A NEW DEFINITION OF GENUS FOR TERNARY QUADRATIC FORMS*

BY

BURTON W. JONES†

1. Introduction. The adjoint of the form $f=ax^2+by^2+cz^2+2ryz+2sxz+2txy$ is $\mathfrak{F}=Ax^2+By^2+Cz^2+2Ryz+2Sxz+2Txy$ where A is the cofactor of a, etc., in the Hessian of f, the Hessian being the determinant of the halves of the second derivatives of f. The primitive contravariant or reciprocal form F of f is $\mathfrak{F}/\Omega$ where Ω is the greatest common divisor of the literal coefficients of $\mathfrak{F}$. The Hessian $H=\Omega^2\Delta$.

The genus of the form f is defined by H. J. S. Smith‡ in terms of the quadratic character of the integers represented by f and F with respect to the odd prime factors of the Hessian, the congruences mod 8 satisfied by the odds represented by f and F and, in certain cases, certain so-called "simultaneous characters."

The "simultaneous characters" are redundant and L. E. Dickson§ omits them in his definition of genus. However, since these additional characters used by Smith and known by him to be redundant (see p. 470 of his article) are closely linked with the arithmetic progressions associated with a form, the author has retained them in his discussion.

In this paper, Smith's definition is shown to be equivalent to a *new* definition of genus expressed in terms of the integers represented by the form f alone without reference to F. (A more precise phrasing of this statement will be found in the theorem of this paper.) Furthermore, f may be indefinite or positive and the character of the integers represented is shown to determine the order (as well as Ω and Δ) of the form.

The new definition proved in this paper has immediate application in proving the important theorem shortly to be published that the integers represented by all the forms of a given genus fall exclusively in certain arithmetic progressions. An example of the ease of application of this definition to finding the genus of a form is given at the end of the paper.

Also, it should be noted that this new definition is peculiar to ternary quadratic forms, for the genus of a binary form depends on the character

* Presented to the Society, October 25, 1930; received by the editors in May, 1930.

† National Research Fellow.

‡ Collected Mathematical Papers, vol. 1, pp. 455–509. This article is constantly being referred to.

§ *Studies in the Theory of Numbers*, p. 52.

of the odd integers represented prime to the determinant and many quaternary forms are universal, i.e. represent all integers, positive if the form is positive.

2. **Notations.** $\phi=\alpha x^2+\beta y^2$, p denotes an odd prime, q a prime, k indicates the range of values $0, 1, 2, \cdots$, and $n=0, \pm 1, \pm 2, \cdots$. The form f of the introduction is abbreviated by enclosing the coefficients in parentheses: $(a, b, c, 2r, 2s, 2t)$; in case $r=s=t=0$ we use the notation $f=(a, b, c)$. For any integers a and b, μ_{ab} is that least positive integer for which a/μ_{ab} is an integer prime to b. Unless otherwise indicated, all letters denote integers. The letters f and g with subscripts and superscripts are used to denote ternary quadratic forms and $(f\,|\,p)=(a\,|\,p)$ means that the integers prime to p represented by f are all of the same quadratic character mod p as a. We use the usual notation $[a/b]$ for the greatest integer in a/b. The other notations used in this paper are explained in H. J. S. Smith's article previously referred to.

3. **Lemmas.** In this section we shall prove a number of lemmas.

LEMMA 1. *$\phi\equiv a \pmod p$, a prime to p, is solvable for all and only the a's for which $(a\,|\,p)=(\alpha\,|\,p)$ or for all a's according as $\alpha\not\equiv 0\equiv\beta \pmod p$ or $\alpha\beta\not\equiv 0 \pmod p$.*

If $\beta\equiv 0\not\equiv\alpha \pmod p$ the proof is obvious. If $\alpha\beta\not\equiv 0 \pmod p$ note* that αx^2 and $a-\beta y^2$ each take $(p+1)/2$ incongruent values mod p as the values of x and y range over all integers and that therefore, for some value of x and y, we have $\alpha x^2\equiv a-\beta y^2 \pmod p$.

LEMMA 2. *$\phi\equiv a \pmod{p^2}$ is solvable for every a prime to p if $\alpha\beta\not\equiv 0 \pmod p$.*

This follows from Lemma 1 by an elementary proof similar to that used in the Annals article referred to above.

COROLLARY 1. *$f=\alpha x^2+\beta y^2+\gamma z^2\equiv ap^r \pmod{p^{r+1}}$, $r=0, 1$, is solvable if $a\alpha\beta\gamma\not\equiv 0 \pmod p$ for we may then take $z=1$ or p according as $r=1$ or 0 and $\alpha x^2+\beta y^2\equiv ap^r-\gamma z^2 \pmod{p^2}$ is solvable.*

COROLLARY 2. *The above corollary holds for all r for $f\equiv ap^r \pmod{p^{r+1}}$ implies, multiplying the variables by p, that $f\equiv ap^{r+2} \pmod{p^{r+3}}$ solvable, etc.*

LEMMA 3. *$\phi\equiv ap \pmod{p^2}$ is solvable for every a prime to p or for none according as $(-\alpha\beta\,|\,p)=1$ or -1 and in the latter case $\phi\equiv 0 \pmod p$ implies $x\equiv y\equiv 0 \pmod p$.*

Suppose $\alpha x^2+\beta y^2\equiv 0 \pmod p$ with both x and y prime to p. Choose x' so that $xx'\equiv 1 \pmod p$ and have $\alpha\equiv -\beta(yx')^2 \pmod p$ which implies $(-\alpha\beta\,|\,p)=1$.

* Cf. Annals of Mathematics, (2), vol. 28 (1927), p. 333.

Otherwise one and therefore both of x and y are divisible by p. On the other hand if $(-\alpha\beta\,|\,p)=1$ there exists a solution (x_1, y_1) of $\alpha x^2+\beta y^2\equiv 0 \pmod{p}$ with $x_1y_1\not\equiv 0 \pmod{p}$. Consider the set (x_1, y_i) where $i=1, 2, \cdots, p$ and $y_{i+1}^2\equiv y_i^2+p \pmod{p^2}$. Note $y_i^2\not\equiv y_j^2 \pmod{p^2}$ if $i\neq j$ and see that $\alpha x_1^2+\beta y_i^2 \equiv 0 \pmod{p}$ takes p incongruent values mod p^2 one of which must be $\equiv ap \pmod{p^2}$.

COROLLARY. $\phi\equiv ap^r \pmod{p^{r+1}}$, $r=0, 1$, *is solvable for every a prime to* p *if* $(-\alpha\beta\,|\,p)=1$.

LEMMA 4. $f=\alpha x^2+\beta y^2+\gamma pz^2\equiv a \pmod{p\mu_{ap}}$ *is solvable for every a if* $(-\alpha\beta\,|\,p)=1$.

This is true for $a\not\equiv 0 \pmod{p^2}$ with $z=0$ from the above corollary and thus is true, multiplying each variable by p, for $ap^2\not\equiv 0 \pmod{p^4}$. This may be continued to prove the lemma.

COROLLARY. *If* $(-\beta\gamma\,|\,p)=1$ *and* $\alpha\not\equiv 0 \pmod{p}$, $f\equiv\alpha x^2+\beta py^2+\gamma pz^2\equiv a \pmod{p\mu_{ap}}$ *is solvable if and only if a is not of the form* $pn+\alpha_{-1}$ *where* $(\alpha_{-1}\,|\,p)=-(\alpha\,|\,p)$.

This follows from Lemmas 1 and 4 if we note that $f\equiv 0 \pmod{p}$ implies $x=px_1$.

LEMMA 5. $f=\alpha x^2+\beta y^2+\gamma pz^2\equiv a \pmod{p\mu_{ap}}$, *where* $\gamma\not\equiv 0 \pmod{p}$ *and* $(-\alpha\beta\,|\,p)=-1$, *is solvable if and only if a is not of the form* $p^{2k}(p^2n+p\gamma_{-1})$ *where* $(\gamma_{-1}\,|\,p)=-(\gamma\,|\,p)$.

If a is prime to p, the proof follows from Lemma 1. Thus Lemma 5 holds for all $ap^{2r}\not\equiv 0 \pmod{p^{2r+1}}$. On the other hand $f\equiv 0 \pmod{p}$ implies, by Lemma 3, $x=px_1$, $y=py_1$, and $f/p\equiv\alpha px_1^2+\beta py_1^2+\gamma z^2\equiv a_1 \pmod{p}$ solvable for a_1 prime to p if and only if $(a_1\,|\,p)=(\gamma\,|\,p)$. This proves the lemma for $a=a_1p\not\equiv 0 \pmod{p^2}$. The congruence $f\equiv 0 \pmod{p^3}$ implies $x\equiv y\equiv pz\equiv 0 \pmod{p^2}$ and $f/p^3=\alpha px_2^2+\beta py_2^2+\gamma z_1^2\equiv a_2 \pmod{p}$ which is solvable for a_2 prime to p if and only if $(a_2\,|\,p)=(\gamma\,|\,p)$ and so the process may be continued.

