THE REGULARITY OF A GENUS OF POSITIVE TERNARY QUADRATIC FORMS*

BY

BURTON W. JONES†

1. **Introduction.** L. E. Dickson‡ has defined a positive ternary quadratic form f to be regular when the integers not represented by the form f coincide with certain arithmetic progressions.

The methods previously used for proving a form regular have been chiefly modifications§ of a method used by Dirichlet|| for the form $x^2+y^2+z^2$ together with certain elementary methods by which results for one form have been derived as corollaries from those of another. Now Dirichlet's method or modifications of it may be applied only when there is but one form in the genus or when it can otherwise be proved that all the integers represented by the forms of a genus are represented by one form. Heretofore it has been necessary to carry out a Dirichlet type of proof for each separate form or very restricted set of forms unless the proof could be referred back by elementary means to previous results for other forms, that is, with the exception of two cases when elliptic functions have been used.

In this paper it is proved that the integers represented by all of the forms of a genus¶ coincide with the positive integers in certain arithmetic progressions, i.e., a form f of genus G is regular if and only if f represents all the integers represented by every form of G. Using this result in the case of any form f, in order to prove f regular, it is necessary merely to show that there is only one class in the genus of f or that every integer represented by a form of the genus is represented by f. Similarly this establishes a new criterion for irregularity. Furthermore the form of these progressions in terms of the generic invariants is given by the author in his previous paper.

Examples are given at the end of this paper. Throughout this paper f

---

* Presented to the Society, December 30, 1930; received by the editors in July, 1930.

† National Research Fellow.

‡ Annals of Mathematics, (2), vol. 28 (1927), pp. 333–341.

§ See Annals of Mathematics, ibid.; Bulletin of the American Mathematical Society, vol. 33 (1927), p. 63.

|| Journal für Mathematik, vol. 40 (1850), pp. 228–32.

¶ For the definition of genus see H. J. S. Smith, Collected Papers, vol. 1, pp. 455–509, and *A new definition of genus for ternary quadratic forms* by the author, in the present number of these Transactions, referred to in this article as "the previous paper." L. E. Dickson in his definition of genus (*Studies in the Theory of Numbers*, p. 52) omits certain of Smith's generic characters because of their redundancy. It is immaterial in this paper whether Dickson's or Smith's definition is used.

denotes a primitive positive ternary quadratic form. In the opinion of the author, this discussion could be easily modified to include indefinite forms, also, but he has refrained from doing this in order to avoid possible duplication with a paper on indefinite forms by Mr. Arnold Ross soon to appear in the Proceedings of the National Academy and Sciences.

2. **Lemmas.** We shall first prove some elementary lemmas.

LEMMA 1. *If a_1 is any integer primitively represented by a primitive form $f=(a, b, c, 2r, 2s, 2t)$, i.e., $f=ax^2+by^2+cz^2+2ryz+2sxz+2txy$, f is equivalent to a form with leading coefficient a_1.*

This has been proved elsewhere but the proof is so simple that it is given here for completeness.

Suppose a primitive solution of $f=a_1$ is (x_1, y_1, z_1). Let $(x_1, y_1)=g$, the g.c.d. of x_1 and y_1, and choose integers u and v such that $x_1v-y_1u=g$. Then g is prime to z_1 since the solution is primitive and there thus exist a k and an n such that $gk-z_1n=1$. Then the transformation

$$x = x_1X + uY + x_1nZ/g, \ \ y = y_1X + vY + y_1nZ/g, \ \ z = z_1X + kZ$$

is of determinant 1, has integral coefficients, and takes f into a form with leading coefficient a_1.

LEMMA 2. *For any prime q and any positive integer k, the replacement of z by $z+\tau_1 y$ and then y by $y+\tau_2 z$ in $f=(a_1, b, c, 2r, 2s, 2t)$ yields, for a proper choice of τ_1 and τ_2 $\pmod{q^k}$, a form*

$$f' = (a_1, b', c', 2r', 2s', 2t')$$

with $s'\equiv t' \pmod{q^k}$.

If we subject f to such a transformation, we see the coefficient of x^2 remains unaltered, $t'=t+s\tau_1$ and $s'=t\tau_2+s(1+\tau_1\tau_2)=\tau_2(t+s\tau_1)+s$. If s is prime to q, take $\tau_2\equiv 0 \pmod{q^k}$ and have $s'\equiv s \pmod{q^k}$. Then τ_1 may be chosen $\pmod{q^k}$ so that $t'=t+s\tau_1\equiv s \pmod{q^k}$. If t but not s is prime to q, proceed similarly. If $s\equiv 0\equiv t \pmod{q}$ and $k>1$, replace s, t, s' and t' above by s/q, t/q, s'/q, t'/q respectively, and prove in precisely the same manner that τ_1 and τ_2 may be so chosen that $s'/q\equiv t'/q \pmod{q^{k-1}}$ unless $s\equiv t\equiv 0 \pmod{q^2}$ and $k>2$. This process may be continued until the proof is complete.

Consider a form $f=(a_1, b, c, 2r, 2s, 2t)$. Transform it first by

$$x = x' + \tau y + \sigma z, \ \ y = y, \ \ z = z, \tag{1}$$

and have

$$\begin{aligned} f' = a_1x'^2 &+ (a_1\tau^2 + 2t\tau + b)y^2 + (a_1\sigma^2 + 2s\sigma + c)z^2 + 2(r + a_1\tau\sigma + t\sigma + s\tau)yz \\ &+ 2(a_1\sigma + s)xz + 2(a_1\tau + t)xy \\ = a_1x'^2 &+ b'y^2 + c'z^2 + 2r'yz + 2s'xz + 2t'xy. \end{aligned}$$

Let $\lambda=(s', t')$ and transform f' by

$$x' = x', \ y = \alpha y' + \beta z', \ z = \gamma y' + \delta z'; \tag{2}$$

where

$$\alpha = - s'/\lambda, \ \gamma = t'/\lambda, \tag{3}$$

and β and δ are chosen so that

$$\alpha\delta - \beta\gamma = 1. \tag{4}$$

This yields

$$f'' = a_1x'^2 + b''y'^2 + c''z'^2 + 2r''y'z' + 2s''x'z' \text{ where } b'' = \alpha^2b' + \gamma^2c' + 2r'\alpha\gamma.$$

Let Ω denote the g.c.d. of the literal coefficients of the form adjoint to f, i.e. the g.c.d. of $bc-r^2$, a_1c-s^2, a_1b-t^2, $st-a_1r$, $rt-bs$, $rs-ct$. Let q be 2 or any odd prime factor of the Hessian H of a primitive form $f=(a_1, b, c, 2r, 2s, 2t)$ and ϵ the highest power of q occurring as a factor of H. We prove

LEMMA 3. *If $a_1\not\equiv 0 \pmod q$ and $\Omega\equiv 0 \pmod{q^\omega}$ but $\Omega\not\equiv 0 \pmod{q^{\omega+1}}$, where ω is a positive integer or zero, it is true that τ_1 and τ_2 in Lemma 2 and τ and σ in (1) may be so chosen modulo q or a power of q that (2) yields a form f'' with $b''\equiv r''\equiv 0 \pmod{q^\omega}$ but $b''\not\equiv 0 \pmod{\pi q^{\omega+1}}$, where $\pi=2$ or 1 according as q is even or odd.*

First note that Ω, being an invariant under transformations (1) and (2), is a divisor of a_1b'' and a_1r'', thus showing $b''\equiv r''\equiv 0 \pmod{q^\omega}$. From Lemma 2 we may consider the following congruence to hold: $t\equiv s \pmod{q^{\epsilon+2}}$. Note that $2\omega\leqq\epsilon$.

