AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF
THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

VOLUME LXVIII
1946

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

INDEX

$$\mathrm{K}_B(z,\bar{\zeta}) \leqq [\sum_{\nu=1}^{\infty} | \phi'_\nu(z) |^2 \cdot \sum_{\nu=1}^{\infty} | \phi'_\nu(\zeta) |^2]^{\frac{1}{2}} \leqq \pi^{-1}\delta_1{}^{-1}\delta_2{}^{-1},$$

which yields the inequality (5.1).

We note that using other inequalities for $\mathrm{K}_B(z,\bar{\zeta})$ and for its derivatives (see [2] § 9) one can obtain other inequalities similar to (5.1).

Brown University.

BIBLIOGRAPHY.

1. Stefan Bergman, "Über die Kernfunktion eines Bereiches und ihr Verhalten am Rande," *Journ. für die reine u. ang. Math.*, vol. 169 (1933), pp. 1-42 and vol. 172 (1934), pp. 89-128.

2. ———, *Partial differential equations, Advanced Topics* (*Conformal Mapping of multiply connected domains*) Publication of Brown University, Providence, R. I., 1941.

3. R. Courant, "Plateau's problem and Dirichlet's principle," *Annals of Mathematics*, vol. 38 (1937), pp. 679-724.

4. C. Carathéodory, "Untersuchungen über die konforme Abbildungen von festen und veränderlichen Gebieten," *Mathematische Annalen*, vol. 72 (1912), pp. 107-144.

5. Paul Koebe, "Abhandlungen zur Theorie der konformen Abbildung II, IV," *Acta Mathematica*, vol. 40 (1915/16), pp. 251-290 and vol. 41 (1916), pp. 305-344.

6. Paul Kufareff, "Über das zweifach zusammenhängende Minimalgebiet," *Bull. Inst. Math. et mec. Université de Tomsk*, vol. 1 (1935-1937), pp. 228-236

7. R. Nevanlinna, *Eindeutige analytische Funktionen*, Berlin, 1936.

8. F. Schottky, "Über die conforme Abbildung mehrfach zusammenhängender ebener Flächen," *Journ. für die reine u. ang. Math.*, vol. 83 (1877), pp. 300-351.

9. K. Zarankiewicz, "Sur la représentation conforme d'un domaine doublement connexe sur un anneau circulaire," *C. R. Acad. Sc.*, Paris, vol. 198 (1934), pp. 1347-1349.

10. ———, "Über ein numerisches Verfahren zur konformen Abbildung zweifach zusammenhängen Gebiete," *Zeit. f. ång. Math. u. Mech.*, vol. 14 (1934), pp. 97-104.

11. B. Fuchs, "Sur la fonction minimale d'un domaine, I," *Mat. Sbornik* (*Recueil Mathem.*), N. S. vol. 16 (58) (1945), pp. 21-38.

12. L. Greenstone, "Mapping of simply and multiply connected domains by analytic functions," to appear.

ON A PROBLEM OF RAMANUJAN.*

By Arnold E. Ross.

1. It was apparently known to Diophantus and first proven by Lagrange (8) that the form $x^2 + y^2 + z^2 + u^2$ represents all positive integers. Examples of other integral forms

$$\Phi = ax^2 + by^2 + cz^2 + du^2 \tag{1.1}$$

which represent all positive integers, were first obtained by Jacobi (5), Liouville (9), and Pepin (13). Ramanujan (14) proved that there are only 54 sets of positive integers a, b, c, d such that (1.1) represents all positive integers. Dickson (2) called such forms *universal*. Universal quaternary quadratic forms with cross products were studied by Dickson (2) and Morrow (11).

In the above mentioned paper Ramanujan proposed another problem, *viz.*, the problem of determining the conditions under which positive quadratic forms (1.1) represent all except a finite number of integers. Kloosterman (7), employing the methods of Hardy-Littlewood succeeded, save for a finite number of exceptions, in solving that problem.

It is natural to ask Ramanujan's question concerning general positive quaternary quadratic forms. Should Tartakowsky's theorem (19) concerning the representation of large integers by positive quadratic forms in $n \geqq 5$ variables hold also for $n = 4$, then one would expect the answer to that question to be found as an elementary corollary of this theorem and to be expressed in terms of the generic characters of quadratic forms. It is of interest to note that, although Tartakowsky's theorem does not carry over unconditionally to forms in four variables, still for forms of odd determinants and certain orders of even determinants, the answer to Ramanujan's question may be obtained as an elementary extension of the results of Kloosterman and some other elementary considerations, and that, moreover, save for a finite number (of classes) of exceptions the conditions are given in terms of the generic characters. The results here obtained suggest conditions which the generic characters of a genus of quaternary forms should fulfil in order that all forms of that genus should represent the same large integers.