COROLLARY. *If* $(-\beta\gamma\,|\,p)=-1$ *and* $\alpha\not\equiv 0 \pmod{p}$, $f=\alpha x^2+\beta py^2+\gamma pz^2\equiv a \pmod{p\mu_{ap}}$ *is solvable if and only if a is not of the form* $p^{2k}(pn+\alpha_{-1})$ *where* $(\alpha_{-1}\,|\,p)=-(\alpha\,|\,p)$.

LEMMA 6. *If* $\alpha\beta\equiv 1 \pmod{4}$, $\phi\equiv 2a \pmod{16}$, *with a odd, is solvable if and only if* $2a\equiv\alpha+\beta \pmod{8}$.

$\alpha+\beta\equiv\alpha+9\beta \pmod{8}$ but they are not congruent mod 16. Thus, if $2a\equiv\alpha+\beta \pmod{8}$, one of $\alpha+\beta$, $\alpha+9\beta$ is $\equiv 2a \pmod{16}$. It is obvious that $\alpha x^2+\beta y^2\equiv\alpha+\beta+4 \pmod{8}$ is not solvable.

LEMMA 7. *If* $\alpha\beta\equiv 3 \pmod 8$, $\phi\equiv 4a \pmod{32}$ *is solvable for every odd* a *and* $\phi\equiv 0 \pmod 8$ *implies* $x\equiv y\equiv 0 \pmod 2$.

The proof is similar to that above.

LEMMA 8. *If* $\alpha\beta\equiv 7 \pmod 8$, $\phi\equiv 2^{r+2}a \pmod{2^{r+5}}$, $r\geqq 0$, *is solvable for every odd* a.

For $r=1$, the proof is similar to the above. $\phi\equiv 4 \pmod 8$ implies $x=2x_1$, $y=2y_1$ and $\phi/4=\alpha x_1^2+\beta y_1^2\equiv a \pmod 8$ is solvable for every odd a. Thus $\phi\equiv 4a \pmod{32}$ is solvable for every odd a.

LEMMA 9. $f=\alpha x^2+\beta y^2+\gamma z^2\equiv a \pmod{8\mu_{a2}}$ *with* $\alpha\beta\gamma\equiv 1 \pmod 8$ *is solvable if and only if* a *is not of the form* $4^k(8n+7)$ *or for all* a *according as* $\alpha\equiv\beta\equiv\gamma\equiv 1 \pmod 4$ *or not.*

If $a\equiv 2 \pmod 4$ note that two of α, β, γ are congruent (mod 4) and, permuting coefficients if necessary, take $\alpha\equiv\beta \pmod 4$. Then $a-16\gamma$ or $a-4\gamma\equiv\alpha+\beta \pmod 8$ and Lemma 6 applies to complete the proof. If a is odd, $f\equiv a \pmod 8$ is solvable unless $\alpha\equiv\beta\equiv\gamma \pmod 4$. Then $\alpha\beta\equiv\gamma \pmod 8$ implies $1\equiv\alpha\equiv\beta\equiv\gamma \pmod 4$ and $f\equiv a \pmod 8$ is solvable if and only if $a\not\equiv\alpha+\beta+\gamma+4\equiv\alpha+\beta+\alpha\beta+4\equiv 7 \pmod 8$. Furthermore, if $\alpha\equiv\beta\equiv\gamma \pmod 4$, $f\equiv 0 \pmod 4$ implies $x\equiv y\equiv z\equiv 0 \pmod 2$ and f represents an integer $4n$ if and only if it represents n.

LEMMA 10. $f=\alpha x^2+\beta y^2+2\gamma z^2\equiv a \pmod{8\mu_{a2}}$ *is solvable for every* a *if* $\alpha\beta\gamma\equiv 1 \pmod 8$ *and* $\alpha+\beta\equiv 6$ *or* $0 \pmod 8$.

This is obvious if μ_{a2} is an even power of 2. Consider $a\equiv 2 \pmod 4$. Then $f\equiv a \pmod{16}$ is solvable from Lemma 8 taking $z=1$ or Lemma 6 taking $z=0$ unless $\alpha+\beta\equiv 6 \pmod 8$ and $a\equiv\alpha+\beta+4\equiv 2 \pmod 8$. Now $f\equiv 2 \pmod 8$ implies $x=2x_1$, $y=2y_1$, and $f\equiv a \pmod{16}$ is solvable for $a\equiv 2 \pmod 8$ if and only if $f/2=2\alpha x_1^2+2\beta y_1^2+\gamma z^2\equiv a/2 \pmod 8$ is solvable. Now $\alpha+\beta\equiv 6 \pmod 8$ implies $\alpha\beta\equiv\gamma\equiv 1 \pmod 4$ and thus γ and $\gamma+2\alpha+2\beta\equiv\gamma+4 \pmod 8$ are $\equiv 1$ and 5 (mod 8) in some order. Thus $f/2\equiv a/2 \pmod 8$ is solvable, $f\equiv a \pmod{16}$ is solvable for all $a\equiv 2 \pmod 4$, and therefore $f\equiv 4^k a \pmod{4^{k+2}}$ is solvable for all $a\equiv 2 \pmod 4$.

COROLLARY. $f=2\alpha x^2+2\beta y^2+\gamma z^2\equiv a \pmod{8\mu_{a2}}$, *where* $\alpha\beta\gamma\equiv 1 \pmod 8$ *and* $\alpha+\beta\equiv 6$ *or* $0 \pmod 8$, *is solvable if and only if* a *is not of the form* $8n+3$.

If a is odd, $f\equiv\gamma, \gamma+2\beta, \gamma+2\alpha, \gamma+2\alpha+2\beta \pmod 8$ is solvable and $f\equiv$ no other odd (mod 8) is solvable. If $\alpha+\beta\equiv 0 \pmod 8$, $\alpha\beta\equiv\gamma\equiv 7 \pmod 8$ and $f\not\equiv 7+4\equiv 3 \pmod 8$. If $\alpha+\beta\equiv 6 \pmod 8$, $\alpha\beta\equiv\gamma\equiv 1 \pmod 4$ and $f\not\equiv\gamma+6\alpha\equiv\alpha(\beta+6)\equiv\alpha(4-\alpha)\equiv 3 \pmod 8$. $f\equiv 1, 5, 7 \pmod 8$ is solvable in both cases. $f\equiv 0 \pmod 2$ implies $z=2z_1$ and the rest follows from Lemma 10.

LEMMA 11. *If* $\alpha\beta\gamma \equiv 1 \pmod 8$ *and* $\alpha+\beta \equiv 2$ *or* $4 \pmod 8$, $f=\alpha x^2+\beta y^2+2\gamma z^2 \equiv a \pmod{8\mu_{a2}}$ *is solvable if and only if* a *is not of the form* $4^k(16n+14)$.

As above we consider $a \equiv 2 \pmod 4$. Then $f \equiv a \pmod{16}$ is solvable from Lemmas 6 and 7 taking $z=0$ and 1 respectively unless $a \equiv 6 \pmod 8$, for $\alpha+\beta \equiv 4 \pmod 8$ implies $\alpha\beta \equiv \gamma \equiv 3 \pmod 8$ and $\alpha+\beta+2\gamma \equiv 2 \pmod 8$. Now $f \equiv 6 \pmod 8$ implies $x=2x_1$, $y=2y_1$ and $f/2=2\alpha x_1^2+2\beta y_1^2+\gamma z^2$. If $\alpha+\beta \equiv 2 \pmod 8$, then $\alpha\beta \equiv 1 \equiv \gamma \pmod 4$, $f/2 \equiv \gamma+2\alpha \equiv \alpha(\beta+2) \equiv 3 \pmod 8$, but $f/2 \not\equiv \gamma+6\alpha \equiv 7 \pmod 8$. If $\alpha+\beta \equiv 4 \pmod 8$, $\alpha\beta \equiv 3 \equiv \gamma \pmod 8$ implies $f/2 \equiv 3 \pmod 8$ but $\not\equiv 7 \pmod 8$. Thus $f \equiv 2a \pmod{16}$ for an odd a if and only if a is not of the form $8n+7$. Noting $f \equiv 0 \pmod 8$ implies $x \equiv y \equiv z \equiv 0 \pmod 2$, we see $f \equiv 8a \pmod{64}$ is solvable for every odd $a \not\equiv 7 \pmod 8$. So the process may be continued.

COROLLARY. *If* $\alpha\beta\gamma \equiv 1 \pmod 8$ *and* $\alpha+\beta \equiv 2$ *or* $4 \pmod 8$, $f=2\alpha x^2+2\beta y^2+\gamma z^2 \equiv a \pmod{8\mu_{a2}}$ *is solvable if and only if* a *is not of the form* $4^k(8n+7)$.

The proof is similar to that for the corollary to Lemma 10.