Now if $a_1b\not\equiv t^2 \pmod{\pi q^{\omega+1}}$, choose τ so that $a_1\tau+t=t'\equiv 0 \pmod{\pi q^{\omega+1}}$ and σ so that $a_1\sigma+s=s'\not\equiv 0 \pmod q$. Then $\gamma\equiv 0 \pmod{\pi q^{\omega+1}}$ and $b''\equiv\alpha^2(a_1\tau^2+2t\tau+b)\equiv\alpha^2(t\tau+b)\not\equiv 0 \pmod{\pi q^{\omega+1}}$ since $a_1(t\tau+b)\equiv -t^2+a_1b\not\equiv 0 \pmod{\pi q^{\omega+1}}$. If $a_1c\not\equiv t^2 \pmod{\pi q^{\omega+1}}$ the proof is similar.

If $a_1b\equiv a_1c\equiv t^2 \pmod{\pi q^{\omega+1}}$ and $a_1r\not\equiv t^2 \pmod{q^{\omega+1}}$, choose τ and σ so $t'\equiv s'\equiv 0 \pmod{\pi q^{\omega+1}}$ and $\alpha\gamma\not\equiv 0 \pmod q$. Then $b''\equiv\alpha^2(t\tau+b)+\gamma^2(t\sigma+c)-2(r+s\tau)\alpha\gamma\equiv -2(r+t\tau)\alpha\gamma\not\equiv 0 \pmod{\pi q^{\omega+1}}$.

Finally $a_1b\equiv a_1c\equiv a_1r\equiv t^2 \pmod{q^{\omega+1}}$ implies $\Omega\equiv 0 \pmod{q^{\omega+1}}$ which is contrary to hypothesis.

LEMMA 4. *If $a_1\equiv 0 \pmod{q^{\omega_1}}$ where $\omega_1\geqq 1$, $\Omega\not\equiv 0 \pmod q$ and q is 2 or an odd prime factor of H, then, for the proper choice in (1) of τ and σ and τ_1 and τ_2 in Lemma 2 modulo q or a power of q, (2) yields a form f'' with $b''\not\equiv 0 \pmod{\pi q^{\omega_1+1}}$ where $\pi=2$ or 1 according as q is even or odd and $a_1\not\equiv 0 \pmod{q^{\omega_1+1}}$.*

From Lemma 2 we need consider only $s\equiv t \pmod{q^{2\omega_1+3}}$. Then suppose

$s\equiv t\equiv 0 \pmod{q^{\omega_2}}$ where ω_2 is the greatest integer for which the congruence holds.

First: $\omega_2\geqq\omega_1>0$. If $b\not\equiv 0 \pmod q$ choose τ and σ so that $\alpha\not\equiv 0\equiv\gamma \pmod q$. Then $b''\equiv\alpha^2 b\not\equiv 0 \pmod q$. Proceed similarly if $c\not\equiv 0 \pmod q$. If $b\equiv c\equiv 0 \pmod q$ we know $r\not\equiv 0 \pmod q$, since f is primitive, and, choosing τ and σ that so $\alpha\gamma\not\equiv 0 \pmod q$ we have $b''\equiv 2r\alpha\gamma\not\equiv 0 \pmod q$ unless $q=2$. If $b+c\equiv 0 \pmod 4$, choose σ and τ divisible by 4, and so that $\alpha\gamma$ is odd, and have $b''\equiv b+c+2r\equiv 2 \pmod 4$. If $b+c\equiv 2 \pmod 4$ and b and c are even, we complete the proof for $\omega_2\geqq\omega_1>0$ as follows.

(1) If $t\equiv 0\equiv b+2 \pmod 4$ take τ so that $\gamma\equiv a_1\tau+t\equiv 0 \pmod 4$ and σ so that α is odd, and see $b''\equiv t\tau+b\equiv 2 \pmod 4$. Make γ odd and $\alpha\equiv 0 \pmod 4$ if $c\equiv 2 \pmod 4$.

(2) If $t\equiv 2\equiv a_1 \pmod 4$ and $b\equiv 0 \pmod 4$, take τ odd and σ even, have α odd, γ even and $b''\equiv a_1\equiv 2 \pmod 4$. Take τ even and σ odd if $c\equiv 0 \pmod 4$.

Second: $\omega_2=0$. Note $\alpha\gamma\not\equiv 0 \pmod q$ and let ω_3 be the greatest integer for which $b+c-2r\equiv 0 \pmod{q^{\omega_3}}$. If $\omega_3\leqq\omega_1$, take $\tau\equiv\sigma\equiv 0 \pmod{q^{\omega_3+1}}$ so that $\alpha\equiv-\gamma \pmod{q^{\omega_3+1}}$, and have $b''\equiv\alpha^2(b+c-2r)\not\equiv 0 \pmod{q^{\omega_3+1}}$. If $\omega_1<\omega_3$, take $\sigma\equiv 0 \pmod{q^{\omega_1+1}}$, and have $b''\equiv\alpha^2(a_1\tau^2+2t\tau+b)+\gamma^2 c+2(r+t\tau)\alpha\gamma \pmod{q^{\omega_1+1}}$. Noting $\gamma\lambda=t+a_1\tau$ and $\alpha\lambda\equiv -t \pmod{q^{\omega_1+1}}$, where λ is prime to q, we have $b''\lambda^2\equiv t\tau a_1\{-t\tau+2(c-r)\} \pmod{q^{\omega_1+1}}$ and τ may be chosen prime to q so that $b''\not\equiv 0 \pmod{q^{\omega_1+1}}$.

Third: $\omega_1>\omega_2>0$. Note $\alpha\gamma\not\equiv 0 \pmod q$. If $\omega_3\leqq\omega_1-\omega_2+\pi$ take $\tau\equiv\sigma\equiv 0 \pmod{q^{\omega_1-\omega_2+3}}$, so that $\alpha\equiv-\gamma \pmod{q^{\omega_1-\omega_2+3}}$, and have $b''\equiv\alpha^2(b+c-2r)\not\equiv 0 \pmod{q^{\omega_1-\omega_2+\pi+1}}$, i.e. $b''\not\equiv 0 \pmod{\pi q^{\omega_1+1}}$. If $\omega_3>\omega_1-\omega_2+\pi$, note that $b\not\equiv r\not\equiv c \pmod q$, since $b+c-2r\equiv 0 \pmod q$ and $b\equiv r \pmod q$ would imply $c-r\equiv bc-r^2\equiv\Omega\equiv 0 \pmod q$ contrary to hypothesis. Now take $\sigma\equiv 0 \pmod{q^{\omega_1+\omega_2+3}}$ and have, as in the paragraph above, $b''\lambda^2/q^{2\omega_2}\equiv ta_1\tau(-t\tau+2\{c-r\})/q^{2\omega_2}+a_1^2\tau^2 c/q^{2\omega_2} \pmod{q^{\omega_1-\omega_2+\pi+1}}$.

Now if $q=p$ an odd prime, the first member on the right of the last congruence is $\equiv 2\tau ta_1(c-r)/p^{2\omega_2} \pmod{p^{\omega_1-\omega_2+1}}$, and the second $\equiv 0 \pmod{p^{\omega_1-\omega_2+1}}$ since $2\omega_1-2\omega_2\geqq\omega_1-\omega_2+1$. Thus, taking $\tau\not\equiv 0 \pmod p$ we have $b''\not\equiv 0 \pmod{p^{\omega_1-\omega_2+1}}$, i.e., $b''\not\equiv 0 \pmod{p^{\omega_1+1}}$.

