UNIVERSAL QUADRATIC FORMS*

BY

L. E. DICKSON

1. A form is called universal if it represents all integers, and *Null* if it is zero when the variables are integers not all zero. We shall determine all universal Null quadratic forms F in n variables for $n \leqq 4$.

For $n=3$, F is readily reduced to $2^e gaxy+f$, where $f=gby^2+cyz+gdz^2$, ga is odd, a is prime to d, and g to c. Let R be the discriminant of f. Let t be the the largest divisor of a which is prime to g. Then F is universal if and only if R is a quadratic residue of t and one of the following sets of conditions holds: (I) $e=0$; (II) c even, $e=1$, either d is odd, or $d \equiv 2 \pmod 4$ and b is odd; (III) c odd, $e \geqq 1$, bd even. There is a canonical form (§21) which depends only on the Hessian.

For $n=4$ numerous subdivisions arise. There is almost an even chance that a Null form taken at random is universal. The conditions for universality are much milder for $n=4$ than for $n=3$. They are still milder for $n \geqq 5$, the theory for which is under elaboration in a Chicago thesis.

2. **Reduction to normal form.** Let $\xi, \eta, \cdots$ be integral values, not all zero, of the variables $x, y, \cdots$ for which the Null form N vanishes. In view of the homogeneity of N, we may assume that $\xi, \eta, \cdots$ have no common factor >1. It is known that there exists a square matrix M of determinant unity whose elements are all integers, those of the first column being $\xi, \eta, \cdots$. The linear substitution with the matrix M evidently replaces N by a form F in which the coefficient of x^2 is zero.

When there are only two variables, $F=axy+by^2$. The case in which a and b have a common factor $c>1$ is excluded since F then represents only multiples of c.

First, let a have an odd prime factor p. Then F represents no integer of the form $b\nu+pk$, where ν is a quadratic non-residue of p.

Second, let a be even and hence b odd. Then F is never the double of an odd integer.

Hence $a=1$. Replacing x by $x-by$, we get xy.

THEOREM 1. *Every universal binary Null quadratic form is the product of two linear functions of determinant unity and hence is equivalent to xy.*

---

* Presented to the Society, December 31, 1928; received by the editors in September, 1928.

Henceforth let there be n variables, where $n \geqq 3$. The part of F which involves x may be written as Axy', where y' is a linear function of $y, z, \cdots$, the greatest common divisor of whose coefficients is unity. As noted above there exists a square matrix of determinant unity whose elements are all integers, those of the first row being the coefficients of y'. Let $z', w', \cdots$ be the linear functions of $y, z, \cdots$ whose coefficients are the elements of the second, third, $\cdots$ rows of that matrix. The resulting linear substitution replaces F by an equivalent form f. After dropping the accents on y', $z', \cdots$, we have

$$f = Axy + \phi(y, z, w, \cdots). \tag{1}$$

If $n=3$, this is of the form (2) with $\psi = z^2$. If $n>3$, the sum of the terms of ϕ which are linear in y is cyz', where z' is a linear function of $z, w, \cdots$, the g. c. d. of whose coefficients is 1. There exist further linear functions $w', \cdots$ such that the determinant of the coefficients in $z', w', \cdots$ is 1. Hence f is equivalent to

$$h = Axy + By^2 + cyz + \Delta\psi(z, w, \cdots), \tag{2}$$

in which the g. c. d. of the coefficients of ψ is 1.

Let $A = 2^e\alpha$, where α is odd. Let g be the g. c. d. of $\alpha = ga$ and $\Delta = gd$. Then c is prime to g. For, if a prime p divides c and g, p is odd and $h \equiv By^2$ (mod p), whence h has at most $\frac{1}{2}(p+1)$ values modulo p and is not universal.

If we replace z by $z+ty$ in h and note that $\Delta \equiv 0$ (mod g), we get a form (1) in which the coefficient of y^2 is $\equiv B+ct$ (mod g). This is divisible by g when t is suitably chosen. Hence we may take $B = gb$ in (2).

THEOREM 2. *Every universal Null quadratic form in three or more variables is equivalent to a form*

$$F = 2^e gaxy + gby^2 + cyz + gd\psi(z, w, \cdots), \tag{3}$$

where g and a are odd, a is prime to d, c is prime to g, and the g. c. d. of the coefficients of ψ is unity.

PART I. CASE OF THREE VARIABLES

3. Here $F = Px + f$, $P = 2^e gay$, $f = gby^2 + cyz + gdz^2$. Let G be any given integer. Our method is briefly as follows. Under specified conditions on the coefficients of F, we shall show how to select an odd prime π, not dividing gad, such that $f \equiv G$ (mod P) has a solution $z = Z$ when $y = \pi$. Thus $f = G + PQ$, where Q is an integer. Hence $F = G$ when $x = -Q$, $y = \pi$, $z = Z$.

If $f \equiv G$ is solvable for the separate moduli 2^e, ga, y, it is solvable modulo P. For modulus y, the condition is

$$(gdz)^2 \equiv gdG \qquad (\text{mod } y). \tag{4}$$

We shall satisfy this condition in §6 by choice of $y=\pi$.

Consider modulus ga. A prime factor of it either divides both g and a or just one of them. Hence we may write

$$(5)\qquad \begin{cases} g=qr,\ a=st,\ q \text{ and } s \text{ have the same distinct prime factors,} \\ r \text{ and } t \text{ are prime to each other and to both } q \text{ and } s. \end{cases}$$

If $f\equiv G$ is solvable for the separate moduli qs, r, t, which are relatively prime in pairs, it is solvable modulo ga, their product. By (5) and Theorem 2,

$$(6)\qquad d \text{ is prime to } st, \quad c \text{ is prime to } q,\ r, \text{ and } s.$$

Since $f\equiv cyz \pmod g$, $f\equiv G \pmod g$ is solvable when $y=\pi$ by (6) and the fact that π does not divide g. This disposes of modulus r.

4. Consider $f\equiv G \pmod{qs}$. Since q is a factor of g, we saw that $f\equiv cyz\equiv G \pmod q$ has a solution z_1 when $y=\pi$, whence $cyz_1=G+Mq$. Its general solution is $z=z_1+\zeta q$, where ζ is arbitrary. Insert the value of z into $f\equiv G$ (mod qs), cancel G, and delete the common factor q. We get

$$rby^2+cy\zeta+M+rd(z_1+\zeta q)^2\equiv 0 \pmod s.$$

If s is a product of powers p^n of distinct primes, it suffices to prove that the like congruence is solvable for each modulus p^n. Let p^m be the highest power of p which divides q, whence $m\geqq 1$. The congruence is of the form

$$(7)\qquad S\zeta+p^m\phi(\zeta)\equiv k \pmod{p^n},$$

where $S=cy$ is not divisible by p by (6), and k depends upon y, but not on ζ. If $m\geqq n$, this is $S\zeta\equiv k$ and is solvable. Next, let $n>m$. As before, (7) has a solution ζ' modulo p^m, whence

$$\zeta=\zeta'+Zp^m,\quad S\zeta'=k+Rp^m.$$

Cancellation of k from (7) and division by p^m gives

$$R+SZ+\phi(\zeta'+Zp^m)\equiv 0,\ \text{ or } SZ+p^mP(Z)\equiv k' \pmod{p^{n-m}}$$

where $k'=\phi(\zeta')-R$ is independent of Z. If $n-m\leqq m$, this is $SZ\equiv k'$ and is solvable. If $n-m>m$, we repeat the process and reduce the problem to a congruence modulo p^{n-2m}.

To proceed by induction on μ, suppose the problem has been reduced to

$$(8)\qquad Su+p^m\phi(u)\equiv k \pmod{p^{n-\mu m}},\quad n>\mu m.$$

If $n-\mu m\leqq m$, then p^m is a multiple of the modulus and (8) is solvable. Next, let $n-\mu m>m$. Evidently (8) has a solution u' modulo p^m, whence

$$u=u'+vp^m,\quad Su'=k+p^mQ.$$

Cancellation of k from (8) and division by p^m gives

$$Sv + Q + \phi(u' + vp^m) \equiv 0, \quad \text{or} \quad Sv + p^m P(v) \equiv k' \quad (\text{mod } p^{n-\mu m-m}),$$

where k' is free of v. Since this is of type (8) with μ replaced by $\mu+1$, the induction is complete. Ultimately we reach a congruence (8) with $n-\mu m \leqq m$, which is therefore solvable. This proves

LEMMA 1. *For every integer G, and for $y=\pi$, $F\equiv G$ is always solvable modulis qs and r.*

5. Let t be a product of powers p^n of distinct primes. Multiplication of $f\equiv G$ (mod p^n) by $4gd$, which is prime to t by (5) and (6), gives the equivalent congruence

$$Z^2 - Ry^2 \equiv k \quad (\text{mod } p^n), \tag{9}$$

where

$$Z = 2gdz + cy, \qquad R = c^2 - 4g^2db, \qquad k = 4gdG.$$

If $R\equiv 0$ (mod p), $4gdF\equiv Z^2$, whence F has only $\frac{1}{2}(p+1)$ values modulo p and is not universal.

Let R be a quadratic non-residue of p, and take $G\equiv 0$, whence $k\equiv 0$ (mod p). Then $y\equiv 0$, $Z\equiv 0$, $z\equiv 0$ (mod p). Thus F is divisible by p^2 and is not universal.

Hence $v^2\equiv R$ (mod p^n) is solvable when $n=1$. To proceed by induction from $n=m$ to $n=m+1$, let $w^2=R+Sp^m$. Then w is not divisible by p, and $2wT+S\equiv 0$ (mod p) has a solution T. Hence $(w+Tp^m)^2\equiv R$ (mod p^{m+1}).