The method employed may be summarized as follows: Through the use of the canonical form of Section **3**, the problem of the representation of in-

* Received August 3, 1942 and June 14, 1945.

tegers by the original form is reduced to that of the representation of integers by a certain quadratic form without the cross products (Section **4**. 1). Kloosterman's conditions (7) applied to this last form (Section **5**) yield a set of generic character conditions which assure the representation of all large integers by the original form. Upon closer examination of these conditions one notices (Sections **6** and **7**) that some of these are necessary but that the failure of the remaining merely implies that a form represents *all large* integers only if it represents *all* integers or *all even* integers. In view of the results in Section **2**, the determinants of such forms do not exceed a fixed number. Thus, outside of forms in Section **5**, there is only a finite number of classes of forms representing all large integers. A study of some of these classes (Section **8**) yields interesting examples of representation of integers by positive quaternary forms in a fixed genus.

2. An upper bound for determinants of classic universal positive quaternary quadratic forms. Among the 54 universal forms of type (1. 1), the form $x^2 + 2y^2 + 4z^2 + 14u^2$ has [1] the largest determinant 112. A simple extension of Ramanujan's argument yields [2] the more general and quite useful

THEOREM 2. *The determinant of every classic universal positive quaternary quadratic form is* $\leqq 112$.

We write

$$\Phi_1(x) = x'Ax = \sum_{i,j=1}^{4} a_{ij}x_ix_j \tag{2.01}$$

where a_{ij} are integers. If $\Phi_1(x)$ represents all positive integers, it represents 1 properly, and hence is equivalent to a form of type (2. 01) with $a_{11} = 1$ and $a_{1j} = 0$ for $j = 2, 3, 4$. Thus

$$\Phi_1(x) \sim \Phi_2(y) = y_1^2 + \phi_2(y_2, y_3, y_4) = y_1^2 + \sum_{i,j=2}^{4} b_{ij}y_iy_j.$$

In order that Φ_1 and, hence, Φ_2 should represent all positive integers, the minimum a of ϕ_2 must be ≤ 2. For otherwise Φ_2, and therefore also Φ_1, would not represent 2. Since the minimum a is represented properly by ϕ_2

$$\phi_2 \sim \phi_3 = az_2^2 + bz_3^2 + cz_4^2 + 2rz_3z_4 + 2sz_2z_4 + 2tz_2z_3, \tag{2.02}$$

where

$$0 \leq s < a \quad \text{and} \quad 0 \leq t < a, \qquad a = 1 \text{ or } 2, \tag{2.03}$$

and hence

$$\Phi_1 \sim \Phi_3 = z_1^2 + \phi_3(z_2, z_3, z_4). \tag{2.04}$$

[1] Cf. Dickson (4), p. 115.

[2] Ross (15), Theorem 8.

2. 1. We let, first, $a = 1$. Then, in view of (2. 02)-(2. 04),

$$\Phi_3 = z_1^2 + z_2^2 + bz_3^2 + cz_4^2 + 2rz_3z_4 = z_1^2 + z_2^2 + \psi_3(z_3, z_4). \tag{2.11}$$

In order that Φ_3 should represent 3, the minimum M of ψ_3 should be ≤ 3. Then

$$\psi_3 \sim \psi_4 = Mu_3^2 + 2Nu_3u_4 + Lu_4^2, \tag{2.12}$$

$$-(M/2) < N \leq M/2, \qquad M = 1, 2, \text{ or } 3, \tag{2.13}$$

and

$$\Phi_1 \sim \Phi_4 = u_1^2 + u_2^2 + \psi_4. \tag{2.14}$$

The form Φ_1 would represent all integers only if $M\Phi_1$ should represent all multiples of M. But in view of (2. 12)-(2. 13)

$$M\Phi_1 \sim M\Phi_4 = Mu_1^2 + Mu_2^2 + (Mu_3 + Nu_4)^2 + Du_4^2$$

where $D = ML - N^2$ is the determinant of Φ_1. Thus in order that $M\Phi_1$ should represent all multiples of M, D must not exceed the smallest multiple of M not represented by