If $q=2$ we have $c-r\equiv 1 \pmod 2$, and thus $b''\equiv A\cdot 2^{\omega_1}\tau^2+B\tau\cdot 2^{\omega_1-\omega_2+1}+C\tau^2\cdot 2^{2\omega_1-2\omega_2} \pmod{2^{\omega_1+3-\omega_2}}$, where AB is odd and $C\equiv c \pmod 4$. Call $C\equiv 2^{\omega_4} \pmod{2^{\omega_4+1}}$, $\omega_4\geqq 0$. Then τ may be chosen so that $b''\not\equiv 0 \pmod{2^{\omega_1+3-\omega_2}}$ as follows.

(1) If one of $\omega_1-\omega_2+1$, ω_1, $2\omega_1-2\omega_2+\omega_4$ is less than the other two, $\tau\equiv 1 \pmod{2^{\omega_1+3-\omega_2}}$.

(2) If $\omega_1-\omega_2+1=\omega_1\leqq 2\omega_1-2\omega_2+\omega_4$, τ may be chosen odd so that $\tau A+B\equiv 2 \pmod 4$ or $\equiv 0 \pmod 4$ according as $2\omega_1-2\omega_2+\omega_4 \geqq \omega_1+2$ or not.

(3) If $\omega_1-\omega_2+1=2\omega_1-2\omega_2+\omega_4<\omega_1$, we have $\omega_4=0$, $\omega_1=1+\omega_2$, and choose τ odd so that $\tau(B+C\tau)\equiv 2$ or $0 \pmod 4$ according as $\omega_1\geqq\omega_1-\omega_2+3$ or not. Now $2\omega_1-2\omega_2+\omega_4<\omega_1-\omega_2+1$ is impossible since $\omega_1-\omega_2+\omega_4\geqq 1$. This completes the proof if we note $\omega_1+3-\omega_2\leqq\omega_1+2$.

THEOREM 1. *Any form f of Hessian H representing primitively an integer a_1 prime to Ω is equivalent to a form $f=a_1x^2+by^2+cz^2+2ryz+2sxz$ with $b=\Omega m\beta$, where $m=m_1m_2$, m_1 being prime to Ω and a divisor of a_1 and therefore of H, $m_2=1$ or 2, β prime to $2a_1H$, and $c\equiv s\equiv r\equiv 0$* $\pmod{\Omega}$. (Ω is defined just preceding Lemma 3.)

Since the choice of τ and σ in Lemmas 3 and 4 and τ_1 and τ_2 in Lemma 2 is purely congruential mod q or powers of q for each q, a choice of τ and σ, τ_1 and τ_2 simultaneously fulfilling the requirements for every q (2 or a prime factor of H) is possible in Lemmas 2, 3, and 4, thus proving that we can make $b=\Omega m\beta$ as in the theorem. By Lemma 3 we have $r\equiv 0 \pmod{\Omega}$. To make $s\equiv 0 \pmod{\Omega}$ after the other conditions of the theorem, except for that on c, are satisfied, replace x by $x+\tau z$, note that the coefficients of x^2 and of the terms in y remain unaltered and that the coefficient of $2xz$ becomes $a_1\tau+s$. τ may be chosen so that $a_1\tau+s\equiv 0 \pmod{\Omega}$. Thus we may consider s in f to be $\equiv 0 \pmod{\Omega}$. Then $a_1c-s^2\equiv 0 \pmod{\Omega}$ implies $c\equiv 0 \pmod{\Omega}$ and the proof is complete.

3. Consider the forms $f=(a, b, c, 2r, 2s, 0)$ and $f'=(a', b', c', 2r', 2s', 0)$ of the same Hessian H. Let the adjoints of the two forms be $\mathfrak{F}$ and $\mathfrak{F}'$ and the reciprocal forms $F=\mathfrak{F}/\Omega$ and $F'=\mathfrak{F}'/\Omega'$ respectively. We prove

THEOREM 2. *Two forms f and f' of Hessian H and having the same properties as f in Theorem 1 are of the same genus if $a\equiv a' \pmod{8h\mu}$, $b\equiv b'$, $c\equiv c'$, $r\equiv r'$, $s\equiv s' \pmod{8h\Omega}$, where h is the product of the first powers of the odd prime factors of H and μ is the smallest integer for which a/μ is an integer prime to $2h$.*

It has been proved by H. J. S. Smith in his article previously referred to, that the genus of a form depends solely on 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." Two forms f and f' of the same Hessian are obviously of the same character with respect to $8h$ if the respective literal coefficients are $\equiv \pmod{8h}$. Now $ac-s^2\equiv a'c'-s'^2 \pmod{8h\Omega}$ since $ac/\Omega\equiv a'c'/\Omega \pmod{8h}$. The same is true of the other literal coefficients of $\mathfrak{F}$ and $\mathfrak{F}'$. Thus $\Omega'=\Omega$, since any factor of $2h$ dividing all the literal coefficients of $\mathfrak{F}/\Omega$ divides all the literal coefficients of $\mathfrak{F}'/\Omega$ and conversely. Thus the literal coefficients of F and F' are respectively congruent mod $8h$. It is easily seen that this implies that the orders and the simultaneous characters of f and f' are the same and the proof is complete.

4. We shall prove the following theorem:

THEOREM 3. *For every form f representing primitively an integer a prime to Ω and any particular integer $a' \equiv a \pmod{16Hh\mu}$, where h and μ are defined in Theorem 2, there exists a form of the same Hessian and genus representing primitively a'.*

The method of proof here is a kind of generalization of that used by Dirichlet, as mentioned in the introduction to this paper.

We may consider f to be in the form of f in Theorem 1 with a_1 replaced by a. Then $H = a\delta - bs^2$ where $\delta = bc - r^2 = \Omega^2 dt$, $b = \Omega m\beta$ (see Theorem 1), d is a power of 2 and t is odd. Take $t = t_1 t_2$, where t_2 is the greatest factor of t prime to H. For a' then we seek integers b', c' and r' satisfying the conditions of Theorem 2 and such that $H = a'\delta' - b's^2$ where $\delta' = b'c' - r'^2 = \Omega^2 dt'$, $b' = \Omega m b_1$, b_1 prime to $2ha'$, and t' is odd. Take $t' = \tau + 16hHmt_1\Omega s^2 k$, where τ is chosen so that $a'\delta' \equiv a\delta \pmod{16Hh\Omega^2 t_1 d\mu m s^2}$. This is possible since this congruence is implied by $a't'/\mu \equiv at/\mu \pmod{16Hht_1 ms^2}$ and a'/μ as well as a/μ is prime to the modulus. (Any factor common to s and a divides H.) Note that this congruence implies that t'/t_1 is an integer prime to h, that $t'/t_1 \equiv t/t_1 \pmod{16Hh}$, and thus $\delta \equiv \delta' \pmod{16Hh\Omega^2 dt_1}$.

Then $b_1 = 16hHdt_1\Omega^2 a'k + (a'\Omega^2 d\tau - H)/(\Omega ms^2)$, since $H = a'\delta' - b's^2$. In view of the choice of τ, b_1 is an integer and $b_1 \equiv \beta \pmod{16h\Omega}$. Now the second member on the right of the last equation involving b_1 is an integer prime to $2H$ since β is, and is prime to a' since any factor common to a' and b_1 divides H. Thus the second member on the right and the coefficient of k are relatively prime, and by a classical theorem in the theory of numbers, we may choose k so that $b_1 = p$, a prime not dividing $2H$. Also β is prime to δ since any factor common to β and δ would divide H. For a similar reason p is prime to δ'. Since $bc - r^2 = \delta$, $(-\delta \mid \beta) = 1$.