Determine δ by $v\delta\equiv 1$ (mod p^n). Multiply (9) by δ^2 and write $u=\delta Z$, $K=\delta^2 k$. We get

$$u^2 - y^2 \equiv K \quad (\text{mod } p^n). \tag{10}$$

Modulo p, this has a solution with y prime to p unless

$$p = 3, \quad K \equiv 1 \quad (\text{mod } 3). \tag{11}$$

To prove this fact, let α be any integer not divisible by p and determine β by $\alpha\beta\equiv 1$ (mod p). Then $2y\equiv\alpha-K\beta$ (mod p) determines an integer y not divisible by p if $\alpha^2\not\equiv K$ (mod p). Since at most three residues α are excluded, we can find a suitable α if $p>3$. In case $p=3$ and $K\equiv 0$ or 2 (mod 3), only $\alpha\equiv 0$ is excluded. Take $u=y-\alpha$. Then $y+u\equiv -K\beta$, and (10) holds.

To show that (10) has a solution with y prime to p, we proceed by induction from $n=m$ to $n=m+1$. Hence let

$$u^2 - Y^2 = K + Sp^m, \quad Y \text{ prime to } p.$$

Then $2Y\eta \equiv S \pmod{p}$ has a solution η, and (10) holds modulo p^{m+1} for $y = Y + \eta p^m$. Except in case (11), there is therefore an integer Y prime to p such that, when $y \equiv Y \pmod{p^n}$, (10) has a solution u, and hence $f \equiv G \pmod{p^n}$ has a solution z.

In case $G \equiv 0$, whence $K \equiv 0 \pmod{p}$, we shall need the fact that (10) has a solution in which y has any assigned value v not divisible by p. If $n = 1$, we may take $u = v$. To proceed by induction, let

$$U^2 - v^2 = K + p^m Q.$$

Then (10) holds modulo p^{m+1} when $u = U + Sp^m$, $y = v$, if $2SU + Q \equiv 0 \pmod{p}$, which is satisfied by choice of S.

6. We are now in a position to prove

LEMMA 2. *If R is a quadratic residue of t, to each G corresponds an odd prime π not dividing agd such that, when $y = \pi$, $f \equiv G \pmod{ty}$ is solvable.*

Write $t = \tau T$, $\tau = p_1^{n_1} \cdots p_k^{n_k}$, where no one of the distinct primes p_i divides G, while each prime factor of T divides G. Except in case (11), we saw that there is an integer Y_i not divisible by p_i such that, when $y \equiv Y_i \pmod{p_i^{n_i}}$, there exists a solution z_i of $f \equiv G \pmod{p_i^{n_i}}$. But there are integers Y and z satisfying

$$Y \equiv Y_1, \quad z \equiv z_1 \pmod{p_1^{n_1}}, \cdots, \quad Y \equiv Y_k, \quad z \equiv z_k \pmod{p_k^{n_k}}.$$

Hence Y is prime to τ, and there is a solution z of $f \equiv G \pmod{\tau}$ when $y = Y$.

Write D for gdG. Since gd is prime to t by (5) and (6), τ is prime to D. The divisor τ of a is odd. Let $\pi_1, \cdots, \pi_h$ be the distinct odd primes which occur in D with odd exponents. The system of congruences

$$\pi \equiv Y \pmod{\tau}, \qquad \pi \equiv 1 \pmod{8}, \qquad \pi \equiv 1 \pmod{\pi_i} \qquad (i = 1, \cdots, h)$$

has a solution $\pi \equiv V \pmod{M}$, where V is prime to $M = 8\tau\pi_1 \cdots \pi_h$. There are infinitely many primes of the form $V + Mw$. Let π be one of them which does not divide $2\,agd$. We shall prove that Lemma 2 holds for this π. For Jacobi's symbols,

$$(\pi_i/\pi) = (\pi/\pi_i) = 1, \quad (2/\pi) = 1, \quad (D/\pi) = 1.$$

Hence by (4), $f \equiv G \pmod{y}$ has a solution z when $y = \pi$. We saw that $f \equiv G \pmod{\tau}$ has a solution z when $y \equiv Y \equiv \pi \pmod{\tau}$. It remains only to prove that $f \equiv G \pmod{T}$ has a solution z when $y = \pi$. Let p^n be a highest power of a prime dividing T. Thus p divides G. Since π is not a divisor of a and hence not of T, $\pi \neq p$. At the end of §5, we saw that, when y has any assigned value not divisible by p, and hence when $y = \pi$, $f \equiv G \pmod{p^n}$ has a solution z. The same is true modulo T.

Combining Lemmas 1 and 2, we have, except for case (11),

THEOREM 3. *Let t denote the largest divisor of a which is prime to g. If F is universal, then*

(12) $$R=c^2-4g^2db \text{ is a quadratic residue of } t.$$

In case (12), *to every G corresponds an odd integer π such that, when $y=\pi$, $f\equiv G$* (mod agy) *has a solution z.*

7. It remains to prove Theorem 3 for the special case (11). Then $\delta^2\equiv 1$, $R\equiv 1$, $k\equiv 1$ (mod 3), and (9) requires $y\equiv 0$. Take Y prime to 3, and $3Y\equiv Y_i$ (mod $p_i^{n_i}$) for each prime factor $p_i\neq 3$ of τ. Now $k+9RY^2$ is a quadratic residue of 3 and hence of 3^{n+1}. For $y\equiv 3Y$, $f\equiv G$ therefore has a solution z modulo 3^{n+1} and hence modulo 3τ. Define π as in §6. For $y\equiv 3\pi$, $f\equiv G$ has a solution z modulo 3τ and modulo π, and hence modulo $3\tau\pi=y\tau$.

By the first remark in §3 and Theorem 3, we have

THEOREM 4. *If $e=0$, F is universal in case* (12).

8. Consider the classic case of forms F in which the coefficients of products of different variables are all even, whence $e\geqq 1$ and c is even. We shall prove

THEOREM 5. *When $e\geqq 1$ and c is even, F is universal if and only if* (12) *holds and*

(13) $$e=1;\ \textit{either } d \textit{ is odd, or } d\equiv 2 \pmod 4 \textit{ and } b \textit{ is odd.}$$

First, let F be universal and employ the notations $A=ga$, $B=gb$, $c=2C$, $D=gd$. Then

$$F=2^eAxy+f,\quad f=By^2+2Cyz+Dz^2,\quad A \text{ odd}.$$

Since F shall represent odd integers, B and D are not both even. If B is even and D odd, we replace z by $z+y$ in F and obtain a like form with $B'=B+2C+D$, which is odd. Hence we may take B odd.

First, let $e\geqq 3$. Since F represents a complete set of residues modulo 8, the same is true of

$$BF\equiv y^2+2BCyz+BDz^2\equiv Y^2+hz^2 \pmod 8,$$

where $Y=y+BCz$. If h is even, Y^2+hz^2 has at most six values modulo 8. Hence h is odd and Y^2+hz^2 has at most seven residues $0, 1, 4; h, h+1, h+4; 5$.

Second, let $e=2$. If $A\equiv 3$ (mod 4), we change the signs of y and z in F and obtain an equivalent form having $A'=-A$. Hence let $A\equiv 1$ (mod 4).

Then $F\equiv 4xy+f$ (mod 16). Replacing x by $x+ky+sz$, we obtain a like form having $B'=B+4k$, $C'=C+2s$. Hence we may take $B=\pm 1$, $C=0$ or 1.

The case $B=C=1$. The residues of F modulo 4 are 0, 1, D, $D+3$. Hence $D=4k+3$. Consider odd values of F. Then $y+z$ is odd and

$$f=(y+z)^2+(D-1)z^2,\quad F\equiv 4x(z+1)+1+(4k+2)z^2 \pmod 8.$$

For z even, $F\equiv 4x+1\equiv 1$ or 5; for z odd, $F\equiv 4k+3$ (mod 8). Hence F represents only three of the four odd classes modulo 8.

The case $B=1$, $C=0$. Then $F\equiv 0$, 1, D, $D+1$ (mod 4), whence $D=4k+2$. Then

$$F\equiv 4xy+y^2+(4k+2)z^2 \pmod{16}.$$

When F is even, $y=2Y$ and $F=2\phi$, $\phi=4xY+2Y^2+mz^2$, $m=2k+1$. Since F represents all even residues modulo 16, ϕ represents all residues modulo 8. But if ϕ is odd, z is odd and $\phi\equiv m$, $m+2$, or $m+6$ (mod 8). Thus $\phi\not\equiv m+4$ (mod 8).

The case $B=-1$. In the universal form $-F$ we change the signs of y and D and obtain F with $B=1$, which was treated in the preceding cases.

This proves that $e=1$. We return to the notations in §3. By hypothesis, c is even and g is odd. Let d be even. Since F is not always even, b is odd. If $d\equiv 0$ (mod 4), $F\equiv 2$ (mod 4) is impossible. For that requires that y be even and then $F\equiv 0$ (mod 4). Hence (13) are necessary conditions that F be universal.

We readily show that (12) and (13) are sufficient conditions. If d is odd, and y is any chosen odd integer, $F\equiv by^2+dz^2\equiv G$ (mod 2) has a solution z when G is arbitrary. Thus F is universal by Theorem 3. Next, let $d=2D$, where D and b are odd. If y is odd, then F is odd and $F\equiv G$ (mod 2) has a solution z when G is odd. Next, let G be even. Take $y=2Y$, where Y is odd. Then $F=4gaxY+4gbY^2+2cYz+gdz^2\equiv 2z^2$ (mod 4), whence $F\equiv G$ (mod 4) has a solution z. This F is derived from (3) by replacing e by 2, b by $4b$, c by $2c$, y by Y, and has the same g, a, d. The conditions in Theorem 2 still hold, while R is multiplied by 4. We may therefore apply Theorem 3 with $Y=\pi$, $e=2$.

9. In view of Theorems 4 and 5, it remains only to treat the case $e\geqq 1$, c odd.

(I) Let d be even. Assign an odd value to y and write k for the odd integer cy. Then $F\equiv gby^2+\phi$ (mod 2^e), where $\phi=kz+gdz^2$. Then ϕ ranges with z over a complete set of residues modulo 2^e. For, $\phi\equiv kZ+gdZ^2$ implies

$$(z-Z)[k+gd(z+Z)]\equiv 0 \pmod{2^e}.$$

Since the second factor is odd, $z \equiv Z \pmod{2^e}$. Hence if G is arbitrary, $F \equiv G \pmod{2^e}$ has a solution z. Hence F is universal if (12) holds.