LEMMA 12. *For any* ∇, f *and its reciprocal form* F *are equivalent to a pair of forms* ϕ *and* Φ *satisfying the congruences*

$$\phi \equiv \alpha x^2 + \beta\Omega y^2 + \gamma\Omega\Delta z^2 \pmod\nabla,$$

$$\Phi \equiv \beta\gamma\Omega\Delta x^2 + \alpha\gamma\Delta y^2 + \alpha\beta z^2 \pmod\nabla,$$

$$\alpha\beta\gamma \equiv 1 \pmod\nabla,$$

except that ∇ *must be taken odd if* f *or* F *is improperly primitive.*

The proof is given by H. J. S. Smith in the article previously referred to, pages 461 and 462.

COROLLARY. *For any* ∇, $f=(\alpha, b, c, 2r, 2s, 2t)$, *with* α *prime to* ∇, *and its reciprocal form* F *are equivalent to a pair of forms* ϕ *and* Φ *above except that* ∇ *must be taken odd if* F *is improperly primitive.*

This follows from Smith's proof if we note α prime to ∇ implies ∇ odd if f is improperly primitive.

LEMMA 13. *For an improperly primitive form* f, *its reciprocal form* F, *and* ∇ *arbitrary (it may be taken even), there exist two forms*

$$f_2 \equiv \alpha x^2 + \beta\Omega y^2 + 4\gamma\Omega\Delta_1 z^2 \pmod\nabla,$$

$$F_2 \equiv \beta\gamma\Omega\Delta_1 x^2 + \alpha\gamma\Delta_1 y^2 + \alpha\beta z^2 \pmod\nabla,$$

where $\alpha\beta\gamma \equiv 1 \pmod\nabla$, $\alpha\beta\Omega \equiv 3 \pmod 4$, $\Delta_1=\Delta/2$, *the integers represented by* f *are the halves of the integers represented by* f_2 *with* $x \equiv y \pmod 2$, *i.e. the*

halves of the evens represented by f_2, and the integers represented by F are those represented by F_2 with $x \equiv y \pmod 2$.

Smith's proof of Lemma 13 carries through for this lemma to the middle of page 462, ibid., since f improperly primitive implies F is properly primitive and if $f=(a, a', a'', 2b, 2b', 2b'')$ we have $f \sim f_1 \equiv ax^2+2b''xy+a'y^2+\gamma\Omega\Delta z^2 \pmod{\nabla'}$, ∇' being $\nabla\Omega^2\Delta$. Now f_1 is equivalent to a similar form with $a \equiv 2 \pmod 4$, for if $a \equiv 0 \equiv a'+2 \pmod 4$ we interchange x and y, while if $a \equiv a' \equiv 0 \pmod 4$ the replacement of y by $x+y$ yields a form with leading coefficient double an odd, since b'' is odd. Similar reasoning shows we may consider $a/2$ to be prime to ∇' since f_1 is primitive. Thus let $a=2\alpha \equiv 2 \pmod 4$, $a'=2\alpha'$, and choose α_1 so that $\alpha\alpha_1 \equiv 1 \pmod{\nabla'}$. Then $2f \equiv \alpha(2x+b''\alpha_1 y)^2+\alpha(4\alpha'\alpha_1 - b''^2\alpha_1^2)y^2+2\gamma\Omega\Delta z^2 \pmod{2\nabla'}$. Now $4\alpha\alpha'-b''^2=\Omega A'' \equiv 3 \pmod 4$ where A'' is defined in Smith's paper. Set $\beta \equiv A''\alpha_1 \pmod{\nabla'}$ and

$$2f_1 \equiv \alpha(2x + b''\alpha_1 y)^2 + \beta\Omega y^2 + 2\gamma\Omega\Delta z^2 \qquad (\text{mod } \nabla'),$$

and double the integers represented by f_1 are the integers represented by f_2 with $x \equiv y \pmod 2$. Then $\alpha\beta\Omega \equiv 3 \pmod 4$ and $\alpha\beta\gamma \equiv 1 \pmod{\nabla}$. Now

$$\Omega F_1 \equiv 2\alpha'\gamma\Omega\Delta x^2 + 2\alpha\gamma\Omega\Delta y^2 + \Omega A''z^2 - 2\gamma\Omega\Delta b''xy \qquad (\text{mod } \nabla'),$$

$$F_1 \equiv \beta\gamma\Delta_1\Omega x^2 + \alpha\gamma\Delta_1(2y - b''\alpha_1 x)^2 + \alpha\beta z^2 \qquad (\text{mod } \nabla'/\Omega),$$

and the integers represented by F_1 are those integers represented by F_2 with $x \equiv y \pmod 2$.

LEMMA 14. *Every properly primitive form f for which $\Omega \equiv 2^{t_1} \pmod{2^{t_1+1}}$, $t_1 \geqq 1$, is equivalent to a form $f_1 \equiv ax^2+2^{t_1}by^2+2^{t_1}cz^2+2^{t_1+1}ryz \pmod{2^n}$ where n is arbitrary, a is odd and b is odd or double an odd according as F is properly or improperly primitive. In the latter case r is odd and c even.*

This is a corollary of Lemma 12 if F is properly primitive. f represents primitively an odd integer a. Transform f by an equivalent transformation so that a is the leading coefficient. Then replace x by $x+\tau y+\sigma z$, choosing τ and σ so the new coefficients of xy and xz are $\equiv 0 \pmod{2^n}$. We have $f \sim f_2 \equiv ax^2+b_1y^2+c_1z^2+2r_1yz \pmod{2^n}$ and $\Omega F_2 \equiv (b_1c_1-r_1^2)x^2+ac_1y^2+ab_1z^2 - 2r_1ayz \pmod{2^n}$. Thus $c_1 \equiv b_1 \equiv r_1 \equiv 0 \pmod{2^{t_1}}$. Now $b_1c_1-r_1^2 \equiv 0 \pmod{2^{2t_1}}$ implies that not all of b_1, c_1 and r_1 are $\equiv 0 \pmod{2^{t_1+1}}$. Furthermore, both of $b_1/2^{t_1}=b$ and $c_1/2^{t_1}=c$ are even if and only if F_2 is improperly primitive. In this case $r_1/2^{t_1}=r \equiv 1 \pmod 2$. If $b \equiv 2 \pmod 4$ the lemma is proved. If $c \equiv 2 \equiv b+2 \pmod 4$ interchange y and z to prove the lemma. If $b \equiv c \equiv 0 \pmod 4$ replace z by $y+z$ to prove the lemma.

LEMMA 15. *If $f \equiv ap^r(p^{r+1})$ is solvable, where a is prime to p, then, for n arbitrary, $f \equiv ap^r(p^n)$ is solvable ($r \geqq 0$).*

By Lemma 12 we may take $f \equiv \alpha_1 x^2 + \beta_1 y^2 + \gamma_1 z^2 \pmod{p^n}$. Let $\alpha_1\xi^2 + \beta_1\eta^2 + \gamma_1\zeta^2 = ap^r + kp^m$ where $m \geqq r+1$. We prove there exists a solution $x = \xi + X$, $y = \eta + Y$, $z = \zeta + Z$ of $f \equiv ap^r \pmod{p^{m+1}}$ if $m+1 \leqq n$. Not all of $\alpha_1\xi^2$, $\beta_1\eta^2$ and $\gamma_1\zeta^2$ are divisible by p^{r+1}. Permute $\alpha_1\xi^2$, $\beta_1\eta^2$ and $\gamma_1\zeta^2$ if necessary to take $\alpha_1\xi^2 \not\equiv 0 \pmod{p^{r+1}}$. Let $Y = Z = 0$ and $\alpha_1 = \alpha_2 p^t$, $\xi = \xi_1 p^s$ where $\alpha_2\xi_1$ is prime to p and $t + 2s \leqq r$. Take $X = p^{m-t-s}X_1$ and have

$$f(x, y, z) \equiv ap^r + p^m(k + 2\alpha_2\xi_1 X_1) + \alpha_2 p^{2m-2s-t}X_1^2 \equiv ap^r + p^m(k + 2\alpha_2\xi_1 X_1) \pmod{p^{m+1}}$$

and X_1 may be chosen so that $k + 2\alpha_2\xi_1 X_1 \equiv 0 \pmod{p}$. Thus, by induction, we prove the lemma.

LEMMA 16. *If $f \equiv 2^r a (2^{r+3})$ is solvable, where a is odd, then, for n arbitrary, $f \equiv 2^r a \pmod{2^n}$ is solvable.*

If f and F are both properly primitive we may by Lemma 12 consider $f \equiv \alpha_1 x^2 + \beta_1 y^2 + \gamma_1 z^2 \pmod{2^n}$ and proceed as above except that $m \geqq r+3$ and we take $X = 2^{m-t-s-1}X_1$.