Now $(-\delta' \mid p) = (-dt' \mid p) = (-d \mid p)(p \mid t')(-1)^\alpha$, where $\alpha = (t'-1)(p-1)/4 \equiv (t-1)(\beta-1)/4 \pmod 2$. Take $H = H'H''$, $m = m'm''$, $\Omega = \Omega'\Omega''$, the first factor in each equality being the greatest odd factor in the left member. Take $t_3' = (t', H)$, $t_3 = (t, H)$, $t'/t_3' = t_4'$, $t/t_3 = t_4$. Then $t_1 \equiv 0 \pmod{t_3'} \equiv 0 \pmod{t_3}$ and $t'/t_3 \equiv t/t_3 \pmod{16Hh}$. Thus $t_3 = t_3'$ and $t_4' \equiv t_4 \pmod{8Hh}$. Let $t_3 = t_{13}t_{23}$, where t_{23} is the greatest odd factor of t_3. Now, noting that $\Omega ms^2/t_3'$ is prime to t_4 and t_4' since H/t_3' is, and $H = a'\Omega^2 dt' - \Omega mps^2$, we have

$$(-\delta' \mid p) = (-d \mid p)(\{-H''\Omega''m''/t_{13}^2\} \mid t_4')(\{H'm'\Omega'/t_{23}^2\} \mid t_4') \cdot (p \mid t_3')(-1)^\alpha$$
$$= (-d \mid p)(\{-H''\Omega''m''/t_{13}^2\} \mid t_4')(p \mid t_3')(t_4' \mid \{H'm'\Omega'/t_{23}^2\})(-1)^\gamma;$$

where

$$\gamma = \alpha + (t_4' - 1)(H'm'\Omega' - 1)/4 \equiv \alpha + (t_4 - 1)(H'm'\Omega' - 1)/4 \pmod{2}.$$

Therefore

$$(-\delta' \mid p) = (-d \mid p)(\{-H''\Omega''m''/t_{13}^2\} \mid t_4)(p \mid t_3)(t_4 \mid \{H'm'\Omega'/t_{23}^2\}),$$
$$(-1)^\gamma = (-d \mid p)(\{-H''\Omega''m''/t_{13}^2\} \mid t_4)(p \mid t_3)(\{H'm'\Omega'/t_{23}^2\} \mid t_4),$$
$$(-1)^\alpha = (-d \mid \beta)(\beta \mid t)(-1)^\alpha,$$

since $(p \mid t_3) = (\beta \mid t_3)$, t_3 being a factor of H. Thus $(-\delta' \mid p) = (-d \mid \beta)(t \mid \beta) = (-\delta \mid \beta) = 1$.

Therefore there exists a ρ such that $-\delta' \equiv \rho^2 \pmod{p}$. Choose $r' \equiv \rho \pmod{p}$ and $\equiv r \pmod{16\Omega^2 dhH}$. Then $\delta + r^2 \equiv \delta' + r'^2 \pmod{16H\Omega}$, showing that $\delta' + r'^2 \equiv 0 \pmod{\Omega m}$, and we have shown the existence of a c' such that $\delta' = \Omega mpc' - r'^2$. Noting that $\delta = \Omega m\beta c - r^2$, we have $\Omega mpc' \equiv \Omega m\beta c \pmod{16Hh\Omega^2 d}$ and thus $pc' \equiv \beta c \pmod{16Hh\Omega d/m}$. Noting that $2H \equiv 0 \pmod{m}$ we have $c' \equiv c \pmod{8h\Omega}$ and the conditions of Theorem 2 that the forms f and f' be of the same genus are satisfied. Since the leading coefficient of f' is a', the representation of a' by f' is primitive.

THEOREM 3a. *For every form f representing an integer a prime to Ω and any particular $a' \equiv a \pmod{8h\mu}$, there exists a form f' of the same genus and Hessian representing a'.*

$16Hh\mu$ may be replaced by $8h\mu$ in the statement of Theorem 3 since $f \equiv a \pmod{16Hh\mu}$ solvable implies $f \equiv a \pmod{8h\mu}$ solvable and, by Lemma 17 of the previous paper* $f \equiv a \pmod{8h\mu}$ solvable implies $f \equiv a \pmod{16Hh\mu}$ solvable.

Suppose $a = k^2 a_1$, where f represents a_1 primitively and $k = k_1 k_2$, k_2 being the largest factor of k prime to $2h$. Then $a_1 k_1^2/\mu$ is prime to $2h$ and $f \equiv a_1 k_2^2 \pmod{8h\mu/k_1^2}$ is solvable.

Now since the quadratic characters of $a_1 k_1^2/\mu$ and of $a_1 k_1^2 k_2^2/\mu$ with respect to the factors of h are the same and since they are congruent mod 8, we have, by the lemmas of the previous paper, that $f \equiv a_1 \pmod{8h\mu/k_1^2}$ is solvable. Then $f \equiv a_1 k_2^2 \pmod{8h\mu/k_1^2}$ is solvable primitively, for, since f represents a_1 primitively, we may transform f to a form f_1 having its leading coefficient a_1 and a primitive solution of $f_1 \equiv a_1 k_2^2 \pmod{8h\mu/k_1^2}$ is $x = k_2$,

* See the sixth footnote of the Introduction.

$y=z=8h\mu/k_1^2$. Thus, from Theorem 3, there exists a form f' of the same genus representing $a'/k_1^2\equiv a_1k_2^2 \pmod{8h\mu/k_1^2}$. Thus f' represents a'.

5. We need two further lemmas.

LEMMA 5. *Any form f with $\Omega=p\Omega'\not\equiv 0 \pmod{p^2}$ and $H\not\equiv 0 \pmod{p^3}$, i.e., $H/\Omega^2=\Delta\not\equiv 0 \pmod{p}$, is equivalent to a form $f_1\equiv\alpha x^2+b'py^2+c'pz^2+2r'pyz \pmod{p^3}$ where $(b'c'|p)=-1$ and $\alpha\not\equiv 0 \pmod{p}$ (p is an odd prime).*

In $f=(\alpha, b_1, c_1, 2r_1, 2s_1, 2t_1)$ we may consider α to be prime to p. Replace x by $x+\tau y+\sigma z$, choosing τ and σ so the coefficients of $2xy$ and $2xz$ are $\equiv 0 \pmod{p^3}$, and have $f\equiv\alpha x^2+by^2+cz^2+2rzy \pmod{p^3}$. Now $\Omega\equiv 0 \pmod{p}$ implies $b=pb'$, $c=pc'$, $r=pr'$ and $f\equiv\alpha x^2+b'py^2+c'pz^2+2r'pyz \pmod{p^3}$. If $(b'c'|p)=-1$ the lemma is proved.

If $b'\equiv c'\equiv 0 \pmod{p}$ we know $r'\not\equiv 0 \pmod{p}$, since $\Omega\not\equiv 0 \pmod{p^2}$ and replacement of z by $y+z$ in $b'y^2+c'z^2+2r'yz$ yields a form with the coefficient of y^2 prime to p. This therefore reduces to the case below.