(II) Let d be odd. If b is odd, $F \equiv y + yz + z \pmod 2$ and F is even only when y and z are both even, whence $F \not\equiv 2 \pmod 4$. Hence for a universal F, b is even.

Determine ω so that $gd\omega \equiv 1$ modulo 2^{e+3}; then $F \equiv G$ is solvable if and only if $\omega F \equiv \omega G$ is solvable. It therefore suffices to study

$$H = 2^e Axy + 2By^2 + Cyz + z^2 \qquad (e \geqq 1,\ C \text{ odd}). \tag{14}$$

(i) Assign a fixed odd value to y. The values of H modulo 2^e are the sums of $2By^2$ and the values of $\phi = z^2 + tz$, where $t = Cy$ is odd. Evidently ϕ is always even. Consider

$$\phi \equiv Z^2 + tZ, \quad (z - Z)(z + Z + t) \equiv 0 \pmod{2^e}.$$

If the first factor is even, the second is odd and $z \equiv Z \pmod{2^e}$. Hence if z ranges over the 2^{e-1} even integers

$$0, 2, 4, \cdots, 2^e - 2, \tag{15}$$

ϕ takes 2^{e-1} even values incongruent modulo 2^e, which are therefore congruent to the numbers (15) rearranged. Since this result is not changed if we add to them the constant $2By^2$, we conclude that $H \equiv k \pmod{2^e}$ has a solution when k is any even integer. Hence Theorem 3 applies when G is any even integer.

(ii) Let $y = 2y_1$, where y_1 is odd, but undetermined. Then

$$H \equiv Z^2 + ry_1^2 \pmod{2^{e+1}}, \quad Z = z + Cy_1, \quad r = 8B - C^2.$$

In view of (i), we need consider only odd values of H. Then $Z = 2\zeta$ and $H \equiv 3 \pmod 4$. If k is any integer $\equiv 3 \pmod 4$,

$$4\zeta^2 + ry_1^2 \equiv k \pmod{2^{e+1}}$$

has a solution with y_1 odd. This is evidently true modulo 8. To proceed by induction, let

$$4a^2 + rb^2 = k + 2^m Q, \quad b \text{ odd}, \quad m \geqq 3.$$

Then

$$4a^2 + r(b + 2^{m-1}w)^2 \equiv k + 2^m(Q + rbw) \equiv k \pmod{2^{m+1}},$$

by choice of w modulo 2. The induction is complete. To each k corresponds an odd G for which $F \equiv G \pmod{2^{e+1}}$ has a solution with y_1 odd.

Since y_1 was not preassigned, but was suitably determined, we must modify our determination of π in §6. Since $D = gdG$ is now odd, we omit

$\pi \equiv 1 \pmod 8$ from the system of congruences for π and replace it by $\pi \equiv y_1 \pmod{2^{e+1}}$.

(iii) Let $y = 4y_2$, where y_2 is a fixed odd integer. Then

$$H \equiv Z^2 + 4ry_2^2 \pmod{2^{e+2}}, \qquad Z = z + 2Cy_2, \qquad r = 8B - C^2.$$

In view of (i), we need consider only odd values of H, whence Z is odd and $H \equiv 5 \pmod 8$. If k is any integer $\equiv 5 \pmod 8$, then $H \equiv k \pmod{2^{e+2}}$ has an odd solution Z. This is evident for modulus 8. To proceed by induction, let

$$a^2 + 4ry_2^2 = k + 2^m Q, \quad a \text{ odd}, \quad m \geqq 3.$$

Then

$$(a + 2^{m-1}x)^2 + 4ry_2^2 \equiv k + 2^m(Q + ax) \equiv k \pmod{2^{m+1}},$$

by choice of x modulo 2. Our F is derived from (3) by replacing e by $e+2$, y by y_2, b by $16b$, and c by $4c$, and has the same g, a, d. The conditions in Theorem 2 hold also here, while R is multiplied by 16.

(iv) Let $y = 8y_3$, where y_3 is a fixed odd integer. Then

$$H \equiv Z^2 + 16ry_3^2 \pmod{2^{e+3}}, \quad Z = z + 4Cy_3.$$

Take Z odd. Then $H \equiv 1 \pmod 8$. If k is any integer $\equiv 1 \pmod 8$, then $H \equiv k \pmod{2^{e+3}}$ has an odd solution Z. This is proved by induction as in (iii).

Since every integer k falls under one of our four cases, we conclude from Theorem 3 that F is universal if (12) holds. This completes the proof of

THEOREM 6. *When $e \geqq 1$ and c is odd, F is universal if and only if* (12) *holds and bd is even.*

10. Another proof of Theorem 6 reveals a property to be utilized in the more complicated case of four variables. When (12) holds, F is universal if and only if $F \equiv G \pmod{2^n}$ is solvable when $n \leqq 2e+2$, irrespective of the evenness or oddness of y.

When G is even, we retain the proof in (i) of §9. Next, let G be odd. Now H is the product of F by ω modulo 2^{2e+2} instead of 2^{e+3}. For n arbitrary and k odd, $H \equiv k \pmod{2^n}$ has a solution with $x = 0$, y even. For proof, put $y = 2Y$. Then

$$H = Z^2 + rY^2, \qquad Z = z + CY, \qquad r = 8B - C^2.$$

Modulo 8, $H \equiv Z^2 - Y^2$ has the values 0, 1, 3, 4, 5, 7, whence $H \equiv \text{odd} \pmod 8$ is solvable. To proceed by induction, let

$$\zeta^2 + r\eta^2 = k + 2^m Q, \quad m \geqq 3.$$

Since ζ and η are not both even,

$$(\zeta + 2^{m-1}u)^2 + r(\eta + 2^{m-1}v)^2 \equiv k + 2^m(Q + \zeta u + r\eta v) \equiv k \pmod{2^{m+1}},$$

by choice of u, v modulo 2.

Now take $n=2e+2$. If in a solution of $H\equiv k \pmod{2^n}$, Y is divisible by $h=2^{e+1}$, then $Z^2\equiv k$, whence $H\equiv k \pmod{2^n}$ has a solution in which Y is an arbitrary multiple of h, and hence a solution with $Y=h$. Next, let there be no solution having Y divisible by h. Then in every solution, Y is the product of 2^s by an odd integer where $s\leqq e$. In both cases there is a solution with $Y=2^\sigma\eta$, where η is odd and $\sigma\leqq e+1$. Then $y=2^l\eta$, $l\leqq e+2$. Since $e+l\leqq n$, we see that $H\equiv k \pmod{2^{e+l}}$ has a solution with $x=0$, $y=2^l\eta$. Insertion of this y into (3) gives a form F_1 which is derived from F by replacing e by $e+l$, y by η, b by $2^{2l}b$, and c by 2^lc. Since F_1 has the same g, a, d as F, F_1 satisfies the conditions in Theorem 2. The R of F_1 is the product of R in (12) by 2^{2l}. For G odd, we proved that $F=F_1\equiv G \pmod{2^{e+l}}$ has a solution with η odd. Thus F_1 and therefore F is universal if (12) holds.

Part II. The case of four variables

11. In (3), let

$$(16) \qquad \psi = hz^2 + jzw + lw^2, \quad 1 = \text{g.c.d. of } h,j,l.$$

We may assume that *h is relatively prime to any given odd integer m.* For, the replacement of w by $w+tz$ alters only h and j. Then $h'=h+jt+lt^2$. We can choose t so that h' is divisible by no one of the distinct prime factors $p_1, \cdots, p_k$ of m. In fact, since h, j, l are not all divisible by p_i, there are at most two incongruent roots t of $h'\equiv 0 \pmod{p_i}$. Since $p_i>2$, there is a value v_i of t such that h' is not divisible by p_i. There exists an integer v such that

$$v \equiv v_1 \pmod{p_1}, \cdots, v \equiv v_k \pmod{p_k}.$$

Hence when $t=v$, h' is divisible by no one of $p_1, \cdots, p_k$.

12. Let F have the properties in Theorem 2. In (16) we may take h prime to ga by §11.

Lemma 3. *If each of the congruences*

$$F \equiv G \pmod{2^e}, \qquad F \equiv G \pmod{ga}$$

has a solution x, y, z, w such that y has a fixed value 1 *or an odd prime dividing no one of g, a, d, h, $N=j^2-4hl$, then $F=G$ is solvable.*

We first prove that $F\equiv G \pmod{y}$ is solvable. Proof is needed only when

y is the specified odd prime. Determine m by $gdm \equiv 1 \pmod{y}$. Multiplication of $F \equiv G$ by $4mh$ yields the equivalent congruence

$$4h\psi \equiv 4mhG \quad \text{or} \quad Z^2 - Nw^2 \equiv 4mhG \pmod{y},$$

where $Z = 2hz + jw$. There is a solution Z, w since N is not divisible by the odd prime y. Since h is not divisible by y, Z determines z.

Hence $F \equiv G \pmod{2^e gay}$ is solvable. As at the beginning of §3, the equation $F = G$ is solvable.

The proof of Lemma 1 applies also here if we take $w = 0$ and multiply the coefficient of z^2 in §4 by h.

Since t is prime to g, d, and h, while t divides a, multiplication of $F \equiv G \pmod{t}$ by $4gdh$ yields the equivalent congruence

$$4g^2dhby^2 + 4gdhcyz + g^2d^2[(2hz + jw)^2 - Nw^2] \equiv 4gdhG \pmod{t}. \tag{17}$$

Let t be a product of powers p^n of distinct primes.