If f is improperly primitive we have, by Lemma 13, a form $f_2 \equiv \alpha_1 x^2 + \beta_1 y^2 + 4\gamma_1 z^2 \pmod{2^{n+1}}$, $\alpha_1\beta_1 \equiv 3 \pmod 4$ such that the evens represented by f_2 are twice the integers represented by f. The primitive contravariant of f_2 is properly primitive and thus the reasoning of the first paragraph of this proof applies to prove $f_2 \equiv 2^{r+1}a \pmod{2^n}$ and therefore $f \equiv 2^r a \pmod{2^n}$ is solvable.

It remains to consider f properly primitive and F improperly primitive. By Lemma 14, we may consider $f \equiv \alpha x^2 + 2^{t+2}\beta y^2 + 2^{t+2}\gamma z^2 + 2^{t+2}\rho yz \pmod{2^n}$ where $\Omega \equiv 2^{t+1}(2^{t+2})$, $\beta\rho\alpha \equiv 1 \pmod 2$ and $t \geqq -1$. Choose β_1 so that $\beta\beta_1 \equiv 1 \pmod{2^n}$.

First, if $t \geqq 0$, $f_1 \equiv \alpha x^2 + 2^t\beta w^2 + 2^t\beta_1\delta z^2 \pmod{2^n}$ where $w = 2y + \rho\beta_1 z$, $4\beta\gamma - \rho^2 = \delta$ and the integers represented by f are those integers represented by f_1 with $w \equiv z \pmod 2$. We have $f_1(\xi, \omega, \zeta) = 2^r a + 2^m k$, $m \geqq r+3$ and $\omega \equiv \zeta \pmod 2$. Let $\xi = 2^\nu\xi_1$, $\omega = 2^\sigma\omega_1$, $\zeta = 2^\mu\zeta_1$ where $\xi_1\omega_1\zeta_1 \equiv 1 \pmod 2$, ν, σ and $\mu \geqq 0$. Note that not all of 2ν, $2\sigma + t$, $2\mu + t$ are $> r$ and $\alpha\beta\beta_1\delta \equiv 1 \pmod 2$. If $2\nu \leqq r$ take $x = \xi + 2^{m-\nu-1}X$, $w = \omega$, $z = \zeta$ and $f_1(x, w, z) = f_1(\xi, \omega, \zeta) + \alpha(2^{m-\nu}\xi X + 2^{2m-2\nu-2}X^2) \equiv 2^r a + 2^m(k + \alpha\xi_1 X) \pmod{2^{m+1}}$, since $2m - 2\nu - 2 \geqq m+1$ and X may be chosen so that $f_1(x, w, z) \equiv f(x, y, z) \equiv 2^r a \pmod{2^{m+1}}$. If $2\nu > r$ and $2\sigma + t \leqq r$ take $x = \xi$, $z = \zeta$, $w = \omega + 2^{m-t-\sigma-1}W \equiv \omega \pmod 2$ and $f_1(x, w, z) \equiv 2^r a + 2^m(k + \beta\omega_1 W) \pmod{2^{m+1}}$ and W may be chosen so that $f_1(x, w, z) \equiv f(x, y, z) \equiv 2^r a \pmod{2^{m+1}}$. Proceed similarly if $2\nu > r$, $2\sigma + t > r$ and $2\mu + t \leqq r$.

Second, if $t = -1$, $f \equiv \alpha x^2 + 2\beta y^2 + 2\gamma z^2 + 2\rho yz \pmod{2^n}$ and $f_2 = 2f \equiv 2\alpha x^2 + \beta w^2 + \beta_1\delta z^2 \pmod{2^{n+1}}$ where w and δ have the same values as for $t \geqq 0$,

$\beta\beta_1\delta \equiv 3 \pmod 4$ and the evens represented by f_2 are twice the integers represented by f. The proof proceeds in a manner similar to that above.

LEMMA 17. *$f \equiv a \pmod{8h\mu}$ implies $f \equiv a \pmod N$ is solvable for N arbitrary, where h is the product of the first powers of the odd prime divisors of H and μ is the least integer for which a/μ is an integer prime to $2H$.*

Let p_i be the odd prime factors common to h and N, and r_i their respective multiplicities in N. Then, by Lemma 15, there exist solutions (x_i, y_i, z_i) of $f \equiv a \pmod{p_i^{r_i}}$. Also, by Lemma 16, there exists a solution (x_0, y_0, z_0) of $f \equiv a \pmod{2^s}$ where $N \equiv 2^s \pmod{2^{s+1}}$. Let p_i' be the odd prime factors of N which are prime to h and s_i their respective multiplicities in N. By Lemma 12 we may take $f \equiv \alpha x^2 + \beta\Omega y^2 + \gamma\Omega\Delta z^2 \pmod{p_i'^{s_i}}$, where $\alpha\beta\gamma\Delta\Omega^2$ is prime to $p_i'^{s_i}$. Thus, by Corollary 2 of Lemma 2 and Lemma 15, there exist solutions x_i', y_i', z_i' of $f \equiv a \pmod{p_i'^{s_i}}$. There exists, by the Chinese Remainder Theorem, an x, y and z such that $x \equiv x_i$, $y \equiv y_i$, $z \equiv z_i \pmod{p_i}$, $x \equiv x_0$, $y \equiv y_0$, $z \equiv z_0 \pmod{2^s}$ and $x \equiv x_i'$, $y \equiv y_i'$, $z \equiv z_i' \pmod{p_i'^{s_i}}$. Such an (x, y, z) is a solution of $f \equiv a \pmod N$.

4. THEOREM. *With every ternary quadratic form of Hessian H there is associated a set of arithmetic progressions:*

$$2^r(8n + a_i')p^{r_i}(p_i n + a_{ij}) \qquad (n = 0, \pm 1, \pm 2, \cdots) \tag{1}$$

such that no integer falling in any one of them is represented by f, and for every integer a not falling in any of (1) *it is true that $f \equiv a \pmod{8h\mu}$, and therefore* (mod N) *for N arbitrary, is solvable, where p_i are odd prime factors of H, a_{ij} are some or all the members of a complete residue system* mod p_i, *r and r_i range over some or all of the positive integers and zero, a_i' are some, none or all of* 1, 3, 5 *and* 7, *h is the product of the first powers of the odd prime factors of H and μ is the smallest positive integer for which a/μ is an integer prime to $2h$.*

The Hessian H and the progressions (1) *serve to define the genus* and to determine the order and invariants Ω and Δ of the form: i.e., all forms of the same Hessian and having the same progressions (1) associated with them are of the same genus and order and have the same invariants Ω and Δ and, conversely, all forms of the same genus and order and having the same Hessian, Ω and Δ, have the same progressions (1). The forms of (1) are more precisely given below in the course of the proof.

I. We first prove, for a given form f, the existence of certain progressions (1) having the desired properties and which, together with H, determine by their nature the invariants Δ and Ω and whether F and f are properly or improperly primitive.

For an odd prime factor p of H we use Lemma 12 to see that we may take $f \equiv \alpha x^2+\beta\Omega y^2+\gamma\Omega\Delta z^2 \pmod{p^t}$ where t is the highest power of p in H. We shall use the following abbreviations: fNa denotes: f represents no integer of the form a; fCa denotes: for every integer of the form a, $f \equiv a \pmod{p\mu_{ap}}$ is solvable. The above congruential form of f shows, using Lemma 1,

$$fC(pn+a), \text{ i.e. } FCp^{2k}(pn+a);\ a \text{ prime to } p \text{ if } \Omega \not\equiv 0 \pmod{p},$$

$$fN(pn+\alpha_{-1}),\ fC(pn+\alpha_1),\ fCp^{2k}(pn+\alpha_1), \text{ where}$$

$$(\alpha_{-1}\,|\,p) = -(\alpha\,|\,p) \text{ and } (\alpha_1\,|\,p) = (\alpha\,|\,p), \text{ if } \Omega \equiv 0 \pmod{p}.$$

In the latter case to find the power to which p occurs in Ω, we note $f \equiv 0 \pmod{p}$ implies $x = px_1$ and $f/p = p\alpha x_1^2+\beta y^2\Omega/p+\gamma\Delta z^2\Omega/p \pmod{p^{t-1}}$ which represents an integer prime to p if and only if $\Omega \not\equiv 0 \pmod{p^2}$. If $\Omega \equiv 0 \pmod{p^2}$, $f/p^2 \equiv \alpha x_1^2+\beta y^2\Omega/p^2+\gamma\Delta z^2\Omega/p^2 \pmod{p^{t-2}}$, and $f/p^2 \equiv \alpha_{-1} \pmod{p}$ if and only if $\Omega \not\equiv 0 \pmod{p^3}$. So continuing we have, taking t_1 to be the highest power of p in Ω,

$$fN(p^{2r+1}a), \qquad r = 0, 1, \cdots, [(t_1-2)/2];$$

$$fNp^{2s}(pn+\alpha_{-1}), \qquad s = 0, 1, \cdots, [(t_1-1)/2];$$

$$fC(\beta\Omega) \text{ and, if } t_1 \text{ is even, } fCp^{t_1}(pn+\alpha_{-1}).$$

This shows the existence of certain progressions (1). Then, given these progressions, we can determine t_1 as follows: find the least odd power $2r_1+1$ of p such that for some integer b prime to p, $p^{2r_1+1}b$ does not occur in (1) and the least even power $2s_1$ of p for which $p^{2s_1}(pn+\alpha_{-1})$ does not occur in (1). Either $2r_1+1$ or $2s_1$ or both are finite, for if t_1 is odd, $fC(\beta\Omega)$ and $\beta\Omega/p^{t_1}$ is an integer prime to p. t_1 is the lesser of $2r_1+1$ and $2s_1$ for $fCp^{t_1}(\beta\Omega/p^{t_1})$ if t_1 is odd.