If b' or c' is prime to p, interchange y and z if necessary to have b', the coefficient of y^2, prime to p. In f replace y by $y+\tau z$ and see that the coefficients of y^2, xy, xz remain unaltered mod p^3 and that of pz^2 becomes $b'\tau^2+2r'\tau+c'$. To show that we may choose τ so that $b'(b'\tau^2+2r'\tau+c')=(b'\tau+r')^2+b'c'-r'^2$ is a non-residue of p, it is only necessary to show that for any a prime to p there exists an x such that x^2+a is a non-residue of p. ($b'c'-r'^2$ is prime to p since $H\equiv p^2\alpha(b'c'-r'^2)\not\equiv 0 \pmod{p^3}$.) This is obvious if $(a|p)=-1$. If $(a|p)=1$ the values $0, 1, \cdots, (p-1)/2$ of x give $(p+1)/2$ incongruent values of $x^2+a \pmod{p}$, one of which must be a non-residue, unless, for one of these values of x, $x^2+a\equiv 0 \pmod{p}$, and for the other values, x^2+a ranges in value over all the residues of p. This can happen only if $(-a|p)=1$, i.e. if $p\equiv 1 \pmod{4}$, and if, for every residue R of p, $x^2+a\equiv -Ra \pmod{p}$ is solvable for x, $-Ra$ being a residue of p. This is true only if $x^2\equiv -a(R+1) \pmod{p}$ is solvable for every R, i.e. if, for every $R\not\equiv -1 \pmod{p}$, $R+1$ is a residue of p. If this were true, since 1 is a residue of p, every positive integer less than p would be a residue of p which is false.

LEMMA 6. *If for a form $f_1=(\alpha', b, c, 2r, 2s, 2t)$, α' odd, $\Omega_1\equiv 2 \pmod{4}$ and $\Delta_1\equiv 2$, 4 or 6 $\pmod{8}$, it is true that $f_1\sim f_1'\equiv\alpha'x^2+2\beta'y^2+2\Delta_1\gamma'z^2 \pmod{128\,\Delta_1\Omega_1}$ and $f_1\sim f_1''\equiv\alpha'x^2+2\beta''y^2+2\Delta_1\gamma''z^2 \pmod{128\,\Delta_1\Omega_1}$ where $\beta'\beta''\equiv 1+\Delta_1\beta'\gamma' \pmod{8}$ and α' prime to $2H$.*

Since $\Omega_1\equiv\Delta_1\equiv 0 \pmod{2}$ implies that f_1 and F_1 are properly primitive, $f_1\sim f_1'$ above from Lemma 12 in the previous paper, and $\beta'=\Omega_1\beta/2$, $\gamma'=\gamma\Omega_1/2$, where $\alpha'\beta\gamma$ is prime to $2\Omega_1\Delta_1$. Thus $\beta'\gamma'$ is odd. The substitution $y=y'$, $z=y'+z'$ transforms $\beta'y^2+\Delta_1\gamma'z^2$ into $(\beta'+\Delta_1\gamma')y'^2+cz'^2+2ry'z'$. Let $\beta''=\beta'$

$+\Delta_1\gamma' \equiv 1 \pmod 2$ and replace y' by $y'+\tau z'$, choosing τ so that the coefficient of $2y'z'$ is $\equiv 0 \pmod{64\Delta_1\Omega_1}$. This does not alter the coefficient of y'^2 and gives $f_1' \sim f_1'' \equiv \alpha' x^2 + 2\beta'' y^2 + 2c'z^2 \pmod{128\Delta_1\Omega_1}$, where $\beta'\beta'' \equiv 1 + \Delta_1\beta'\gamma' \pmod 8$. Now $H \equiv 4\alpha'\beta''c' \pmod{128\Delta_1\Omega_1}$, i.e., $H/(4\Omega') \equiv \alpha'\beta''c'/\Omega' \pmod{64\Delta_1}$ where $\Omega' = \Omega_1/2$. We have $\alpha'\beta''/\Omega' \not\equiv 0 \pmod{\Delta_1}$ and thus $c' \equiv H/(4\Omega') \equiv 0 \pmod{\Delta_1}$ and the lemma is proved.

6. We use the following abbreviation throughout the remainder of the paper: $g = f/n$ means "the multiples of n represented by f are n multiplied by the integers represented by g."

THEOREM 4. *For any genus G of primitive forms f and Hessian H and any prime factor q of Ω there exists a genus G_1 (or G_2) of primitive forms f_1 (or f_2) of Hessian H/q (or H/q^4) such that the multiples of q (or q^2) represented by a form f of G are q (or q^2) multiplied by the integers represented by a form f_1 (or f_2) of G_1 (or G_2).*

Use the part of the theorem in parentheses if $\Omega \equiv 0 \pmod{q^2}$. Furthermore if $\Omega \not\equiv 0 \pmod{q^2}$, Ω_1, the Ω-factor of f_1, is Ω or Ω/q according as $\Delta \equiv 0 \pmod q$ or not, i.e. according as $H \equiv 0 \pmod{q^3}$ or not. If $\Omega \equiv 0 \pmod{q^2}$, $\Omega_2 = \Omega/q^2$. Note that by the notation explained above $f_1 = f/q$ and $f_2 = f/q^2$.

I. $q = p$ an odd prime. From Lemma 12 of the previous paper we may consider $f \equiv \alpha x^2 + \beta\Omega y^2 + \gamma\Omega\Delta z^2 \pmod{p^{t+1}}$ where t is the highest power of p in H and $\alpha\beta\gamma \equiv 1 \pmod{p^{t+1}}$. Then $f \equiv 0 \pmod p$ implies $x = px_1$ and, making the substitution in f and dividing by p, we have $f_1 \equiv p\alpha x_1{}^2 + \beta\Omega y^2/p + \gamma\Omega\Delta z^2/p \pmod{p^t}$. $f_1 = f/p$.

First if $\Omega \not\equiv 0 \pmod{p^2}$, f_1 is primitive since the coefficients are altered only by multiples of p or $1/p$ and $\Omega/p \not\equiv 0 \pmod p$. The Hessian of f_1 is H/p. Take the genus G_1 to be the genus of f_1. Now the progressions (1) of the previous paper associated with f_1 are those obtained by dividing by p all the multiples of p in the progressions (1) associated with f. By the theorem of the previous paper all forms f of genus G have the same progressions (1) associated with them. Thus all forms f_1 obtained by the above process from forms f of G have the same progressions (1) associated with them, and, by the same theorem, are thus of the same genus G_1. Conversely consider any form f_1' of genus G_1 and Hessian H/p. Below we prove the existence of a form f' for which $f'/p = f_1'$ and the quadratic character of the integers prime to p represented by f' is the same as that of the integers prime to p represented by f. This proves that the progressions (1) associated with f' and f are the same and therefore that f and f' are of the same genus.

Take $f \equiv \alpha x^2 + \beta\Omega y^2 + \gamma\Omega\Delta z^2 \pmod{p^{t+1}}$ to be a form of genus G.

A. $\Omega_1 = \Omega = p\Omega'$ and $\Delta_1 = \Delta/p \equiv 0 \pmod p$. Then by Lemma 12 of the previous paper, we take $f_1' \equiv \alpha' x^2 + \beta'\Omega y^2 + \gamma'\Omega\Delta_1 z^2 \pmod{p^t}$. Multiply f_1' by p, replace py by y and have $f' \equiv \alpha' p x^2 + \beta'\Omega' y^2 + \gamma'\Omega\Delta z^2 \pmod{p^{t+1}}$ and $f'/p = f_1'$. Furthermore $(\beta'\Omega' | p) = (\alpha | p)$, for the multiples of p represented by f_1' and by f_1 must be of the same character since f_1' and f_1 are of the same genus and $f_1'/p \equiv \alpha' p x_1^2 + \beta'\Omega' y^2 + \gamma\Omega'\Delta_1 z^2 \pmod{p^{t-1}}$, while $f_1/p \equiv \alpha x_1^2 + \beta\Omega y_1^2 + \gamma\Omega\Delta z^2/p^2 \pmod{p^{t-1}}$. Thus the conditions on f' required above are satisfied.