13. **Case N not divisible by p.** The product of (17) by N is

$$Nu^2 - v^2 + Jy^2 \equiv k \pmod{p^n}, \tag{18}$$

where

$$u = gd(2hz + jw) + cy, \qquad v = Ngdw + cjy, \qquad k = 4NgdhG,$$

$$R = c^2 - 4g^2dhb, \qquad J = c^2j^2 - NR. \tag{19}$$

(I) $J \not\equiv 0 \pmod{p}$. Since $Nu^2 - v^2 \equiv k - J \pmod{p}$ is solvable, (18) has a solution modulo p with $y \equiv 1 \pmod{p}$. Write $Nu^2 - v^2 + J = k + pQ$. Determine c_1 so that $Q + 2Jc_1 \equiv 0 \pmod{p}$. Then (18) holds modulo p^2 with $y \equiv 1 + c_1p \pmod{p^2}$. Hence

$$Nu^2 - v^2 + J(1 + c_1p)^2 = k + p^2T.$$

Determine c_2 so that $T + 2Jc_2 \equiv 0 \pmod{p}$. Then (18) holds modulo p^3 with $y \equiv 1 + c_1p + c_2p^2 \pmod{p^3}$. To proceed by induction from $n = m$ to $n = m+1$, let (18) hold modulo p^m when $y \equiv Y \pmod{p^m}$, where $Y = 1 + c_1p + \cdots + c_{m-1}p^{m-1}$. Write

$$Nu^2 - v^2 + JY^2 = k + p^mS.$$

Determine c_m so that $S + 2Jc_m \equiv 0 \pmod{p}$. Then (18) holds modulo p^{m+1} with $y \equiv Y + c_mp^m \pmod{p^{m+1}}$. The induction is therefore complete and shows that (18) has solutions with $y \equiv \eta \pmod{p^n}$, $\eta = 1 + c_1p + \cdots + c_{n-1}p^{n-1}$, with each c_i determined modulo p. There exist infinitely many primes y of the form $\eta + xp^n$.

(II) N a quadratic residue of p. Thus $N \equiv T^2 \pmod{p}$. Write U for Tu, K for $k-J$. Take $y=1$. Then (18) holds modulo p if $U^2-v^2 \equiv K \pmod{p}$. This has solutions. In case $K \equiv 0$, take $U \equiv v \equiv 1$. Hence $Nu^2-v^2 \equiv K$ always has solutions u, v, not both divisible by p. To proceed by induction from $n=m$ to $n=m+1$, let

$$Nu^2 - v^2 \equiv K \qquad \pmod{p^m}$$

have solutions u, v, not both divisible by p. Then

$$Nu^2 - v^2 = K + p^m Q,$$

$$N(u + p^m \xi)^2 - (v + p^m \eta)^2 \equiv K + p^m L \qquad \pmod{p^{m+1}},$$

where $L = Q + 2Nu\xi - 2v\eta \equiv 0 \pmod{p}$ has solutions ξ, η. Since the induction is complete, (18) has solutions with $y=1$.

(III) If N is a quadratic non-residue of p and $J \equiv 0 \pmod{p}$, F is not universal. Consider (18) for $k=pK$ and write $J=Tp$. Then $Nu^2-v^2 \equiv 0$, $u \equiv v \equiv 0 \pmod{p}$. By the origin of (18),

$$4gdhN(F - G) = Nu^2 - v^2 + Jy^2 - k.$$

The second member is $\equiv pM \pmod{p^2}$, where $M = Ty^2 - K$. We can choose K so that M is not divisible by p for any y. To each K corresponds a single G by the value of k below (18). Hence F is never congruent modulo p^2 to certain multiples G of p.

14. **Case** $N \equiv 0 \pmod{p}$. Write $N = p\epsilon$.

(I) Let $jc \not\equiv 0 \pmod{p}$. In (17) we may solve $2hz \equiv -jw \pmod{p^n}$ for z, since h is prime to ga and hence to p. Take $y=1$ and write

$$\mu = 2gdcj, \qquad \nu = g^2d^2\epsilon, \qquad k = 4g^2dhb - 4gdhG.$$

Then (17) is equivalent to

$$(20) \qquad \mu w + \nu p w^2 \equiv k \pmod{p^n}, \qquad \mu \not\equiv 0 \pmod{p}.$$

This has a solution w' modulo p, and $w = w' + \omega p$, $\mu w' = k + \gamma p$. Then (20) is equivalent to

$$\mu\omega + \gamma + \nu(w' + \omega p)^2 \equiv 0 \quad \text{or} \quad \mu\omega + pf(\omega) \equiv K \qquad \pmod{p^{n-1}}.$$

Suppose we have similarly reduced the solution of (20) to

$$(21) \qquad \mu u + pf(u) \equiv K \qquad \pmod{p^{n-m}}.$$

This has a solution u' modulo p, and

$$u = u' + vp, \quad \mu u' = K + \delta p.$$

Then (21) is equivalent to

$$\mu v + \delta + f(u' + vp) \equiv 0 \quad \text{or} \quad \mu v + pP(v) \equiv K' \qquad (\text{mod } p^{n-m-1}).$$

This is of type (21) with m replaced by $m+1$. Hence the induction from m to $m+1$ is complete, and (20) is solvable.

(II) Let $j \equiv 0$ (mod p). Then (17) gives

$$(22) \qquad Z^2 - Ry^2 \equiv k \pmod{p}, \qquad Z = 2gdhz + cy, \qquad k = 4gdhG.$$

Since this is of type (9), R is not divisible by p. Next, if R is a quadratic non-residue of p, and if $G \equiv 0$ (mod p), then $y \equiv 0$, $Z \equiv 0$, $z \equiv 0$ (mod p), $F \equiv gd\psi$ (mod p^2). Since $N = p\epsilon$ and $\zeta = 2hz + jw$ is divisible by p,

$$4hF = gd(\zeta^2 - Nw^2) \equiv \tau p w^2 \pmod{p^2}, \quad \tau = -gd\epsilon.$$

Hence F represents only those multiples mp of p for which $4hm \equiv \tau w^2$ (mod p). Hence m has at most $\frac{1}{2}(p+1)$ values modulo p. Thus F is not universal.

Hence R must be a quadratic residue of p. We take $w = 0$. The discussion in §§5, 7 applies here. There are infinitely many primes y having specified residues with respect to odd moduli p^n.

(III) Let $c \equiv 0, j \not\equiv 0$ (mod p). In (17) write Z for $gd(2hz + jw)$. We get the congruence (22). As in (II), R must be a quadratic residue of p. By §5 with $n = 1$, (22) then has a solution with y prime to p except in case (11).

There is a solution with $w = 0$, y prime to p, of

$$(23) \qquad F \equiv G\colon\ gby^2 + cyz + gdhz^2 \equiv G \qquad (\text{mod } p^n).$$

To proceed by induction from $n = m$ to $n = m+1$, let

$$gbY^2 + cYZ + gdhZ^2 = G + kp^m, \quad Y \text{ prime to } p.$$

Then (23) holds modulo p^{m+1} for $y = Y + \eta p^m$, $z = Z$, if

$$k + 2gbY\eta + c\eta Z \equiv 0 \pmod{p}.$$

This has a solution η since $c \equiv 0$, $R \not\equiv 0$, whence $gb \not\equiv 0$ by (19).

15. This completes the proof of

THEOREM 7. *For the form F defined by* (3) *and* (16), *let g and a be odd, a prime to d, c prime to g, and h prime to ga. Employ the abbreviations*

$$(24) \qquad N = j^2 - 4hl, \quad R = c^2 - 4g^2dhb, \quad J = c^2j^2 - NR.$$

We may assign to y a fixed value which is 1 *or an odd prime such that $F \equiv G$* (mod gay) *is solvable for every G except in the following cases*:

$$(25) \qquad \begin{array}{l} J \equiv 0 \ (\text{mod } p),\ (N/p) = -1;\ N \equiv cj \equiv 0 \ (\text{mod } p) \text{ and either} \\ R \equiv 0 \ (\text{mod } p) \text{ or } (R/p) = -1, \end{array}$$

where p is any prime dividing a but not g. In these cases F is never universal.

By the first remark in §3, we have

THEOREM 8. *If* $e=0$, *F is universal except in cases* (25).

16. Assume that the coefficients of products of different variables in F are all even, as in the classic theory. Hence $e\geqq 1$, c and dj are even. First, let $e=1$.

If d is odd, j is even and h and l are not both even by (16). Then $F=by+hz+lw\equiv G \pmod 2$ is solvable when y has an assigned odd value and G is arbitrary. Then F is universal except in cases (25).

Next, let $d=2D$. Then b must be odd. For G odd, $F\equiv y^2\equiv G \pmod 2$ holds if y is odd, whence §15 applies. Finally, let $G=2\gamma$. Then must $y=2Y$ and $F=2f$, where

$$f = 2gaxY + 2gbY^2 + cYz + gD(hz^2 + jzw + lw^2).$$

Since $f=\gamma$ shall be solvable for every γ, D must be odd. The function in parenthesis can be made congruent to either 0 or 1 modulo 2. Whatever be Y or γ, $f\equiv\gamma \pmod 2$ is therefore solvable. Since f is derived from F by replacing b and d by $2b$ and $\frac{1}{2}d$, the initial conditions in Theorem 7 are satisfied by f, and N, R, J are unaltered. Hence f and F are universal except in cases (25).

THEOREM 9. *Let* $e=1$. *If d is odd, let c and j be even; then F is universal except in cases* (25). *If* $d=2D$, *let c be even. Necessary and sufficient conditions that F be universal are that b and D be both odd except in cases* (25).