To determine the greatest power t_1 of 2 occurring in Ω as a factor if f is properly primitive, we use Lemma 14 and consider $f \equiv ax^2+2^{t_1}by^2+2^{t_1}cz^2+2^{t_1+1}ryz \pmod{2^{3+t}}$. If $t_1 \geqq 2$, $f \equiv 0 \pmod 2$ implies $x = 2x_1$ and $f/4 \equiv ax_1^2+2^{t_1-2}by^2+2^{t_1-2}cz^2+2^{t_1-1}ryz \pmod{2^{1+t}}$. So proceeding we have

$$\text{for } t_1 \text{ even}, \quad f/2^{t_1-4} \equiv ax^2+16by^2+16cz^2+32ryz \pmod{128} \text{ if } t_1 \geqq 4,$$

$$f/2^{t_1-2} \equiv ax^2+4by^2+4cz^2+8ryz \pmod{32} \text{ if } t_1 \geqq 2,$$

$$f/2^{t_1} \equiv ax^2+by^2+cz^2+2ryz \pmod{8};$$

$$\text{for } t_1 \text{ odd}, \quad f/2^{t_1-3} \equiv ax^2+8by^2+8cz^2+16ryz \pmod{64} \text{ if } t_1 \geqq 3,$$

$$f/2^{t_1-1} \equiv ax^2+2by^2+2cz^2+4ryz \pmod{16} \text{ if } t_1 \geqq 1.$$

Let s_1 be the least value of s for which $f \equiv 4^s(a+4) \pmod{8 \cdot 4^s}$ is solvable and s_2 the least value of s for which $f \equiv 4^s(a+2) \pmod{8 \cdot 4^s}$ is solvable for some integer a represented by f. Inspection of the above, taking into account the conditions of Lemma 14, gives the following table:

t_1 even, F p.p.	t_1 even, F i.p.	t_1 odd, F p.p.	t_1 odd, F i.p.
$2s_1 = t_1 - 2$ or $t_1 = 2s_1 = 0$	$\geqq t_1$	$\geqq t_1 - 1$	$= t_1 - 1$
$2s_2 \geqq t_1$	$= t_1$	$= t_1 - 1$	$> t_1 - 1$

p.p. and i.p. are abbreviations of "properly primitive" and "improperly primitive" respectively.

The above table shows the existence of certain progressions (1). Given the progressions we note that F can be improperly primitive only if Δ is odd, i.e. only if t (the highest power of 2 in H) is even and $t_1 = t/2$. The numbers $2s_1$ and $2s_2$ can be found from progressions (1).

If $0 \neq 2s_1 \geqq 2s_2$ we have only the second and third columns of the table to consider and see that $2s_2 = t_1$ or $t_1 - 1$. If $t = 4s_2$ then $t_1 = 2s_2$ and F is improperly primitive, for if $2s_2 = t_1 - 1$, $4s_2 = 2t_1 - 2 < t$. If $t \neq 4s_2$, F is properly primitive and $t_1 - 1 = 2s_2$.

If $0 \neq 2s_1 < 2s_2$, we see from the first and fourth columns that $2s_1 = t_1 - 2$ or $t_1 - 1$. If $t = 4s_1 + 2$ then $t_1 = 2s_1 + 1$ and F is improperly primitive, for $t_1 - 2 = 2s_1$ implies $4s_1 + 2 = 2t_1 - 2 < t$. If $t \neq 4s_1 + 2$, F is properly primitive and $2s_1 = t_1 - 2$.

If $2s_1 = 0$ note that $H \not\equiv 0 \pmod 4$ implies $t_1 = 0$. We consider below only $H \equiv 0 \pmod 4$.

If $2s_1 = 0 = 2s_2$ and $H \equiv 0 \pmod 4$ we have to consider the first and third columns, for, if the second held, $0 = t_1$, $H \equiv 0 \pmod 2$ and F would be improperly primitive, which is impossible. Thus F is properly primitive, $0 = t_1, t_1 - 1$, or $t_1 - 2$ and, using Lemma 12, we may take $f \equiv \alpha x^2 + \beta \Omega y^2 + \gamma \Omega \Delta z^2 \pmod 8$ and note that $t_1 = 0$ and $H \equiv 0 \pmod 4$ implies $\Delta \equiv 0 \pmod 4$. Inspection of the three cases gives the following table:

t_1	Progressions (1) contain
0	$4n+2$ or $4n+3\nu$ but not both
1	neither $4n+2$ nor $4n+3\nu$
2	$4n+2$ and $4n+3\nu$

where ν is an integer such that $f \equiv \nu \pmod 4$ is solvable. Thus the value of t_1 may be determined from the form of progressions (1).

If $2s_1=0<2s_2$ and $H\equiv 0 \pmod 4$ we have to consider the first and fourth columns and see that $t_1=0$ or 2 and F is properly primitive or $t_1=1$ and F is improperly primitive. If $t_1=2$, $H\equiv 0 \pmod{16}$ while, if $t_1=1$ and F is improperly primitive, Δ is odd and thus $H\equiv 4 \pmod 8$. We have the following table:

t_1	F	H	Progressions (1) contain
0	p.p.	$\equiv 0 \pmod 4$	$4n+2$ or $4n+3\nu$ but not both
2	p.p.	$\equiv 0 \pmod{16}$	$4n+2$ and $4n+3\nu$
1	i.p.	$\equiv 4 \pmod 8$	$4n+2$ and $4n+3\nu$

where ν is an integer such that $f\equiv\nu \pmod 4$ is solvable. Thus, in this case, the value of t_1 and whether F is properly or improperly primitive may be determined from H and the progressions (1).

f is improperly primitive if and only if $2n+1$ occurs in progressions (1). Here $t_1=0$.

Thus progressions (1) determine not only t_1, the highest power of 2 contained in Ω, but whether F and f are properly or improperly primitive.

II. After Ω and Δ have been determined by the above process we must exhibit the progressions (1) and show that the genus is determined by them. Since, for any odd prime factor p of H, the progressions (1) determine the quadratic character with respect to p of the integers represented by the form, it remains to show that the progressions (1) involving a particular p determine the quadratic character with respect to p of the integers represented by F. We exhibit the progressions (1) and show their relation to the character of the integers represented by F.

Consider f to be of the form of ϕ in Lemma 12 with $\nabla=p^{t+1}$ where t is the highest power of p in H. For any α we use α_{-1} to denote any α_{-1} for which $(\alpha_{-1}\,|\,p)=-(\alpha\,|\,p)$ and a is any integer prime to p.

A. If p is prime to Ω, it must divide Δ. Then from the form of f and Lemma 1 we see $f\equiv a \pmod p$ is solvable for every a prime to p and therefore $f\equiv ap^{2r} \pmod{p^{2r+1}}$ is solvable. Let $\Delta/p^t=\Delta'\not\equiv 0 \pmod p$. First if $(-\alpha\beta\Omega\,|\,p)=1$ the first row in the table below results from Lemma 4 and $(F\,|\,p)=(\alpha\beta\,|\,p)$. Second, if $(-\alpha\beta\Omega\,|\,p)=-1$ we see from Lemma 3 that $f\equiv 0 \pmod p$ implies $x=px_1$, $y=py_1$ and $f/p\equiv\alpha px_1^2+\beta py_1^2+\gamma\Omega\Delta z^2/p \pmod{p^t}$, which represents integers prime to p if and only if $\Delta\not\equiv 0 \pmod{p^2}$ when we use Lemma 5. If, on the other hand, $\Delta\equiv 0 \pmod{p^2}$ we have $f/p^2\equiv\alpha x_1^2+\beta\Omega y_1^2+\gamma\Omega\Delta z^2/p^2 \pmod{p^{t-1}}$ and $f/p^2\equiv pa \pmod{p^2}$ is solvable for every a prime to p if and only if $\Delta\not\equiv 0 \pmod{p^3}$ from Corollary 1 of Lemma 2. This process may be repeated until we have the results below:

$(-\alpha\beta\Omega\,\vert\,p)$	Progressions (1) involving p	$(F\,\vert\,p)$
1	none	$(-\Omega\,\vert\,p)$
-1	$p^{2r+1}a$, $r=0, 1, \cdots, [(t-2)/2]$ if $t\geqq 2$ and, if t is odd, $p^{2k+1}(pn+\alpha_1)$	$-(-\Omega\,\vert\,p)$

where $(\alpha_1\,\vert\,p)=-(\gamma\Omega\Delta'\,\vert\,p)=-(\alpha\beta\Omega\Delta'\,\vert\,p)=(-\Delta'\,\vert\,p)$ and a is prime to p. The character of the progressions thus determines $(F\,\vert\,p)$.