B. $\Omega_1 = \Omega = p\Omega'$ and $\Delta_1 = \Delta/p \not\equiv 0 \pmod{p}$. Then, by Lemma 5, we may consider $f_1' \equiv \alpha' x^2 + b' p y^2 + c' p z^2 + 2r' p yz \pmod{p^3}$ with $(b'c' | p) = -1$. Thus we can interchange y and z if necessary to make $(b' | p) = (\alpha | p)$. Then multiply f_1' by p and replace py by y, having $f' \equiv \alpha' p x^2 + b' y^2 + c' p^2 z^2 + 2r' p^2 yz \pmod{p^3}$, where $f'/p = f_1'$ and, as above, is of genus G.

C. $\Omega_1 = \Omega/p$. Then $\Delta_1 = \Delta p \not\equiv 0 \pmod{p^2}$ for $\Omega_1 F_1 \equiv \beta\gamma\Omega^2\Delta x^2/p^2 + \alpha\gamma\Omega\Delta y^2 + \alpha\beta\Omega z^2 \pmod{p}$ and $\Delta \equiv 0 \pmod{p}$ contradicts $\Omega_1 \not\equiv 0 \pmod{p}$. Thus we take $f_1' \equiv \alpha' x^2 + \beta'\Omega_1 y^2 + \gamma'\Omega\Delta z^2 \pmod{p^3}$. Multiply through by p, replace pz by z, and have $f' \equiv p\alpha' x^2 + \beta'\Omega y^2 + \gamma'\Delta\Omega_1 z^2 \pmod{p^3}$. Now $f'/p = f_1'$ and $(\gamma'\Delta\Omega_1 | p) = (\alpha | p)$ for f_1' and f_1, being of the same genus, have the same progressions (1) associated with them, and, by Lemmas 4 and 5 of the previous paper, $(-\beta\gamma\Delta | p) = (-\alpha'\beta'\Omega_1 | p)$, i.e. $(\alpha\Delta | p) = (\gamma'\Omega_1 | p)$.

Second, if $\Omega \equiv 0 \pmod{p^2}$, $f_1/p = f_2 \equiv \alpha x_1^2 + \beta\Omega y^2/p^2 + \gamma\Delta\Omega z^2/p^2 \pmod{p^{t-1}}$, where the Hessian of f_2 is H/p^4 and $\Omega_2 = \Omega/p^2$. Now $f/p^2 = f_2$ and, as above, we define G_2 to be the genus of f_2. All forms f_2 so obtained from forms of genus G are of the same genus G_2. Conversely any f_2' of genus G_2 may be taken $f_2' \equiv \alpha' x^2 + \beta'\Omega y^2/p^2 + \gamma'\Omega\Delta z^2/p^2 \pmod{p^{t-1}}$ where $(\alpha' | p) = (\alpha | p)$, for f_2' represents some integer α' prime to $2H$ for which $(\alpha' | p) = (\alpha | p)$, thus represents some such integer primitively, and, by Lemma 1 of this paper, is equivalent to a form with leading coefficient α'. Smith's process (ibid., pp. 460–462) by which f' is reduced to the form above leaves such a leading coefficient unaltered as is pointed out in the corollary to Lemma 12 of the previous paper. Now multiply the above form of f_2' by p and replace px by x having $f' \equiv \alpha' x^2 + \beta'\Omega y^2 + \gamma'\Omega z^2 \pmod{p^{t+1}}$, where $f'/p^2 = f_2'$. f' represents no multiple of $p \not\equiv 0 \pmod{p^2}$, $(\alpha' | p) = (\alpha | p)$, and therefore the progressions (1) of the previous paper associated with f' and f are the same and f' and f are of the same genus.

II. $q = 2$. Since $\Omega \equiv 0 \pmod{2}$ we know f is properly primitive. If further F is properly primitive we apply Lemma 12 of the previous paper as for $q = p$ and have $f \equiv \alpha x^2 + \beta\Omega y^2 + \gamma\Omega\Delta z^2 \pmod{2^{3+t}}$, $f_1 \equiv 2\alpha x_1^2 + \Omega\beta y^2/2 + \gamma\Delta z^2\Omega/2 \pmod{2^{2+t}}$ and $f/2 = f_1$. F is properly primitive if $\Delta \equiv 0 \pmod{2}$.

First, if $\Omega \equiv 2 \pmod{4}$ and F is properly primitive, 2 may be substituted for p in the corresponding discussion for $q = p$ if "the quadratic character of an odd integer mod 2" we interpret to mean the congruence satisfied mod 8, i.e. a_1 and a_2 are of the "same quadratic character with respect to 2" if $a_1 \equiv a_2 \pmod 8$.

A. $\Omega_1 = \Omega = 2\Omega'$ and $\Delta_1 = \Delta/2 \equiv 0 \pmod 8$. Using Lemma 12 of the previous paper we may take $f_1' \equiv \alpha' x^2 + 2\beta'\Omega' y^2 + 2\gamma'\Omega'\Delta_1 z^2 \pmod{8\Delta_1}$. Multiply by 2, replace $2y$ by y, and have $f' \equiv 2\alpha' x^2 + \beta'\Omega' y^2 + 4\gamma'\Omega'\Delta_1 z^2 \pmod{16\Delta_1}$ and $f'/2 = f_1'$. Now the evens represented by f_1' and by f_1 satisfy the same congruences mod 16. Thus $f_1'/2 \equiv 2\alpha' x^2 + \beta'\Omega' y^2 + \gamma'\Omega'\Delta_1 z^2 \pmod{4\Delta_1}$ and $f_1/2 \equiv \alpha x_1^2 + 2\beta\Omega' y^2 + \gamma\Omega'\Delta_1 z^2 \pmod{4\Delta_1}$ implies that $\beta'\Omega'$ and $\beta'\Omega' + 2\alpha'$ are congruent $\pmod 8$ in some order to α and $\alpha + 2\beta\Omega'$, which proves that the odd integers represented by f and f' satisfy the same congruences mod 8.

B. $\Omega_1 = \Omega = 2\Omega'$ and $\Delta_1 = \Delta/2 \equiv 4 \pmod 8$. Using Lemma 6 we may take $f_1' \equiv \alpha' x^2 + 2\beta' y^2 + 2\Delta_1\gamma' z^2 \pmod{128\Delta_1}$ and also $f_1' \sim f_1'' \equiv \alpha' x^2 + 2\beta'' y^2 + 2\Delta_1 \gamma'' z^2 \pmod{128\Delta_1}$ where $\beta'\beta'' \equiv 5 \pmod 8$. Now f_1' represents primitively an integer $\equiv \beta\Omega' \pmod 8$, since f_1 does. Then we may take $\alpha' \equiv \beta\Omega' \pmod 8$. Noting that $f_1' \equiv \alpha' x^2 + 2\beta' y^2 \pmod 8$ and $f_1 \equiv 2\alpha x_1^2 + \beta\Omega' y^2 \pmod 8$ we see that $\alpha \equiv \beta' \pmod 4$. Replacing f' by f'' if necessary, we have $f_1' \equiv \alpha' x^2 + 2by^2 + 2\Delta_1\gamma' z^2 \pmod{128\Delta_1}$ with $b \equiv \dot{\alpha} \pmod 8$ and $\alpha' \equiv \beta\Omega' \pmod 8$. Multiplying f_1' by 2 and replacing $2y$ by y we have $f' \equiv 2\alpha' x^2 + by^2 + 4\Delta_1\gamma' z^2$ (mod 128Δ), $f'/2 = f_1'$, and f' is of genus G.