17. Let $e\geqq 2$, d odd. Then $c=2C$, $j=2s$. The products of h, s, l by the odd interger gd will be designated H, S, L. Write β for gb. Then

$$F = 2^e gaxy + \beta y^2 + 2Cyz + Hz^2 + 2Szw + Lw^2, \tag{26}$$

where H and L are not both even. Here let L be odd. Write

$$\lambda = LH - S^2, \qquad W = Lw + Sz.$$

Since our moduli are powers of 2, we may take W and z as new variables in place of w, z. We get

$$LF = L(2^e gaxy + \beta y^2 + 2Cyz) + \lambda z^2 + W^2. \tag{27}$$

Here let also λ be odd. Write

$$A = \lambda Lga, \qquad M = \lambda L\beta - L^2C^2, \qquad Z = \lambda z + LCy, \qquad F_1 = \lambda LF.$$

Then

$$F_1 = 2^e Axy + My^2 + Z^2 + \lambda W^2 \qquad (A,\lambda \text{ odd}). \tag{28}$$

If F is universal, $F_1 \equiv k \pmod{2^{2e}}$ is solvable when k is arbitrary. Conversely, let there be solutions. If y is divisible by 2^e, the terms in y drop out and there is a solution with $y = 2^e$. In every case we may write $y = 2^s\eta$, η odd, $s \leqq e$. The solution gives one of $F_1 \equiv k \pmod{2^{e+s}}$. Insertion of this y into (3) gives a form F' which is derived from F by replacing y by η, e by $e+s$, b by $2^{2s}b$, and c by $2^s c$. Since F' has the same g, a, d, h, j, l as F, F' satisfies the initial conditions in §15. While N is unaltered, R and J are multiplied by 2^{2s}. Hence conditions (25) are unaltered. This proves that, *except in cases* (25), *F is universal if and only if $F_1 \equiv k$* (mod 2^{2e}) *is solvable when k is arbitrary*. Solutions with y even are here not excluded.

(I) $\lambda \equiv 3 \pmod 4$. The case $M \equiv 0 \pmod 4$ is excluded since $Z^2 + 3W^2$ takes only the values 0, 1, 3 modulo 4.

Let $M \not\equiv 0 \pmod 4$. Then F_1 with $x = 0$ represents all residues of 8. For $Z^2 + \lambda W^2$ represents exclusively 0, 1, 3, 4, 5, 7 (mod 8). The missing 2 and 6 are obtained from $y = 1$. We may select u from the six so that $M + u \equiv 2 \pmod 8$ since $2 - M \equiv 2$ or 6 only if $M \equiv 0$ or $-4 \pmod 8$. Similarly, we may select v from the six so that $M + v \equiv 6 \pmod 8$.

To proceed by induction from $m \geqq 3$ to $m+1$, let

$$x = 0, \quad My^2 + Z^2 + \lambda W^2 = k + 2^m Q. \tag{29}$$

Then

$$M(y + 2^{m-1}\eta)^2 + (Z + 2^{m-1}\zeta)^2 + \lambda(W + 2^{m-1}\omega)^2 \equiv k \pmod{2^{m+1}}$$

if $Q + My\eta + Z\zeta + \lambda W\omega \equiv 0 \pmod 2$. The latter has solutions η, ζ, ω unless My, Z, W are all even. This disposes of odd k's.

Let $k \equiv 2 \pmod 4$. First, let M be odd and take $x = 0$. Then $My^2 + Z^2 + 3W^2 \equiv 2 \pmod 4$ shows that one of y, Z, W is even and two are odd. For y and Z odd, W even, $F_1 \equiv M+1$ or $M+5 \pmod 8$. For y and W odd, Z even, the values of F_1 are $M + \lambda$ and $M + \lambda + 4$, i.e., $M+3$ and $M+7 \pmod 8$. Hence F_1 takes all even residues and therefore the value k modulo 8, when y is odd. By the above induction, $F_1 \equiv k \pmod{2^n}$ is solvable.

Second, let $k \equiv M \equiv 2 \pmod 4$. Then $y \equiv 1$, $Z \equiv W \pmod 2$. Take $x = 0$. For y, Z, W all odd, $F_1 \equiv M + 1 + \lambda \pmod 8$. Now $M + 1 + \lambda$ and k are congruent modulo 4. If they are congruent modulo 8, the preceding induction yields solutions modulo 2^n. There remains the case $k \equiv M + 1 + \lambda + 4 \pmod 8$. Write $k = 2\kappa$, $M = 2\mu$, $\lambda = 4t + 3$. Then κ and μ are odd and $\kappa \equiv \mu + 2t \pmod 4$. Since Z and W must now be even, write $Z = 2\zeta$, $W = 2\omega$. Thus $F_1 \equiv k \pmod{2^n}$ becomes

$$\mu y^2 + 2\zeta^2 + 2\lambda\omega^2 \equiv \kappa \pmod{2^{n-1}}, \quad y \text{ odd}. \tag{30}$$

Since $\kappa=\mu+2t+4s$, this holds modulo 8 if and only if

$$\zeta^2+3\omega^2\equiv t+2s \pmod{4}.$$

This is solvable except when

$$(31)\qquad t+2s\equiv 2 \pmod{4},\qquad \kappa\equiv\mu+4 \pmod{8},$$
$$k\equiv M+8 \pmod{16},\qquad \lambda\equiv 3 \pmod{8}.$$

In the latter case, $F_1\equiv k$ (mod 16) has no solution with $x=0$ and hence no solution if $e\geqq 4$. This excludes the case $\lambda\equiv 3$ (mod 8), $e\geqq 4$.

When (31_1) fails, (30) is solvable modulo 8. We proceed by induction. If (30) holds modulo 2^m, $m\geqq 3$, it holds modulo 2^{m+1} for the same ζ, ω, but with y replaced by $y+2^{m-1}\eta$, where η is determined modulo 2 since μy is odd. Hence $F_1\equiv k$ (mod 2^n) is solvable when $k\equiv M\equiv 2$ (mod 4), $\lambda\equiv 7$ (mod 8).

Let (31) hold and $e=3$. We do not now take $x=0$. The conclusions preceding (30) continue to hold modulo 8. But (30) is now replaced by

$$(30')\qquad 4Axy+\mu y^2+2\zeta^2+2\lambda\omega^2\equiv\kappa \pmod{2^{n-1}},\quad y \text{ odd}.$$

This holds modulo 8 if $x\equiv Ay$, $\zeta\equiv w$ (mod 2). There is always a solution with $x=Ay$. Equate the left member to $\kappa+2^mQ$. Then if $m\geqq 3$,

$$(4A^2+\mu)(y+2^{m-1}\eta)^2+2\zeta^2+2\lambda\omega^2$$
$$\equiv\kappa+2^m[Q+(4A^2+\mu)y\eta]\equiv\kappa \pmod{2^{m+1}}$$

by choice of η modulo 2.

Let (31) hold and $e=2$. The first coefficient 4 in (30′) is now replaced by 2. There is a solution with $x=2Ay$.

If in a solution of $F_1\equiv k$ (mod 2^n) we multiply the variables by 2^s, we obtain a solution of $F_1\equiv 4^sk$.

(II) $\lambda\equiv 1$ (mod 4). The case $M\equiv 0$ (mod 4) is excluded since Z^2+W^2 takes only the values 0, 1, 2 modulo 4.

Modulo 8, $Z^2+\lambda W^2$ represents exclusively

$$(32)\qquad 0,1,4,5,\lambda+1.$$

First, let M be odd. Then $My^2\equiv 0$, M, or $4M\equiv 4$ (mod 8). Adding 4 to (31), we get the single new residue $\lambda+5$. It with $\lambda+1$ gives 2, 6 (mod 8). These with (32) give all residues except 3, 7. If one of the latter is congruent to the sum of M and a number (32), the latter must be even and hence 0, 4, or $\lambda+1$. These plus $M\equiv 1$ or 5 (mod 8) give a single new residue, viz., $\lambda+1+M$. If $e\geqq 3$, F_1 has a missing residue. Hence if $M\equiv 1$ (mod 4) and $e\geqq 3$, F_1 has a missing residue. Hence if $M\equiv 1$ (mod 4) and $e\geqq 3$, F_1 is not universal.

But if $e=2$, F_1 has the missing residue $\lambda+5+M$ modulo 8, when x, y, Z, W are all odd; and (28) represents all residues modulo 16.

If $M\equiv 3$ or 7 (mod 8), $M+0$ and $M+4$ give the missing 3, 7.

If $M\equiv 2$ (mod 4), $My^2\equiv 0$ or M (mod 8). The first four in (32) include all $\equiv 0$ or 1 (mod 4). Adding 0 and M, we get all residues modulo 4 and hence all modulo 8.

Hence if $M\equiv 2$ or 3 (mod 4), $F_1\equiv k$ is solvable modulo 8 with $x=0$ for every k. The first induction under (I) yields solutions modulo 2^n for every odd k.

Let $M\equiv 3$, $k\equiv 2$ (mod 4). For* $y=2Y$, Z and W odd, $F_1\equiv 4Y^2+1+\lambda$ (mod 8). According as $1+\lambda\equiv k$ or $k+4$ (mod 8), $F_1\equiv k$ holds for $Y=0$ or 1. To proceed by induction, note that (29) implies

$$My^2+(Z+2^{m-1}\zeta)^2+\lambda W^2\equiv k+2^m(Q+Z\zeta)\equiv k \pmod{2^{m+1}},$$

by choice of ζ modulo 2. Hence if $M\equiv 3$ (mod 4), $F_1\equiv k (\text{mod } 2^n)$ is solvable when k, n are arbitrary.

Let $M\equiv k\equiv 2$ (mod 4). Then $2y^2+Z^2+W^2\equiv 2$ (mod 4). There are only two possibilities. Either Z and W are odd, and $y=2Y$, whence $F_1\equiv k$ if $k\equiv 1+\lambda$ (mod 8), with induction to 2^n. Or $Z=2\zeta$, $W=2\omega$, and y is odd; then, for $x=0$, $F_1\equiv M+4\zeta^2+4\omega^2\equiv M$ or $M+4$ (mod 8), whence $F_1\equiv k$ (mod 8) is solvable. For $x=0$, we have (30), which for modulus 8 is equivalent to $\zeta^2+\omega^2\equiv d$ (mod 4), where $2d=\kappa-\mu$. This is solvable unless

$$(33)\qquad d\equiv 3 \pmod 4,\quad 6\equiv\kappa-\mu \pmod 8,\quad 12\equiv k-M \pmod{16}.$$

There was a solution with $y=2Y$ unless $k\equiv 1+\lambda+4$ (mod 8). If both fail,

$$(34)\qquad M\equiv 1+\lambda \pmod 8.$$

Except in this case, $F_1\equiv k$ (mod 2^n) is solvable. When $e\geqq 4$ and (33) and (34) hold, we saw that $F_1\equiv k$ (mod 16) has no solution. If (33) and (34) hold and $e=3$, we have (30′), which holds modulo 8 if and only if $\zeta+\omega$ is odd, $x\equiv Ay$ (mod 2). The former induction on (30′) applies also here. Likewise when $e=2$.