B. If $\Omega\equiv 0 \pmod{p^{t_1}}$, $t_1>0$ and $\Omega/p^{t_1}=\Omega'\not\equiv 0 \pmod p$, we have $\Delta\equiv 0 \pmod{p^{t-2t_1}}$ and $\Delta/p^{t-2t_1}=\Delta'\not\equiv 0 \pmod p$ where $t-2t_1\geqq 0$. Now $f\equiv 0 \pmod p$ implies $x=px_1$ and $f/p\equiv p\alpha x_1^2+\beta y^2\Omega/p+\gamma\Delta z^2\Omega/p \pmod{p^t}$ and f/p represents integers prime to p if and only if $\Omega\not\equiv 0 \pmod{p^2}$. If $\Omega\equiv 0 \pmod{p^2}$, $f/p^2\equiv\alpha x_1^2+\beta\Omega y^2/p^2+\gamma\Delta z^2\Omega/p^2 \pmod{p^{t-1}}$. So continuing we have

$$\text{if } t_1 \text{ is even, } f/p^{t_1}\equiv \alpha x'^2+\beta\Omega' y^2+\gamma\Omega'\Delta z^2 \pmod{p^{t-t_1}},$$

and

$$\text{if } t_1 \text{ is odd, } f/p^{t_1}\equiv p\alpha x'^2+\beta\Omega' y^2+\gamma\Omega'\Delta z^2 \pmod{p^{t-t_1}}.$$

First, if $t=2t_1$, $(F\,\vert\,p)=\pm 1$ and the progressions (1) are $p^{2r}(pn+\alpha_{-1})$, $p^{2s+1}a$, where the second progression occurs only if $t_1>1$, where $s=0, 1, \cdots, [(t_1-2)/2]$ and, if t_1 is odd and $(-\beta\gamma\Delta\,\vert\,p)=(-\alpha\Delta\,\vert\,p)=-1$, $r=0, 1, 2, \cdots$. Otherwise $r=0, 1, 2, \cdots, [(t_1-1)/2]$.

Second, if $t>2t_1$ set $t_2=t-2t_1>0$. Note that, if t_1 is even and $(-\alpha\beta\Omega'\,\vert\,p)=-1$, it is true that $f/p^{t_1}\equiv 0 \pmod p$ implies $x'=px_2$, $y=py_2$ and $f/p^{t_1+1}\equiv p\alpha x_2^2+\beta\Omega' py_2^2+\gamma\Delta\Omega' z^2/p \pmod{p^{t-t_1-1}}$. Also if t_1 is odd, $f/p^{t_1}\equiv 0 \pmod p$ implies $y=py_1$ and $f/p^{t_1+1}\equiv\alpha x'^2+\beta\Omega' py_1^2+\gamma\Omega'\Delta z^2/p \pmod{p^{t-t_1-1}}$. So continuing we have

If t_1 is even

$(-\alpha\beta\Omega'\,\vert\,p)$	Progressions (1) involving p	$(F\,\vert\,p)$
1	$p^{2r}(pn+\alpha_{-1})$, $p^{2s+1}a$, $s=0, 1, \cdots, t_1/2-1$	$(-\Omega'\,\vert\,p)$
-1	$p^{2r}(pn+\alpha_{-1})$, $p^{2s+1}a$, and if t_2 is odd, $p^{2k+1}(pn+\alpha_1)$	$-(-\Omega'\,\vert\,p)$

where in the second row $s=0, 1, \cdots, [(t-t_1-2)/2]$ and $(\alpha_1\,\vert\,p)=-(\gamma\Omega'\Delta')=(-\Delta'\,\vert\,p)$. In both cases $r=0, 1, \cdots, t_1/2-1$. It should be noted that the progressions in the first and second rows are not the same even if t_2 is even for $t_1/2-1\neq(t-t_1-2)/2$.

If t_1 is odd

Conditions	Progressions (1) involving p	$(F\,\vert\,p)$
t_2 even, $(-\alpha\Delta'\,\vert\,p)=1$	$p^{2r}(pn+\alpha_{-1})$, $p^{2s+1}a$, $p^{2s_1+1}(pn+\alpha_1)$	$-(-\alpha_1\Delta'\Omega'\,\vert\,p)$
t_2 even, $(-\alpha\Delta'\,\vert\,p)=-1$	$p^{2k}(pn+\alpha_{-1})$, $p^{2s+1}a$, $p^{2s_1+1}(pn+\alpha_1)$	$(-\alpha_1\Delta'\Omega'\,\vert\,p)$
t_2 odd, $(-\alpha_1\Delta'\,\vert\,p)=1$	$p^{2r}(pn+\alpha_{-1})$, $p^{2s+1}a$, $p^{2k+1}(pn+\alpha_1)$	$-(-\alpha\Delta'\Omega'\,\vert\,p)$
t_2 odd, $(-\alpha_1\Delta'\,\vert\,p)=-1$	$p^{2r}(pn+\alpha_{-1})$, $p^{2s+1}a$, $p^{2s_1+1}(pn+\alpha_1)$	$(-\alpha\Delta'\Omega'\,\vert\,p)$

where $r=0, 1, \cdots, [(t-t_1-1)/2]$, $s_1=0, 1, \cdots, [(t-t_1-2)/2]$ and $s=0, 1, \cdots, (t_1-3)/2$, the progressions in s being excluded unless $t_1 \geqq 3$, $-(\alpha_1 | p)=(\beta\Omega' | p)=(\alpha\gamma\Omega' | p)=(\alpha F\Omega' | p)$, $(F | p)$ is determined from the progressions by the above tables.

III. We find completely the progressions (1) involving 2 and show that H, Δ, Ω, together with the progressions (1), determine the complete generic character of f.

If f and F are properly primitive we use Lemma 12 and have

$$\Delta' f \equiv \alpha\Delta' x^2 + \beta\Delta'\Omega y^2 + \gamma\Omega\Delta'' z^2 \pmod{8\Omega''\Delta''},$$

$$\Omega' F \equiv \beta\gamma\Delta\Omega'' x^2 + \alpha\gamma\Delta\Omega' y^2 + \alpha\beta\Omega' z^2 \pmod{8\Delta''},$$

where $\alpha\beta\gamma \equiv 1 \pmod{8\Delta''}$, $\Omega=\Omega'\Omega''$, $\Delta=\Delta'\Delta''$, Δ'' and Ω'' being the greatest powers of 2 dividing Δ and Ω respectively. Let $\alpha'=\alpha\Delta'$, $\beta'=\beta\Delta'\Omega'$, and $\gamma'=\gamma\Omega'$ and then replace α', β', γ' by α, β, γ respectively to get

$$\Delta' f \equiv \alpha x^2 + \beta\Omega'' y^2 + \gamma\Omega''\Delta'' z^2 \pmod{8\Omega''\Delta''},$$

$$\Omega' F \equiv \alpha\Delta''\Omega'' x^2 + \beta\Delta'' y^2 + \gamma z^2, \quad \alpha\beta\gamma \equiv 1 \pmod{8}.$$

A. If $\Omega \not\equiv 0 \not\equiv \Delta \pmod 4$, and both f and F are properly primitive, the generic character involves a symbol Ψ defined in Smith's article. In his paper the generic character is given for the four cases in terms of this Ψ.

If H is odd we use Lemma 9 and referring to Smith's discussion, pages 465, 466, we have the following table:

Progressions (1) involving 2	Ψ
None	$+1$
$4^k(8n+7\Delta')$	-1

If $\Omega''=2$, $\Delta''=1$, we abbreviate Smith's notation $(-1)^{(f^2-1)/8}$ to read $(2 | f)$, etc., and see from his case ii, page 466, that $f \not\equiv 3\Delta' \pmod 8$ implies $(2 | f)\Psi=(2 | \Delta)$ and $f \not\equiv 7\Delta' \pmod 8$ implies $(2 | f)\Psi=-(2 | \Delta)$. Thus, using the corollaries to Lemmas 10 and 11, we have the following table:

$\beta+\gamma \equiv \pmod 8$	Progressions (1) involving 2	Character
6 or 0	$8n+3\Delta'$	$(2 | f)\Psi=(2 | \Delta)$
4 or 2	$4^k(8n+7\Delta')$	$(2 | f)\Psi=-(2 | \Delta)$

If $\Omega'=1$, $\Delta''=2$, we have similarly

$\alpha+\beta\equiv$ (mod 8)	Progressions (1) involving 2	Character
6 or 0	None	$(2\,\|F)\Psi=(2\,\|\,\Omega)$
4 or 2	$4^k(16n+14\Delta')$	$(2\,\|F)\Psi=-(2\,\|\,\Omega)$

for if $\alpha+\beta\equiv 0$ or 6 (mod 8), ΩF represents no $8n+3$ and if $\alpha+\beta\equiv 2$ or 4 (mod 8), $\Omega F\not\equiv 7$ (mod 8).

