The result is as follows:

$$\begin{cases}\text{when } I \equiv 0(p), F \text{ is not universal;} \\ \text{when } I \not\equiv 0(p), (69) \text{ is solvable, where } I = hB_1^2 + \alpha N_1C_1.\end{cases} \tag{73}$$

Z, y and z are fixed, modulo p, by (72) and (70). It remains to determine when (69) is solvable modulis p^2 and p^n.

32231. $C_1 \equiv B_1 \equiv 0(p)$. Then F is not universal.

For, by (72) and (70), $k = pK$ requires $Z \equiv y \equiv z \equiv 0(p)$. By (69), $\phi \equiv -pg^2d^2\alpha^2N_1w^2(p^2) \not\equiv pK(p^2)$ for some K.

32232. $C_1 \equiv 0$, $B_1 \not\equiv 0(p)$. Then (69) is solvable.

Choose w so that $A_1z + B_1w = M \not\equiv 0(p)$. By (69)

$$4g^2d^2\alpha hpMv \equiv K(p^2), \tag{74}$$

where

$$K = k - Z^2 + Ry^2 - g^2d^2\alpha^2(4hjzw + j^2w^2) = pK_1 \text{ (independent of } v).$$

Dividing out p we find (74) solvable. Using (69), assume $\phi(v) = \phi(y, z, w, v) = k + p^mH$, with $m \geqq 2$. Take $v' = v + Xp^{m-1}$. Then $\phi(v') \equiv k + p^m[H + 4g^2d^2\alpha hMX](p^{m+1})$, etc., completing the induction.

32233. $C_1 \not\equiv 0$, $I \equiv 0(p)$, with I as in (73). F is not universal.

Completing the square in (69), we get

$$pEV^2 + \delta w^2 + \epsilon w \equiv K_1(p^n), \tag{75}$$

where

$$V = 2C_1v + B_1w + A_1z, \tag{76}$$

$$E = g^2d^2\alpha h \not\equiv 0(p), \tag{77}$$

$$\delta = g^2d^2\alpha(\alpha C_1j^2 - pI), \text{ with } I \text{ as in (73)}, \tag{78}$$

$$\epsilon = 2g^2d^2\alpha h(2\alpha jC_1 - pA_1B_1)z, \tag{79}$$

$$K_1 = C_1(k - Z^2 + Ry^2) + pg^2d^2\alpha hA_1^2z^2 = pK_2. \tag{80}$$

By (72) and (70), $k = pK$ requires $Z \equiv y \equiv z \equiv 0(p)$, and hence, since $j \equiv I \equiv 0(p)$, $\delta \equiv \epsilon \equiv 0(p^2)$. Then by (75) and (80),

$$pEV^2 \equiv pC_1K(p^2), \tag{81}$$

which is not solvable for some K.

32234. $C_1I \not\equiv 0(p)$, with I as in (73). Then (69) is solvable.

Z, y and z are fixed, modulo p, by (72) and (70). Writing $\delta = p\delta'$, $\epsilon = p\epsilon'$ (since $j \equiv 0(p)$), we have by (75) and (80), after dividing out p,

$$EV^2 + \delta'w^2 + \epsilon'w \equiv K_2(p^{n-1}), \tag{82}$$

where $\delta' \equiv -g^2d^2\alpha I \not\equiv 0(p)$. Since $E\delta' \not\equiv 0(p)$, we may complete the square in w and have (82) solvable modulo p, fixing V, w and v, modulo p, by (82) and (76). Hence (69) is solvable modulo p^2.

Using (69), assume $\phi = k + p^mH$, with $m \geqq 2$. By (70), if $Z \equiv 0(p)$, either $y \not\equiv 0(p)$ or $z \equiv y \equiv 0(p)$. Also, if $Z \equiv z \equiv y \equiv 0(p)$ we may assume that one of N_1w, $v \not\equiv 0(p)$, since $j \equiv 0(p)$ and by (21) k may be taken $\not\equiv 0(p^2)$. The following induction substitutions then cover all cases:

(a) $Z \not\equiv 0(p)$. Take $z' = z + Xp^m$, hence $Z' = Z + 2gd\alpha hXp^m \not\equiv 0(p)$.

(b) $Z \equiv 0$, $y \not\equiv 0(p)$. Take $z' = z(1 + Xp^m)$, $y' = y(1 + Xp^m)$, hence $Z' = Z(1 + Xp^m) \equiv 0(p)$.

(c) $Z\equiv z\equiv y\equiv B_1w\equiv 0$, $v\not\equiv 0(p)$. Take $v'=v+Xp^{m-1}$.