THEOREM 10. *Let* $e\geqq 2$, $c=2C$, $j=2s$, d, l, *and* $\lambda=g^2d^2(lh-s^2)$ *be odd. Write* $M=\lambda g^2dbl-g^2d^2l^2C^2$. *Then F is universal, if and only if we exclude cases* (25) *and the following*:

$$M\equiv 0 \pmod 4;\quad \lambda\equiv 3 \pmod 8,\quad e\geqq 4;\qquad \lambda\equiv M\equiv 1 \pmod 4,\ e\geqq 3;$$
$$\lambda\equiv 1 \pmod 4,\quad M\equiv 1+\lambda \pmod 8,\quad e\geqq 4.$$

* These are the only possible values modulo 4.

18. Next, let L be odd and λ even in the notations of §17. It suffices to treat the form (27) which we denote by

$$f = 2^eAxy + By^2 + 2Ryz + \lambda z^2 + W^2 \qquad (e \geqq 2). \tag{35}$$

If $e=2$, $2R+\lambda\equiv 2 \pmod 4$, f is universal except in cases (25). For, when y is odd, $f-B$ has the values 0, 1, $\tau=2R+\lambda$, $\tau+1 \pmod 4$, which form a complete set of residues modulo 4. If $e\geqq 3$, we separate the case $\tau\equiv 2$ into two subcases.

I. Let $e\geqq 2$, $\lambda\equiv 0 \pmod 4$, R odd. Assign a fixed odd value to y. Then $f-By^2\equiv 2tz+4hz^2+W^2 \pmod{2^e}$, where $t=Ry$ is odd and $4h=\lambda$. By (I) of §9, $tz+2hz^2$ ranges with z over a complete set of residues modulo 2^n. Take $n=e-1$. Hence $2tz+4hz^2$ takes all even values modulo 2^e. By use of $W=0$ and 1, we see that f takes all values modulo 2^e.

II. Next, let $e\geqq 3$, $\lambda=2r$, $R=2\rho$, where r is odd. Then

$$F_1 = rf = 2^erAxy + Ty^2 + 2Z^2 + rW^2, \quad Z = rz + \rho y, \quad T = rB - 2\rho^2. \tag{36}$$

Since y enters linearly only in the first term, the first italicized result in §17 holds here. Hence we ask if $F_1\equiv k \pmod{2^{2e}}$ is solvable when k is arbitrary and both odd and even y's are allowed.

The values modulo 8 of $2Z^2+rW^2$ (r odd) are

$$0,\, 2,\, 4,\, 6,\, r,\, r+2. \tag{37}$$

If $T\equiv 0 \pmod 8$, F_1 has only these six values and is excluded. If $T\equiv 2$ or 6 (mod 8), the values of F_1 are (37) and the same increased by 2 or 6, and hence are (37) and either $r+4$ or $r+6$; thus F_1 has only seven values and is excluded.

Let $T=4t$, where t is odd, and consider even values of F_1. Then $W=2w$, and F_1 is the double of

$$2^{e-1}rAxy + \phi, \qquad \phi = 2ty^2 + Z^2 + 2rw^2.$$

Since $2r\equiv \pm 2 \pmod 8$, $Z^2+2rw^2\equiv 0, 1, 2, 4, 6, 1\pm 2 \pmod 8$. The further values of ϕ are obtained from these by adding $2t$. If such sums yield both missing values 1 ∓ 2, 5, they are obtained by adding the odd 1, 1 ± 2 to $2t$. This is impossible since t is odd and $2t\equiv 2$ or 6 (mod 8). This excludes $e\geqq 4$. But F_1 yields universal forms if $e=3$. First, if y is odd, the values of F_1 modulo 8 are (37) increased by 4 and hence are all even residues and $r+2$, $r+6$. We lack r, $r+8$, $r+2$, $r+10 \pmod{16}$. We get these odd residues by taking $y=2Y$, Y odd, whence $F_1\equiv 2Z^2+rW^2$, whose odd values modulo 16 are derived by adding 0, 2, 8 to each r, $9r$. The sum $9r+2\equiv r+10 \pmod{16}$.

Finally, let T be odd. Then F_1 represents all residues modulo 8, as shown by the first four numbers (37) and the values 0 and 1 of y. If k is odd, $F_1 \equiv k \pmod{2^n}$ is solvable with $x=0$. For, if $F_1 = k+2^m Q$, then

$$T(y+2^{m-1}\eta)^2+2Z^2+r(W+2^{m-1}w)^2$$
$$\equiv k+2^m(Q+Ty\eta+rWw)\equiv k \pmod{2^{m+1}}$$

by choice of η, w modulo 2.

Henceforth, let $k=2\kappa$. Then $y+W$ is even. We may set $y=\eta+\zeta$, $W=\eta-\zeta$, $T+r=2M$. From $F_1\equiv 2\kappa \pmod{2^n}$, we cancel 2 and get

$$2^{e-1}rAxy+M\eta^2+M\zeta^2+2(M-r)\eta\zeta+Z^2\equiv\kappa \pmod{2^{n-1}}. \tag{38}$$

(a) If M is odd, multiply (38) by M and write

$$Y=M\eta+(M-r)\zeta,\qquad \lambda=2Mr-r^2\equiv 1 \pmod{4}.$$

We get

$$2^{e-1}MrAxy+MZ^2+Y^2+\lambda\zeta^2\equiv\kappa M \pmod{2^{n-1}}. \tag{39}$$

Aside from the first term, in which $y=\eta+\zeta$, this is of type (27) for the case (II) of §17 and M odd. It was proved there that, when $M\equiv 3 \pmod 4$, (39) is solvable with $x=0$ for every κ; but, when $M\equiv 1 \pmod 4$, $MZ^2+Y^2+\lambda\zeta^2$ represents all residues of 8 except $\lambda+5+M$. Hence if $e\geqq 4$, F_1 is not universal. The same is true if $e=3$ since

$$4MrAxy+MZ^2+Y^2+\lambda\zeta^2\equiv\lambda+5+M \pmod{8},\quad y=\eta+\zeta, \tag{40}$$

are not solvable. For, $Z^2+Y^2+\zeta^2\equiv 3 \pmod 4$ requires that Z, Y, ζ be all odd. By $Y\equiv\eta \pmod 2$, η is odd and y even. The left member of (40) is $M+1+\lambda$ (mod 8).

(b) Let $M=2m$. Write t for the odd integer $M-r$. Let ϕ denote the sum of the terms other than the first and last in the left member of (38). Then $\phi=2m\eta^2+2m\zeta^2+2t\eta\zeta$. For η even, $\phi\equiv 0,\ 2m,\ 2m+4 \pmod 8$. By symmetry, ϕ takes the same values when ζ is even. For η and ζ both odd, $\phi\equiv 4m\pm 2$ (mod 8).

(b_1) Let $m=2\mu$. Then ϕ takes all even values modulo 8. This holds also modulo 2^e. For proof, take $\eta=1$. Then $\phi=2m+2\psi$, $\psi=2\mu\zeta^2+t\zeta$. By (I) of §9, ψ ranges with ζ over a complete set of residues modulo 2^{e-1}. Give Z the values 0 and 1. Hence (38) is solvable with $x=0$, κ arbitrary.

(b_2) Let m be odd. Then $\phi\equiv 0,\ 2,\ 6 \pmod 8$. Hence (38) is not always solvable modulo 8 if $e\geqq 4$ and F_1 is then not universal. This is true also if $e=3$. For, we saw that $\phi+Z^2$ fails to represent 4 or 5 (mod 8). Suppose that

$$4rAxy+\phi+Z^2\equiv 4 \text{ or } 5 \pmod{8}. \tag{41}$$

Then

$$\phi + Z^2 \equiv 0 \text{ or } 1, \quad \phi \not\equiv 2, \quad \phi \equiv 0 \pmod 4, \quad \eta^2 + \zeta^2 + \eta\zeta \equiv 0 \pmod 2,$$

whence η and ζ are even. Thus y is even and (41) is impossible.

THEOREM 11. *Let $e \geqq 2$, $c=2C$, $j=2s$, d and l be odd. Write $\lambda = g^2d^2 \cdot (lh-s^2)$, $R=gdlC$. If $\lambda \equiv 0 \pmod 4$, F is universal. Next, let $\lambda = 2r$, $R=2\rho$, where r is odd. If $e=2$, F is universal. For $e \geqq 3$, write $T=rg^2dlb-2\rho^2$. If $T\equiv 0$, 2, or 6 (mod 8), F is not universal. If $T\equiv 4$ (mod 8), F is universal if and only if $e=3$. If T is odd, write $2M=T+r$. Then F is universal if and only if $M\equiv 0$ or 3 (mod 4). Throughout, universality is to be qualified by excepting cases* (25).

19. Consider (35) for R odd, $\lambda \equiv 2 \pmod 4$. We may assume that $R\equiv 1 \pmod{2^{e+2}}$. For, if $R=1+2\gamma$, $\lambda=2r$, replace z by $z+\epsilon y$. We obtain a form like (35) with

$$R' = 1 + 2(\gamma + r\epsilon), \qquad B' = B + 2R\epsilon + 2r\epsilon^2.$$

Since r is odd, we may choose ϵ so that $\gamma + r\epsilon \equiv 0 \pmod{2^{e+1}}$. Note that $B' \equiv B \pmod 4$, so that the later conditions for universality are independent of this transformation.