C. $\Omega_1 = \Omega = 2\Omega'$ and $\Delta_1 = \Delta/2 \equiv 2 \pmod 4$. Let $\Delta/4 = \Delta_1/2 = \Delta'$. Here

$$\Delta' f_1' \equiv \alpha' x^2 + 2\beta' y^2 + 4\gamma' z^2 \pmod{64},$$

$$\Delta' f \equiv \alpha x^2 + 2\beta y^2 + 8\gamma z^2 \pmod{128},$$

$\alpha'\beta'\gamma' \equiv 1 \pmod 8$ since $8\alpha'\beta'\gamma' \equiv \Delta'\dot{H}_1 \equiv 8 \pmod{64}$. Similarly $\alpha\beta\gamma \equiv 1 \pmod 8$. Now, since $f_1' \equiv$ all odds $\pmod 8$ is solvable, we may consider $\alpha' \equiv \beta \pmod 4$. Since, by Lemma 6, β' may be replaced by $\beta'' \equiv 3\beta' \pmod 4$ and $\alpha'\beta''\gamma'' \equiv 1 \pmod 8$, we have $\gamma'' \equiv 3\gamma' \pmod 4$. We therefore can make $\gamma' \equiv \alpha'$ or $3\alpha' \pmod 4$ according as $\beta \equiv \gamma$ or $3\gamma \pmod 4$. Now the multiples of 4 represented by $\Delta' f_1'$ and by $\Delta' f_1$ satisfy the same congruences (mod 32), i.e. the evens represented by $\Delta' f_1'/2 \equiv 2\alpha' x^2 + \beta' y^2 + 2\gamma' z^2 \pmod{16}$ and by $\Delta' f_1/2 \equiv \alpha x^2 + 2\beta y^2 + 2\gamma z^2 \pmod{16}$ satisfy the same congruences mod 16. Thus, by the corollaries to Lemmas 10 and 11 of the previous paper, $\alpha' + \gamma' \equiv 2$ or $4 \pmod 8$ if and only if $\beta + \gamma \equiv 2$ or $4 \pmod 8$ in some order. If $\beta + \gamma \equiv 2 \pmod 8$, we see that $\beta \equiv \gamma \pmod 4$, and, by the above choice of γ', $\alpha' + \gamma' \equiv 2 \pmod 4$ and therefore $\alpha' + \gamma' \equiv 2 \pmod 8$. Similarly for all cases, the above choice of γ' is seen to make $\alpha' + \gamma' \equiv \beta + \gamma \pmod 8$.

Now if $\beta + \gamma \equiv 2a \pmod 8$, $\alpha \equiv 2a\beta - 1 \pmod 8$ and the odds represented by $\Delta' f$ are exclusively $\equiv 2a\beta - 1$, $2\beta(a+1) - 1 \pmod 8$. Multiply $\Delta' f_1'$ by 2, replace $2y$ by y, and have $\Delta' f' \equiv 2\alpha' x^2 + \beta' y^2 + 8\gamma' z^2 \pmod{128}$. $\Delta' f'/2$

$=\Delta'/f_1'$, and the odds represented by $\Delta' f'$ are exclusively $\equiv\beta'$ and $\beta'+2\alpha'$ (mod 8). $\beta'\equiv 2a\alpha'-1\equiv 2a\beta-1$ (mod 8) and $\beta'+2\alpha'\equiv 2\beta(a+1)-1$ (mod 8) show that the odds represented by $\Delta' f'$ and by $\Delta' f$ satisfy the same congruences (mod 8) and thus f' and f are of the same genus.

D. $\Omega_1=\Omega=2\Omega'$ and $\Delta_1=\Delta/2=\Delta'\equiv 1$ (mod 2). Now f_1 represents $\beta\Omega'$ and $\beta\Omega'+2\alpha\equiv 3\beta\Omega'$ (mod 4) and thus from the form of f_1 in Lemma 14 of the previous paper we see this can happen only if F_1 is properly primitive. Furthermore for any form f_1' of genus G_1, F_1' is properly primitive since f_1', too, must represent integers $\equiv 1$ and 3 (mod 4). Thus only $f_1'\equiv\alpha' x^2+2\Omega'\beta' y^2+2\Omega'\Delta'\gamma' z^2$ (mod 8) need be considered. Multiply by 2, replace $2y$ by y and $f'\equiv 2\alpha' x^2+\Omega'\beta' y^2+4\Omega'\Delta' z^2$ (mod 16). f' and $f\equiv 1$, 3, 5 or 7 (mod 8) are solvable, $f'/2=f_1'$, and thus f' and f are of the same genus.

E. $\Omega_1=\Omega/2\equiv 1$ (mod 2) and F properly primitive. Then $\Delta_1=2\Delta\equiv 2$ (mod 4) as in the case IC. Here f_1 represents an odd and thus the genus is composed of properly primitive forms. We have

$$\Delta f = \Delta' f \equiv \alpha x^2 + 2\beta y^2 + 2\gamma z^2 \pmod{16};$$

$$\Delta f_1 \equiv 2\alpha x_1^2 + \beta y^2 + \gamma z^2, \quad \alpha\beta\gamma \equiv 1 \pmod{8};$$

$$\Delta f_1' \equiv \alpha' x^2 + \beta' y^2 + 2\gamma' z^2, \quad \alpha'\beta'\gamma' \equiv 1 \pmod{8}.$$

Since the odds represented by Δf_1 and $\Delta f_1'$ satisfy the same congruences mod 8, we have, from Lemmas 10 and 11 of the previous paper, $\beta+\gamma\equiv 2$ or 4 (mod 8) if and only if $\alpha'+\beta'\equiv 2$ or 4 (mod 8) in some order. Multiply $\Delta f_1'$ by 2, replace $2z$ by z, and have $\Delta f'\equiv 2\alpha' x^2+2\beta' y^2+\gamma' z^2$ (mod 16), and, by virtue of the corollaries to Lemmas 10 and 11 of the previous paper, the odds represented by $\Delta f'$ and Δf satisfy the same congruences (mod 8). $\Delta f'/2=\Delta f_1'$ and thus f' and f are of the genus G.

F. $\Omega_1=\Omega/2\equiv 1$ (mod 2) and F improperly primitive. Then, as above, $\Delta_1=2\Delta\equiv 2$ (mod 4). Using Lemma 14 of the previous paper we take a form f of genus G as follows: $f\equiv ax^2+4by^2+4cz^2+4ryz$ (mod 16) with $br\equiv 1$ (mod 2). $f/2=f_1\equiv 2ax_1^2+2by^2+2cz^2+2ryz$ (mod 8) and the genus G_1 of f_1 is composed of improperly primitive forms. Now from the proof of Lemma 13 of the previous paper we may take $f_1'\equiv 2\alpha x^2+2b'' xy+2\alpha' y^2+2\beta z^2$ (mod 16), where $\alpha b''$ is odd and $\beta=\gamma\Omega_1\Delta_1/2\equiv 1$ (mod 2) since γ is an odd integer. Multiply f_1' by 2, replace $2z$ by z and have $f'\equiv\beta z^2+4\alpha x^2+4b'' xy+4\alpha' y^2$ (mod 16), $f'/2=f_1'$. Since f' represents only integers $\equiv\beta$ and $\beta+4\alpha$ (mod 8) and multiples of 4, it remains to prove $\beta\equiv a$ (mod 4). This is done as follows: From the form of f', $H\equiv 4\beta(4\alpha\alpha'-b''^2)\equiv 12\beta$ (mod 16), and likewise for f, $H\equiv 4a(4bc-r^2)\equiv 12a$ (mod 16). Thus $a\equiv\beta$ (mod 4).