(d) $Z\equiv z\equiv y\equiv N_1\equiv 0$, $B_1wv\not\equiv 0(p)$. Take $w'=w+Xp^{m-1}$.

(e) $Z\equiv z\equiv y\equiv B_1v\equiv 0$, $N_1w\not\equiv 0(p)$. Take $w'=w+Xp^{m-1}$.

(f) $Z\equiv z\equiv y\equiv 0$, $B_1N_1wv\not\equiv 0(p)$. Take $w'=w+Xp^{m-1}$, $v'=v+Yp^{m-1}$. Then $\phi\equiv k+p^m[H+LX](p^{m+1})$, etc., completing the induction in cases (a) to (e) inclusive, where $L\not\equiv 0(p)$ and is as follows:

(a) $4gd\alpha hZ$; (b) $-2Ry^2$; (c) $8g^2d^2\alpha hC_1v$; (d) $4g^2d^2\alpha hB_1v$; (e) $-2g^2d^2\alpha N_1w$.

In case (f), $\phi\equiv k(p^{m+1})$ unless

$$S\equiv T\equiv 0(p), \tag{83}$$

where

$$S = 2hB_1v - \alpha N_1w,\quad T = 2C_1v + B_1w.$$

But on eliminating w, (83) is equivalent to $2vI\equiv 0(p)$, contradicting the hypotheses, hence (83) is impossible and the induction is complete.

The results in the subcases of 3223 satisfy (73).

We have now proved the solvability of (19), and hence, by Theorems 2 and 2A, of (10), except in cases (84) below.

Let p be any prime dividing a but not g. Let the appearance of b_1 indicate that $b=pb_1$, of D_1 that $D=pD_1$, etc. Define

$$D = 4\alpha hC - A^2,\quad E = 2\alpha jC - AB,\quad K = 4\alpha lC - B^2,\quad R = c^2 - 4g^2db\alpha h,$$
$$L = RC + g^2dbA^2,\quad \theta = DK - E^2,\quad \delta = g^2dbD - c^2C,\quad \gamma = gdcCE,$$
$$N = j^2 - 4hl,\quad J = c^2j^2 - NR,\quad I = hB_1 - \alpha N_1C_1,$$
$$Q = \alpha C_1J_1N - c^2h(jB_1 - 2lA_1)^2.$$

Then F is not universal in the following cases:

1. $C\not\equiv 0(p)$, and one of 11 to 14 holds:

(84)

11. $b\equiv c\equiv D\equiv E\equiv K\equiv 0(p)$;
12. $(-dbC/p)=-1$, $g^2dbE_1^2+L_1K_1\equiv 0(p)$;
13. $(-D/p)=-1$, $\gamma_1^2-g^2d^2C\theta_1\delta_1\equiv 0(p)$;
14. $(-K/p)=-1$, $c_1^2CK-g^2d_1b\theta_1\equiv 0(p)$;

2. $A\equiv B\equiv C\equiv 0(p)$, and one of 21, 22 holds:

21. $J\equiv Q\equiv 0(p)$, $(N/p)=-1$;
22. $N\equiv j\equiv 0(p)$, and either $R\equiv 0(p)$ or $(R/p)=-1$ and $I\equiv 0(p)$.

Since y is odd we then have, by Lemma 1,

THEOREM 3. *If $e=0$, F is universal except in cases* (84).

REMARKS ON THE CONGRUENCE $F \equiv G \pmod{2^n}$

5. **The briefer results.** The initial problem was solved completely in the writer's thesis, but the conditions upon the coefficients as found are so numerous that the bare listing of the results, except those given below for the case $e=1$, requires a prohibitive amount of space. We shall omit further proofs and close with the statements of two fundamental lemmas which give additional freedom in the choice of y, and of the theorem for the case $e=1$.

LEMMA 3. *If there exists an odd y satisfying $(4)_2$, it may be chosen congruent to any desired odd residue, modulo 2^n.*

LEMMA 4. *If the solution of*

$$F \equiv G(2^e) \tag{85}$$

requires the factor 2^s in y, where $s \geqq 0$ depends upon G, then F is universal, subject to exceptions (84), *if and only if*

$$F \equiv G(2^{e+s}) \tag{86}$$

is solvable with $x=0$ for every pair G, s.

THEOREM 4. *When $e=1$, F is universal subject to* (84) *unless* (a), *$bcd\alpha h$ is odd, $l \equiv B \equiv C \equiv 0(4)$, j and A are even, or* (b), *$d=2D$, c is even, and b or D is even. If either* (a) *or* (b) *holds, F is not universal.*

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.