If $B\equiv 1 \pmod 4$, there is no solution of $f\equiv \lambda+5 \pmod 8$. The latter implies

$$(y + z)^2 + z^2 + W^2 \equiv 3 \pmod 4.$$

Whence $y+z$, z, W are all odd. Then $y=2Y$ and

$$f \equiv 4Y^2 + 4Y + \lambda + 1 \equiv \lambda + 1 \pmod 8.$$

If $B\equiv 2 \pmod 4$, there is no solution of $f\equiv 5 \pmod 8$. That implies $2\phi + W^2 \equiv 1 \pmod 4$, $\phi = y^2+yz+z^2$, whence W is odd and ϕ is even. Thus y and z are even and $f\equiv W^2 \pmod 8$.

Hence when f is universal, $B\equiv 0$ or 3 (mod 4).

First, let $x=0$, $y=1$, $z=2Z$. Then $f=B+4Z+4\lambda Z^2+W^2$. By (I) of §9, $Z+\lambda Z^2$ ranges with Z over a complete set of residues modulo 2^n. Hence f represents all $4t+B$ and $4t+B+1 \pmod{2^n}$.

Second, let $x=0$, $y=2Y$, $z=1$, where Y is odd. Then

$$f \equiv 4BY^2 + 4Y + \lambda + W^2. \tag{42}$$

If k is any odd integer, $f\equiv 2k \pmod{2^n}$ is solvable with $W=2\omega$. Since $2k-\lambda$ is a multiple 4ϵ of 4, this is equivalent to $BY^2+Y+\omega^2\equiv\epsilon \pmod{2^{n-2}}$. But $Y=2\eta+1$. Hence $2\tau+B+1+\omega^2\equiv\epsilon$, where $\tau=2B\eta^2+(2B+1)\eta$. But τ ranges with η over a complete set of residues. Hence the congruence is solvable with $\omega=0$ or 1. Thus if κ is any integer $\equiv 2 \pmod 4$, $f\equiv\kappa$ (mod 2^n) is solvable with y a double of an odd integer.

Third, let $x=0$, $z=1$, $y=4\eta$, $\eta=2\xi+1$. Then

$$f\equiv 16B\eta^2+8\eta+\lambda+W^2=16\mu+16B+8+\lambda+W^2,$$

where $\mu=4B\xi^2+(4B+1)\xi$ ranges with ξ over a complete set of residues modulo 2^n. Take $W=1$ and 3. Thus if $k\equiv\lambda+1 \pmod 8$, $f\equiv k$ (mod 2^n) is solvable.

When $B\equiv 0 \pmod 4$, our three cases dispose of all except $\lambda+5 \pmod 8$. We then take $W=1$ in (42). Cancellation of 4 now gives $BY^2+Y\equiv 1$, $2\tau+B+1\equiv 1$ (mod 2^{n-2}), which is solvable for η.

When $B\equiv 3 \pmod 4$, our first two cases dispose of all except 1 (mod 4). Take $x=0$, $y=4\eta=4(2\xi+1)$, $z=2$. Then

$$f=16B\eta^2+16\eta+4\lambda+W^2=32u+16(B+1)+4\lambda+W^2,$$

where $u=2B\xi^2+(2B+1)\xi$ ranges with ξ over a complete set of residues modulo 2^n. Take $W=1, 3, 5, 7$. Then $32u+W^2$ represents all $8\sigma+1$, and the same is true of f modulo 2^n. There remains only the $8\sigma+5$. We take $x=0$, $z=2$, $y=2Y$, $Y=2\eta+1$. Write $B+1=4b$. Then

$$Bf=4\epsilon^2-4+4B\lambda+BW^2,\quad \epsilon=BY+1=2\tau,$$
$$\tau=B\eta+2b.$$

We may employ τ as a new variable in place of η modulo 2^n. If $k\equiv B \pmod 8$, $16\tau^2+BW^2\equiv k$ (mod 2^n) is solvable with W odd. For $m\geqq 3$, let $16\tau^2+BW^2=k+2^mQ$. Then

$$16\tau^2+B(W+2^{m-1}\omega)^2\equiv k+2^m(Q+BW\omega)\equiv k \pmod{2^{m+1}}$$

by choice of ω modulo 2. Hence if $\kappa\equiv B+4 \pmod 8$, $Bf\equiv\kappa$ (mod 2^n) is solvable. Thus $f\equiv 8\sigma+5$ (mod 2^n) is solvable when σ is arbitrary.

THEOREM 12. *Employ the initial assumptions and notations of Theorem* 11. *Write* $B=g^2dbl$. *Now let R be odd and* $\lambda\equiv 2 \pmod 4$. *Except in cases* (25), *F is universal if and only if* $B\equiv 0$ *or* 3 (mod 4).

20. Finally, consider (35) for $R=2\rho$, $\lambda=4r$. Then $f\equiv By^2+W^2 \pmod 4$, and f has the values 0, 1, B, $B+1$, which form a complete set of residues only if $B\equiv 2 \pmod 4$.

First, let $e=2$. For y odd, $f\equiv 2$ or 3 (mod 4). For $y=2Y$, $f\equiv 4rz^2+W^2 \pmod 8$, independently of Y. If r is even, $f\equiv 5 \pmod 8$ is impossible, and F is not universal. But if r is odd, $f\equiv 0, 1, 4, 5 \pmod 8$ for Y odd, and F is universal.

Next, let $e \geqq 3$. If r is even, $f \equiv By^2+4\rho yz+W^2 \equiv 5 \pmod 8$ is impossible, since it holds modulo 4 only when W is odd and y is even. If r and ρ are odd, $f \equiv By^2+4yz+4z^2+W^2 \equiv B+5 \pmod 8$ is impossible, since it holds modulo 4 only when W and y are odd.

There remains only the case $B=2\beta$, $\rho=2\sigma$, with β, σ, r all odd. Write $Z=rz+\sigma y$, $T=r\beta-2\sigma^2$. Then

$$F_1 = rf = 2^e rAxy + \phi, \quad \phi = 4Z^2 + 2Ty^2 + rW^2.$$

As in §17, F is universal except in cases (25) if and only if $F_1 \equiv k \pmod{2^{2e}}$ is solvable when k is arbitrary, when both even and odd values of y are allowed. The even residues modulo 8 of ϕ are 0, 4, $2T$, $2T+4$, which are a permutation of 0, 2, 4, 6. The odd residues are obtained by adding r to these four. Hence $F_1 \equiv k \pmod 8$ is solvable when k is arbitrary.

For κ odd, $\kappa - T = 2q$. Then $\phi \equiv 2k \pmod{16}$ requires

$$W = 2w, \quad y \text{ odd}, \quad Z^2 + rw^2 \equiv q \pmod 4.$$

But $Z^2+rw^2 \equiv 0, 1, r, r+1 \pmod 4$, which lack 3 or 2 according as $r\equiv 1$ or $3 \pmod 4$. Hence $\phi \equiv k \pmod{16}$ is impossible for certain integers k, whence F is not universal if $e \geqq 4$.

If $e=3$, $B\equiv 2 \pmod 4$, r is odd and ρ even, we shall prove that F is universal. For y odd,

$$f - B \equiv 4z^2 + W^2 \equiv 0,1,4,5 \pmod 8.$$

Since $f-B$ takes the values 0, 1 (mod 4),

$$f \equiv 2,3,6,7,10,11,14,15 \pmod{16}. \tag{43}$$

For $y=2Y$, Y odd, $f-4B \equiv \psi = 4rz^2+W^2 \pmod{16}$.

(i) Let $r\equiv 1 \pmod 4$. Then $\psi \equiv 0, 1, 4, 5, 8, 9, 13 \pmod{16}$. To these we add $4B\equiv 8$ and get 0, 1, 5, 8, 9, 12, 13 (mod 16). From these and (43) only 4 is missing. For $y=4\eta$, $f\equiv 4rz^2+W^2 \pmod{32}$. We take $W=2$, $z=0$, 2 and get 4, 20 (mod 32) and hence the missing 4 (mod 16).

(ii) Let $r\equiv 3 \pmod 4$. Then $\psi\equiv 0, 1, 4, 5, 9, 12, 13 \pmod{16}$. To these we add $4B\equiv 8$ and get 1, 4, 5, 8, 9, 12, 13. From these and (43) only 0 is missing. We use $y=4\eta$, $z=0$, $W=0$, 4 and get 0, 16 (mod 32).

THEOREM 13. *Employ the initial assumptions and notations of Theorem* 11. *Write* $B=g^2dbl$. *Now let* $R=2\rho$, $\lambda=4r$. *Except in cases* (25), *F is universal if and only if* $B\equiv 2 \pmod 4$, *either* $e=2$, *and r odd, or* $e=3$, *r odd and ρ even.*

Theorems 10–13 cover all classic forms with $e>1$, d and l odd, c and j even. The remaining forms will be treated in a later paper.

Part III. Equivalence and canonical forms

21. We consider henceforth only classic forms f in which the coefficients of products of different variables are all even. By the Hessian of f is meant the determinant of the halves of the second partial derivatives of f. We shall prove

Theorem 14. *The Hessian H of a universal classic ternary quadratic Null form f is either odd or the double of an odd integer. In the respective cases, f is equivalent to*

$$\phi = 2xy - Hz^2, \quad \psi = 2xy + y^2 - Hz^2. \tag{44}$$

Each of these forms is universal.

By §8, f is equivalent to

$$2Axy + By^2 + 2Cyz + Dz^2, \quad A \text{ odd}. \tag{45}$$

First, let $A=1$. Replacing x by $x+ky-Cz$, we get a form like (45) with $C'=0$, $B'=B+2k=0$ or 1 by choice of k. Then $H=-D$ and we have (44).

First, let H be even. Then ϕ is excluded. If $H\equiv 0 \pmod 4$, ψ is never $\equiv 2 \pmod 4$. Hence $H\equiv 2 \pmod 4$ in ψ. For $y=1, z=0$; $y=2, z=0, 1$, the values of ψ are $2x+1$, $4(x+1)$, $4(x+1)-H$, which together give all integers.