Second: $\Omega\equiv 0$ (mod 4). Then by Lemma 14 of the previous paper we may consider any form f of genus G to be of the form

$$f \equiv ax^2 + 2^{t_1}by^2 + 2^{t_1}cz^2 + 2^{t_1+1}ryz \pmod{2^{t_1+3}}$$

where $\Omega \equiv 2^{t_1} \pmod{2^{t_1+1}}$, b is odd if F is properly primitive and $b \equiv c \equiv r+1 \equiv 0 \pmod 2$ if F is improperly primitive. Now $t_1 \geqq 2$ and $f \equiv 0 \pmod 2$ implies $x = 2x_1$ and $f_2 = f/4 \equiv ax_1^2 + 2^{t_1-2}by^2 + 2^{t_1-2}cz^2 + 2^{t_1-1}ryz \pmod{2^{t_1+1}}$. $H_2 = H/16$, $\Omega_2 = \Omega/4$ and $\Delta_2 = \Delta$. Now F_2 is improperly primitive if and only if $b \equiv c \equiv r+1 \equiv 0 \pmod 2$, i.e., if and only if F is improperly primitive. Define the genus G_2 to be the genus of f_2. Take any form f_2' of genus G_2 and see by Lemma 14 of the previous paper that we may take

$$f_2 \equiv a'x^2 + 2^{t_1-2}b'y^2 + 2^{t_1-2}c'z^2 + 2^{t_1-1}r'yz \pmod{2^{t_1+1}},$$

where $a' \equiv a \pmod 8$, b' is odd if F_2, and therefore F, is properly primitive, and $b' \equiv c' \equiv r'+1 \equiv 0 \pmod 2$ if F_2, and therefore F, is improperly primitive. Multiply by 4, replace $2x$ by x, and have

$$f' \equiv a'x^2 + 2^{t_1}b'y^2 + 2^{t_1}c'z^2 + 2^{t_1+1}r'yz \pmod{2^{t_1+3}}.$$

$f'/4 = f_2'$, f' represents no $4n+2$, and is of the same genus as f.

7. We prove the following theorem:

THEOREM 5. *The integers represented by no primitive form f of a given genus G are exclusively those occurring in progressions* (1), *of the previous paper, associated with f.*

Consider any integer a included in none of the progressions (1) associated with f. It follows from the theorem of the previous paper that $f \equiv a \pmod{8h\mu}$ is solvable. If a is prime to Ω, Theorem 3a applies to prove the theorem above. Otherwise we proceed as follows.

First let q be a prime factor of a which, when squared, divides Ω. Then $a \equiv 0 \pmod{q^2}$ since reference to the proofs of the previous paper shows $\Omega \equiv 0 \pmod{q^2}$ implies that qa occurs in progressions (1). Then there exists by Theorem 4 a form f_1 with $\Omega_1 = \Omega/q^2$ and $H_1 = H/q^4$ such that $f_1 = f/q^2$ and thus $f_1 \equiv a/q^2 \pmod{8h\mu/q^2}$. If $a/q^2 \equiv 0 \pmod q$ and $\Omega_1 \equiv 0 \pmod{q^2}$, we have $a/q^2 \equiv 0 \pmod{q^2}$ and the process may be repeated until, after r times, $f_r \equiv a/q^{2r} \pmod{8h\mu/q^{2r}}$ where $\Omega_r = \Omega/q^{2r}$, $f_r = f/q^{2r}$, $H_r = H/q^{4r}$ and either $a/q^{2r} \not\equiv 0 \pmod q$ or $\Omega_r \not\equiv 0 \pmod{q^2}$. If there is another prime factor, q_1, of a which, when squared, divides Ω, it is true that $\Omega_r \equiv 0 \pmod{q_1^2}$ and the above process may be applied to f_r. So this may be continued until we have the case below.

$g \equiv a/\mu_1^2 = a' \pmod{8h\mu/\mu_1^2}$ where $\Omega_g = \Omega/\mu_1^2$, $H_g = H/\mu_1^4$, $g = f/\mu_1^2$ and no prime factor of a' is, when squared, a factor of Ω_g. Let q' be a prime factor of a' dividing Ω_g. Since $\Omega_g \not\equiv 0 \pmod{q'^2}$, there exists a form $g_1 = g/q'$ of $\Omega_{g1} = \Omega_g$ or Ω_g/q' according as $H_g \equiv 0 \pmod{q'^3}$ or not. Then $g_1 \equiv a'/q'$

(mod $8h\mu/\{\mu_1^2 q'\}$) is solvable. If $H_g \equiv 0 \pmod{q'^3}$ and $a'/q' \equiv \Omega_{g1} \equiv 0 \pmod{q'}$, we repeat the process until after t times we have $g_t = g/q'^t$ where $\Omega_{gt} = \Omega_g/q'^t$ or $\Omega_g/(q')^{t-1}$, $g_t \equiv a'/q'^t \pmod{8h\mu/\{\mu_1^2 q'^t\}}$ is solvable and either a'/q'^t or Ω_{gt} is prime to q'. Then any other factor q_1' dividing a' and Ω_g divides Ω_{gt} and the above process may be applied to g_t. This may be carried through for every factor q' dividing a' and Ω_g until we have a form $g' = f/\{\mu_1^2\mu_2\}$ where $g' \equiv a/\mu_1^2\mu_2 \pmod{8h\mu/\{\mu_1^2\mu_2\}}$, $\Omega_g' = \Omega/(\mu_1^2\mu_2')$, where $\mu_2 \equiv 0 \pmod{\mu_2'}$, $H_{g'} = H/(\mu_1^4\mu_2)$ and $a/(\mu_1^2\mu_2)$ is prime to $\Omega_{g'}$.

Then by Theorem 3a there exists a form g'' of the same genus and Hessian as g' which represents $a/(\mu_1^2\mu_2)$. Following through the above process in the reverse order, applying the theorem of the previous paper at every step, we have the existence of a form f' of the same genus and Hessian as f such that $f'/(\mu_1^2\mu_2) = g''$, which proves that f' represents a.

COROLLARY. *A form f of genus G is regular if and only if f represents all the integers represented by every form of G.*

For suppose some integer k is not represented by f but is represented by some form f' of G. Then k occurs in no progression (1) and thus $f \equiv k \pmod{N}$ is solvable for N arbitrary, every arithmetic progression containing k contains an integer represented by f, and therefore, from the definition of regularity, f is irregular.

Note. Whenever f is the only reduced form of a genus it is regular, but, though most regular forms represent the only class in the genus, this is not always the case. See the following.

8. This section gives three examples.

I. $f = x^2 + 8y^2 + 24z^2$ and $g = x^2 + 2(2y+x)^2 + 6(2z+x)^2 = 8y^2 + 9x^2 + 24z^2 + 8xy + 24xz$ are of the same genus. They are not of the same class since g does not represent 1. Every odd integer n represented by g is represented by f, for if (x_1, y_1, z_1) is a solution of $g = n$, the $\pm$ sign may be so chosen in $2y_1 + x_1 \pm (2z_1 + x_1) = 4Y$ that the equation is solvable for Y and $n = x_1^2 + 8(2z + x_1 \mp Y)^2 + 24Y^2$. The evens represented by f and g are obviously the same. f is regular since f and g represent the only classes in the genus, but g is irregular.

II. The forms $x^2 + 3y^2 + 6z^2$ and $2x^2 + 3y^2 + 3z^2$ are regular, for each represents the only class in the genus. (See the examples of the previous paper.)

III. The forms $f = (1, 1, 18)$ and $g = (2, 2, 5, 0, -2, 0)$ are of the same genus and both are irregular, for f but not g represents 1 and g but not f represents 7.

CORNELL UNIVERSITY,
ITHACA, N. Y.