If $\Delta''=\Omega''=2$ we note case iv in Smith's article on pages 465 and 467 and that $\Delta' f\equiv 0$ (mod 2) implies $x=2x_1$. We have the following:

$\alpha+\gamma\equiv$ (mod 8)	Progressions (1) involving 2	$(2\,\|f)(2\,\|F)(2\,\|\Delta')(2\,\|\,\Omega')\Psi$
0 or 6	$16n+6\Delta'$	$+1$
2 or 4	$4^k(16n+14\Delta')$	-1

This may be deduced as follows: $(2\,|f)(2\,|F)(2\,|\Delta')(2\,|\,\Omega')\Psi=(2\,|f\Delta')(2\,|F\Omega')\Psi$ $=(-1)^\nu$, referring to page 465 of Smith's article, where $\nu=(\Delta'^2m^2+\Omega'^2M^2+2\Omega'M+2\Delta'm+2\Delta'm\Omega'M)/8=\{(\Delta'm+\Omega'M+1)^2-1\}/8$. Then, taking for $\Delta'm$ and $\Omega'M$ the first pair of values given on page 465: α, γ, we have $\nu\equiv\{(\alpha+\gamma+1)^2-1\}/8$ (mod 2).

B. If $\Omega''=1$ and $\Delta\equiv 0$ (mod 4) with f properly primitive, using the lemmas and the forms given at the beginning of section III for $\Delta' f$ and $\Omega' F$, we obtain the following table:

Δ''	$\alpha+\beta\equiv$ (mod 8)	Progressions (1) involving 2	$\Omega' F\equiv$ (mod 8) only
4	0 or 4	$4n+2$	3, 7
4	2 or 6	$4n+3\alpha\Delta'$ and, if $\alpha\equiv 1$ (mod 4), $4^k(8n+7\Delta')$	1, 5
8	0	$4n+2$	7
8	2	$4n+3\alpha\Delta'$, $8n+6\Delta'$, $4^k(16n+14\Delta')$	$2\alpha-1$
8	4	$4n+2$, $4^k(16n+14\Delta')$	3
8	6	$4n+3\alpha\Delta'$, $8n+2\Delta'$	$6\alpha-1$
$8\cdot 4^\tau$, $\tau>0$	0	$4n+2$	7
$8\cdot 4^\tau$, $\tau>0$	2, 4, or 6	4^τ times the values given above for $\Delta''=8$ where $\tau=0, 1, \cdots, \tau$	see $\Delta''=8$

If $\Delta''=4\cdot 4^{\tau}$, $\tau>0$, we have the following table:

$\alpha\beta\equiv$ (mod 8)	Progressions (1) involving 2	$\Omega'F\equiv$ (mod 8) only
7	$4n+2$	7
5	$4^{r}(4n+3\alpha\Delta')$, $4^{s}(8n+2\alpha\Delta')$ and, if $\alpha\equiv 1$ (mod 4), $4^{k}(8n+7\Delta')$	5
3	$4^{r}(4n+2)$	3
1	$4^{r}(4n+3\alpha\Delta')$, $4^{s}(8n+6\alpha\Delta')$ and, if $\alpha\equiv 1$ (mod 4), $4^{k}(8n+7\Delta')$	1

where $r=0, 1, \cdots, \tau$ and $s=0, 1, \cdots, \tau-1$.

C. If $\Omega''=2$ and $\Delta\equiv 0$ (mod 4), f and F are properly primitive. In the first line of the table note that $\alpha\equiv\beta$ (mod 4) and $\alpha\equiv 1$ or 3 (mod 8) implies that $\beta+\gamma\equiv 2$ or 4 (mod 8) to find the progressions (1). A similar situation exists for the rest of the table. If $\Delta''=4$, we have the table following:

Conditions on α and β	Progressions (1) involving 2	$\Omega'F\equiv$ (mod 8) only
$\alpha\equiv\beta$ (mod 4), $\alpha\equiv 1$ or 3 (mod 8)	$8n+5\Delta'$, $4^{k}(8n+7\Delta')$	1, 5
$\alpha\equiv\beta$ (mod 4), $\alpha\equiv 5$ or 7 (mod 8)	$8n+\Delta'$, $8n+3\Delta'$, $4(8n+3\Delta')$	1, 5
$\alpha\equiv 3\beta$ (mod 4), $\alpha\equiv 3$ or 5 (mod 8)	$8n+\Delta'$, $4^{k}(8n+7\Delta')$	3, 7
$\alpha\equiv 3\beta$ (mod 4), $\alpha\equiv 1$ or 7 (mod 8)	$8n+3\Delta'$, $8n+5\Delta'$, $4(8n+3\Delta')$	3, 7

Thus if $f\not\equiv\nu$ or 3ν (mod 8) for some odd ν, only $\Omega'F\equiv 1$ or 5 (mod 8) is solvable, while $f\not\equiv\nu$ or 7ν (mod 8) implies that only $\Omega'F\equiv 3$ or 7 (mod 8) is solvable.

If $\Delta''=8$, the multiples of 4 in progressions (1) are 4 multiplied by the progressions (1) given under the heading $\Omega''=2=\Delta''$. The remainder of the progressions are given below:

$\alpha\beta\equiv$ (mod 8)	Progressions (1) $\not\equiv 0$ (mod 4) but involving 2	$\Omega'F\equiv$ (mod 8) only
1	$2^{r}(8n+5\alpha\Delta')$, $2^{r}(8n+7\alpha\Delta')$, $r=0, 1$	1
3	$8n+5\alpha\Delta'$, $8n+3\alpha\Delta'$, $16n+2\alpha\Delta'$, $16n+14\alpha\Delta'$	3
5	$8n+5\alpha\Delta'$, $8n+7\alpha\Delta'$, $16n+2\alpha\Delta'$, $16n+6\alpha\Delta'$	5
7	$2^{r}(8n+3\alpha\Delta')$, $2^{r}(8n+5\alpha\Delta')$, $r=0, 1$	7

Thus the third column is related to the second.

If

$$\Delta'' \equiv 0 \pmod{16}$$

the progressions (1) which are $\not\equiv 0 \pmod 4$ and the corresponding character of $\Omega' F$ are given by the table above for $\Delta'' = 8$. If

$$\Delta = 4 \cdot 4^{\tau}, \quad \tau \geqq 1,$$

the progressions (1) involving 2 and divisible by 4 are 4^s multipled by the odd progressions given in the table above for $\Delta'' = 8$, 4^{s_1} multiplied by the progressions $\equiv 2 \pmod 4$ for $\Delta'' = 8$, and 4^{τ} multiplied by the progressions for $\Delta'' = 4$ where $s = 1, 2, \cdots, \tau$, and if $\tau > 1$, $s_1 = 1, 2, \cdots, \tau - 1$. If

$$\Delta'' = 8 \cdot 4^{\tau},$$

the progressions (1) divisible by 4 are those given above for $\Delta'' = 8$ multiplied by 4^s, $s = 1, 2, \cdots, \tau$, together with those for $\Omega'' = \Delta'' = 2$ multiplied by $4^{\tau+1}$.

D. $\Delta'' = 1$, $\Omega \equiv 0 \pmod 4$ and F properly primitive. If $\Omega'' = 4$, we have

$\alpha \equiv \pmod 4$	Progressions (1) involving 2	$\Omega' F \equiv \pmod 8$ only
1	$4n+2, 4n+3\Delta'$ and, if $\beta \equiv \gamma \equiv 1 \pmod 4$, $4^k(8n+7\Delta')$	$\beta, 5\beta$
3	$4n+2, 4n+\Delta'$	1, 3, 5 or 7

If $\Omega'' = 8$ we have the following table:

$\beta+\gamma \equiv \pmod 8$	Progressions (1) involving 2	$\Omega' F \equiv \pmod 8$ only
6	$4n+2, 4n+3\Delta', 8n+5\alpha\Delta', 4(8n+3\Delta')$	$-(2 \mid \alpha), -5(2 \mid \alpha)$
2	$4n+2, 4n+3\Delta', 8n+5\alpha\Delta', 4^k(8n+7\Delta')$	$(2 \mid \alpha), 5(2 \mid \alpha)$
4	$4n+2, 4n+\Delta', 4^k(8n+7\Delta')$	1, 3, 5 or 7
0	$4n+2, 4n+\Delta', 4^r(8n+3\Delta'), r = 0, 1$	1, 3, 5 or 7

If $\Omega'' = 4 \cdot 4^{\tau}$, $\tau \geqq 1$, the progressions (1) involving 2 are the above for $\Omega'' = 4$ multiplied by 4^r, where $r = 0, 1, \cdots, \tau$, and $4^s(8n+5\alpha\Delta')$, where $s = 0, 1, \cdots, \tau - 1$. The character of $\Omega' F$ is determined as for $\Omega'' = 4$.