Second, let H be odd. In ψ replace x by $x+Hz$ and z by $z+y$; we get $2xy+(1-H)y^2-Hz^2$. We now replace x by $x+\frac{1}{2}(H-1)y$ and get ϕ. Hence we may drop ψ. The values of ϕ for $y=1$, $z=0, 1$ are $2x$ and $2x-H$ and together give all integers.

This proves Theorem 14 when $A=1$.

22. Case A prime to D. There exist solutions s and t of $Ds-At=C$. Replacing x by $x+tz$, we get a form (45) having $C'=C+At=Ds$. We now, replace z by $z-sy$ and obtain a form (45) lacking yz. In the notation (3), it has $g=1$ and is

$$F = 2axy + by^2 + dz^2 \quad (a \text{ odd and prime to } d). \tag{46}$$

If F is universal the first part of §5 with $t=a$, $c=0$, shows that $-bd$ is a quadratic residue of each power of a prime which divides a and hence of a itself. Thus b is prime to a, and $b=-r^2d+am$, where r and m are integers, and r is prime to a.

(I) Let d be odd. If m is even, write $m=2\mu$, $r=\rho$. Then

$$b = -\rho^2 d + 2a\mu \quad (\rho, a \text{ relatively prime}). \tag{47}$$

If m is odd, then $m+2rd+ad$ is an even integer 2μ; for $\rho=r+a$ we again have (47). For $x=X-\mu y$, (46) becomes

$$F = 2aXy - \rho^2dy^2 + dz^2.$$

Put $z = Z + \rho y$. Then $F = 2y\xi + dZ^2$, where $\xi = aX + \rho dZ$. Since a and $d\rho$ are relatively prime, there exist solutions of $av - d\rho u = 1$. Write $\eta = uX + vZ$. The transformation from X, Z to ξ, η is of determinant unity and replaces F by $2y\xi + d(a\eta - u\xi)^2$. Replacing y, ξ, η by x, y, z, we obtain a form (45) having $A = 1$.

(II) Let d be even. If F is universal, b is odd and $d \equiv 2 \pmod 4$. For, if $d \equiv 0 \pmod 4$, F is never $\equiv 2 \pmod 4$. Thus $d = 2D$, where D is odd. Then m is odd, $m = 2n+1$. Replacing x by $x - ny$, we obtain

$$F = 2axy + Ty^2 + 2Dz^2, \quad T = a - 2r^2D.$$

Write $\theta = 4r^2D - a$. Since $4rD$ is prime to a, it is prime to θ. Hence there exist integers β and γ satisfying $4rD\gamma - \theta\beta = 1$. Now $F = 0$ for $x = -1$, $y = 2$, $z = 2r$. Hence the substitution

$$x = -\xi, \quad y = 2\xi + \beta\eta + 4D\zeta, \quad z = 2r\xi + \gamma\eta + \theta\zeta$$

has determinant unity and replaces F by a form G in which the coefficient of ξ^2 is zero. That of $2\xi\eta$ is

$$-a\beta + 2T\beta + 4Dr\gamma = a\beta + 4rD(\gamma - r\beta) = 4rD\gamma - \theta\beta = 1.$$

That of $\xi\zeta$ is $8rD(\theta - a + 2T) = 0$. Replacing ξ, η, ζ by x, y, z, we see that G is of the type (45) with $A = 1$.

The Hessian $-a^2d$ of (46) is odd in (I) and $\equiv 2 \pmod 4$ in (II). This completes the proof of

THEOREM 15. *When A is odd and prime to D,* (45) *is equivalent to* (46), *which is universal if and only if $-bd$ is a quadratic residue of a and either d is odd or b is odd and $d \equiv 2$* (mod 4). *In the respective cases,* (46) *is equivalent to* (44).

This proves Theorem 14 when A is prime to D.

23. Let the form (3) be universal and classic, whence $e \geqq 1$, $c = 2C$, $\psi = c_{11}z^2 + 2c_{12}zw + \cdots$, where $c_{11}, c_{12}, \cdots$ have no common factor >1.

If b is even, then d is odd and $c_{11}, c_{22}, c_{33}, \cdots$ are not all even. We may assume that c_{11} is odd. If the number n of variables is 3, $c_{11} = 1$. If $n > 3$ and if c_{11} is even and c_{22}, for example, is odd, replace w by $w + z$; then the new c_{11} is odd. In (3) we replace z by $z + gy$ and obtain a form $2^e gaxy + \phi(y, z, w, \cdots)$ in which the coefficient of y^2 is the product of g by $b + 2C + dg^2c_{11}$, which is odd. Hence (3) is equivalent to a like form with b odd.

Let D be the g.c.d. of $a = D\alpha$ and $b = D\beta$. Then D, α, β are odd, while

$2^e\alpha$ and β are relatively prime. Let E be the g.c.d. of $D=E\delta$ and $C=E\gamma$. Then δg is prime to 2γ. Hence there are solutions $r, s; M, v; h, u$ of

$$2^e\alpha r+\beta S=-2\gamma, \tag{48}$$

$$\delta g M+2\gamma v=1,\quad 2^e\alpha h+\beta u=M. \tag{49}$$

The form (3) is

$$F=2^e gE\delta\alpha xy+gE\delta\beta y^2+2E\gamma yz+gd\psi(z,w,\cdots). \tag{50}$$

Consider the linear substitution

$$S:\qquad \begin{aligned} x &= \beta X+hY+rZ,\\ y &= -2^e\alpha X+uY+sZ,\\ z &= vY+g\delta Z, \end{aligned}$$

which does not alter w, etc. Multiply the second row of its determinant Δ by β. To the new second row add the product of the first row by $2^e\alpha$ and apply (48) and (49_2). Hence

$$\beta\Delta=\beta\begin{vmatrix} M & -2\gamma\\ v & g\delta\end{vmatrix},\qquad \Delta=1$$

by (49_1). We see that S replaces F by a form in which the coefficient of X^2 is zero, and that of XY is

$$2^e gE\delta\alpha(\beta u-2^e\alpha h)+gE\delta\beta(-2\cdot 2^e\alpha u)+2E\gamma(-2^e\alpha v)$$
$$=-2^e\alpha E(g\delta M+2\gamma v)=-2^e\alpha E,$$

by (49). The coefficient of XZ is the product of $-2^e gE\alpha\delta$ by $-\beta S+2^e\alpha r+2\beta s+2\gamma=0$, by (48). Changing the signs of Y and Z, we get an equivalent form

$$2^e\alpha EXY+\chi(Y,Z,w,\cdots). \tag{51}$$

Let m denote the minimum odd positive integer such that a given universal classic form is equivalent to $2^e mxy+\phi(y, z, w,\cdots)$. By (50), $m=gE\delta\alpha$. Since F is equivalent to (51), $\alpha E\geqq m$. Hence $1\geqq g\delta$, $g=\delta=1$.

Since $g=1$ and a is prime to d, when we express a ternary form (3) with $e=1$ in the notation (45), we see that A is prime to D. Hence Theorem 15 applies and proves Theorem 14.

Incidentally we have also

THEOREM 16. *Every universal classic Null quadratic form is equivalent to* (2) *with $A=2^e m$, where the minimum m is prime to Δ, $c=2C$, m and B are odd and their g. c. d. divides C.*

PART IV. ALL UNIVERSAL $f=ax^2+by^2+cz^2$

24. THEOREM 17. *f is universal if and only if* (i) *a, b, c are not all of like sign and no one is zero*; (ii) *a, b, c are relatively prime in pairs*; (iii) *$-bc$, $-ac$, $-ab$ are quadratic residues of a, b, c, respectively*; (iv) *abc is odd or double an odd integer.*

This was proved elsewhere* by the writer. We shall give here a new proof that the conditions are sufficient. By† (i), (ii), (iii), $f=0$ has solutions ξ, η, ζ, relatively prime in pairs. Then $s\xi-r\eta=1$ has solutions s, r. The substitution

$$x = \xi X + rY, \quad y = \eta X + sY, \quad z = \zeta X + Z$$

has determinant unity and replaces f by

$$F = 2uXY + 2c\zeta XZ + vY^2 + cZ^2,$$

where $u = a\xi r + b\eta s$, $v = ar^2 + bs^2$.

The Hessians abc and $-c(u^2+cv\zeta^2)$ of f and F must be equal, whence

$$u^2 + cv\zeta^2 = -ab. \tag{52}$$

This follows also from the identity

$$u^2 - v(a\xi^2 + b\eta^2) \equiv -ab(s\xi - r\eta)^2$$

in ξ, η. By (52) and (ii), no prime divides both u and c. Suppose u and ζ have a common prime factor p. By (52), p divides ab. If p divides a, it divides the second term of $a\xi^2+b\eta^2+c\zeta^2=0$, whereas b is prime to a, and η to ζ. Similarly, p cannot divide b.

Hence the coefficients of $y_1=uY+c\zeta Z$ are relatively prime. Thus there is another linear function z_1 of Y and Z such that the determinant of the coefficients in y_1 and z_1 is unity. Hence F is equivalent to $2Xy_1+\phi$, where ϕ is quadratic in y_1 and z_1. The new form is of type (45) with $A=1$. Its Hessian abc has property (iv). By §21, it is universal.

Finally, we give a new proof that (i)-(iv) are necessary conditions that a Null form f be universal. Such an f is equivalent to F in §8 with $e=1$. Then the Hessian of F is $-A^2D$, where D is odd or double an odd. This proves (iv). If a and b have a common odd prime factor p, $f\equiv cz^2 \pmod{p}$ and f would not be universal. This proves (ii). Suppose that $-bc$ is a non-residue of an odd prime factor p of $a=pA$. Consider values x, y, z for which f is divisible by p. Then $-bcy^2\equiv(cz)^2 \pmod{p}$, whence $y\equiv z\equiv 0$, $f=pF$, $F\equiv Ax^2 \pmod{p}$, and f would not be universal.

* Bulletin of the American Mathematical Society, vol. 35 (1929).

† Dirichlet-Dedekind, *Zahlentheorie*, 4th edition, §157, p. 432.

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.