If $\Omega'' = 8 \cdot 4^{\tau}$ the progressions (1) are the above for $\Omega'' = 8$ multiplied by 4^r where $r = 0, 1, \cdots, \tau$, and the character of $\Omega' F$ is determined as for $\Omega'' = 8$.

E. $\Delta'' = 2$ and $\Omega \equiv 0 \pmod 4$. We have the following table:

Ω''	$\alpha \equiv \pmod 8$	$\alpha \equiv \pmod 4$	Progressions (1) involving 2	$\Omega' F \equiv \pmod 8$ only
4	$6-\beta$ or $-\beta$	1	$4n+3\Delta', 4n+2$	5, 7
4	$6-\beta$ or $-\beta$	3	$4n+\Delta', 4n+2$	1, 7
4	$2-\beta$ or $4-\beta$	1	$4n+3\Delta', 4n+2, 4^k(16n+14\Delta')$	1, 3
4	$2-\beta$ or $4-\beta$	3	$4n+\Delta', 4n+2, 4^k(16n+14\Delta')$	3, 5
8	$6-\gamma$ or $-\gamma$	1	$4n+3\Delta', 4n+2, 8n+5\alpha\Delta', 4(16n+6\Delta')$	5α, 7α
8	$6-\gamma$ or $-\gamma$	3	$4n+\Delta', 4n+2, 8n+5\alpha\Delta', 4(16n+6\Delta')$	α, 7α
8	$2-\gamma$ or $4-\gamma$	1	$4n+3\Delta', 4n+2, 8n+5\alpha\Delta', 4^k(16n+14\Delta')$	α, 3α
8	$2-\gamma$ or $4-\gamma$	3	$4n+\Delta', 4n+2, 8n+5\alpha\Delta', 4^k(16n+14\Delta')$	3α, 5α

If $\Omega \equiv 0 \pmod{16}$ the same discussion applies as for case D.

F. If $\Delta'' = 2^{t_2}$, $\Omega'' = 2^{t_1}$, $t_1 \geqq 2 \leqq t_2$, the progressions (1) involving 2 are $4^r(4n+2)$, $4^r(4n+3\alpha\Delta')$, $4^s(8n+5\alpha\Delta')$ and 4^τ multiplied by the progressions given for $\Delta'' = 2^{t_2} \equiv 0 \pmod 4$ and $\Omega'' = 1$ or 2 according as t_1 is odd or even, where $r = 0, 1, \cdots, [(t_1-2)/2]$, $\tau = [t_1/2]$, and $s = 0, 1, \cdots, [(t_1-3)/2]$, the progressions in s being omitted if $t_1 = 2$.

The character of F is determined as for $\Delta'' = 2^{t_2}$ and $\Omega'' = 1$ or 2 according as t_1 is odd or even.

G. Since F has no character with respect to 2 if improperly primitive, it remains to consider f improperly primitive but F properly primitive. Now f is improperly primitive if and only if $2n+1$ occurs in progressions (1). Then $\Omega \equiv 1 \not\equiv \Delta \pmod 2$. We use Lemma 13 to obtain

$$\Delta' f_2 \equiv \alpha\Delta' x^2 + \beta\Delta'\Omega y^2 + 4\gamma\Omega\Delta_1'' z^2 \pmod{8\Delta''},$$

$$\Omega F_2 \equiv \beta\gamma\Delta_1 x^2 + \alpha\gamma\Delta_1\Omega y^2 + \alpha\beta\Omega z^2 \pmod 8$$

where $\alpha\beta\Omega \equiv 3 \pmod 4$ and $x \equiv y \pmod 2$. $(\Delta_1'' = \Delta''/2.)$

Let $\alpha' = \alpha\Delta'$, $\beta' = \beta\Delta'\Omega$, $\gamma' = \gamma\Omega$ and replace α', β', γ' by α, β, γ respectively, and

$$\Delta' f_2 \equiv \alpha x^2 + \beta y^2 + 4\Delta_1'' \gamma z^2 \pmod{8\Delta''},$$

$$\Omega F_2 \equiv \alpha\Delta_1'' x^2 + \beta\Delta_1'' y^2 + \gamma z^2 \pmod 8,$$

with $x \equiv y \pmod 2$, $\alpha\beta \equiv 3 \pmod 4$ and $\alpha\beta\gamma \equiv 1 \pmod 8$. From Lemma 13 the integers represented by $\Delta' f$ are the halves of the evens represented by

$\Delta' f_2$ with $x \equiv y \pmod 2$ and the integers represented by ΩF are those represented by ΩF_2 with $x \equiv y \pmod 2$.

If $t_2 = 1$, i.e. $\Delta_1'' = 1$, no progressions (1) involving 2 occur except $2n+1$ and $\Omega F \equiv a \pmod 8$ is solvable if and only if $a \equiv 3 \pmod 4$.

If $t_2 = 2$, the progressions (1) involving 2 are $2n+1$ and, if $\alpha\beta \equiv 3 \pmod 8$, $4^k(8n+7\Delta')$. The congruence $\Omega F \equiv a \pmod 8$ is solvable if and only if $a \equiv \alpha\beta \pmod 8$.

If $t_2 > 2$ and $\alpha\beta \equiv 3 \pmod 8$ progressions (1) involving 2 are $4^r(2n+1)$ and, if t_2 is even, $4^k(8n+7\Delta')$, $r = 0, 1, \cdots, [(t_2-1)/2]$. Only $\Omega F \equiv 3 \pmod 8$ is solvable.

If $t_2 > 2$ and $\alpha\beta \equiv 7 \pmod 8$, the progression in (1) is $2n+1$ and only $\Omega F \equiv 7 \pmod 8$ is solvable.

IV. We have thus found associated with every prime factor of $2H$ progressions (1) such that for every integer a not contained in a progression involving an odd prime p it is true that $f \equiv a \pmod{p\mu_{ap}}$ is solvable and for every integer a not contained in a progression involving 2 it is true that $f \equiv a \pmod{8\mu_{a2}}$ is solvable. Thus if a is included in none of (1) it is true that $f \equiv a \pmod{8h\mu}$ is solvable. Also we have shown that these progressions determine the invariants Δ and Ω, the order and the genus of the form.

Conversely the invariants H, Δ and Ω together with order and generic character determine the progressions (1). This may be proved by inspection of the results listed above or from the theorem proved by Smith (pp. 480 ff.) that two forms of the same genus and order and having the same H, Ω and Δ may be transformed one into the other by a rational transformation of determinant 1, the denominators of the coefficients being prime to $2H$.

5. **Examples.** We apply this new definition of genus to the set of reduced properly primitive forms of Hessian 18.*

Consider the form $f = x^2+3y^2+6z^2$. Using the corollary of Lemma 4 we see the progression (1) involving 3 is $3n+2$. From Lemma 11, the progression (1) involving 2 is $4^k(16n+14)$.

Consider the form $g = 2x^2+3y^2+4z^2-2yz-2xy$. We have $10g = 5(2x-y)^2 + (5y-2z)^2+36z^2$ and the integers represented by $5g$ are the halves of the multiples of 10 represented by $g' = 5X^2+Y^2+36z^2$, for $g' \equiv 0 \pmod 5$ implies $Y^2 \equiv 4z^2 \pmod 5$ and the sign of Y may be so chosen that $5y-2z = Y$ is solvable for y while $g' \equiv 0 \pmod 2$ implies $X \equiv Y \pmod 2$ and thus $2x-y = X$ is solvable for x. Now, by Lemma 4, no progressions involving 3 occur in (1)

* See Eisenstein's table, Journal für Mathematik, vol. 41 (1851), p. 170.

for g' and therefore for g. By Lemma 6, no $4n+2$ occurs in progressions (1) for g' and therefore no $2n+1$ in progressions (1) for g. The condition $g' \equiv 0 \pmod 4$ implies $X = 2X_1$, $Y = 2Y_1$, and $g'/4 = 5X_1^2 + Y_1^2 + 9z^2$, and thus, using Lemma 9, $g'/4$ represents no $4^k(16n+6)/2$ and the progressions (1) for g are $4^k(16n+14)$.

The other forms are similarly dealt with. We have the following table:

Form	Progressions (1)
(1, 1, 18)	$9n \pm 3$, $4^k(16n+14)$
(2, 2, 5, 0, −2, 0)	$9n \pm 3$, $4^k(16n+14)$
(1, 2, 9)	$4^k(16n+14)$
(2, 3, 4, −2, 0, −2)	$4^k(16n+14)$
(1, 3, 6)	$3n+2$, $4^k(16n+14)$
(2, 3, 3)	$9^k(3n+1)$

The first and second forms are of the same genus, also the third and fourth. Each of the last two forms represents the only class in its genus.

CORNELL UNIVERSITY,
ITHACA, N.Y.