$$f_M(u_1, u_2, U_3) = Mu_1^2 + Mu_2^2 + U_3^2.$$

If $M = 1$, $f_1 = u_1^2 + u_2^2 + U_3^2 \neq 7$ and hence $D \leq 7$.
If $M = 2$, $f_2 = 2u_1^2 + 2u_2^2 + U_3^2 \neq 28$ and therefore $D \leq 28$.
If $M = 3$, $f_3 = 3u_1^2 + 3u_2^2 + U_3^2 \neq 18$ and therefore $D \leq 18$.

Thus, in case $a = 1$, there is no universal form Φ_1 of determinant > 28.

2. 2. Next, let $a = 2$. In order that Φ_1 should be universal $2\Phi_1$ should represent all even integers. But in view of (2. 02) and (2. 04),

$$2\Phi_1 \sim 2\Phi_3 = 2z_1^2 + (2z_2 + tz_3 + sz_4)^2 + \psi_3(z_3, z_4)$$

where

$$\psi_3(z_3, z_4) = (ab - t^2)z_3^2 + 2(ar - st)z_3z_4 + (ac - s^2)z_4^2.$$

Since $2z_1^2 + Z_2^2 \neq 10$, the minimum M of $\psi_3(z_3, z_4)$ is ≤ 10. Also,

$$\psi_3 \sim \psi_4 = Mu_3^2 + 2Nu_3u_4 + Lu_4^2$$
$$2\Phi_1 \sim 2\Phi_4 = 2u_1^2 + (2u_2 + t_1u_3 + s_1u_4)^2 + \psi_4(u_3, u_4)$$

and

$$\begin{aligned} 2M\Phi_1 \sim 2M\Phi_4 = 2Mu_1^2 &+ M(2u_2 + t_1u_3 + s_1u_4)^2 \\ &+ (Mu_3 + Nu_4)^2 + (ML - N^2)u_4^2. \end{aligned}$$

In order that Φ_1 should be universal $2M\Phi_1$ should represent all multiples of $2M$. Hence $ML - N^2$ does not exceed the smallest multiple of $2M$ not represented by

$$f_M(u_1, U_2, U_3) = 2Mu_1^2 + MU_2^2 + U_3^2.$$

Since by a well known theorem on determinants the determinant D of Φ_1 is equal to $\frac{1}{2}(ML - N^2)$, we have the following results which we state in a schematic form:

M	$f_M = 2Mu_1^2 + MU_2^2 + U_3^2 \neq 2Mk$	$ML - N^2 \leq 2Mk$	$D \leq$
1	$2u_1^2 + U_2^2 + U_3^2 \neq 14$	≤ 14	≤ 7
2	$4u_1^2 + 2U_2^2 + U_3^2 \neq 56$	≤ 56	≤ 28
3	$6u_1^2 + 3U_2^2 + U_3^2 \neq 30$	≤ 30	≤ 15
4	$8u_1^2 + 4U_2^2 + U_3^2 \neq 56$	≤ 56	≤ 28
5	$10u_1^2 + 5U_2^2 + U_3^2 \neq 50$	≤ 50	≤ 25
6	$12u_1^2 + 6U_2^2 + U_3^2 \neq 120$	≤ 120	≤ 60
7	$14u_1^2 + 7U_2^2 + U_3^2 \neq 98$	≤ 98	≤ 48
8	$16u_1^2 + 8U_2^2 + U_3^2 \neq 224$	≤ 224	≤ 112
9	$18u_1^2 + 9U_2^2 + U_3^2 \neq 126$	≤ 126	≤ 63
10	$20u_1^2 + 10U_2^2 + U_3^2 \neq 200$	≤ 200	≤ 100

Thus in every case the determinant D does not exceed 112.

2. 3. We have just seen that there is but a finite number of classes of classic universal positive quaternary quadratic forms. We inquire next whether the same would be true of forms which, although not universal, do nevertheless represent all even integers. We show that

THEOREM 2. 3. *The determinants of classic positive quaternary quadratic forms which represent all even integers, do not exceed a fixed upper bound B_2.*

Let $\Phi_1(x)$ in (2. 01) represent all even integers. Let a_{11} be the minimum of Φ_1. Then

(2. 31) $$a_{11} \leq 2.$$

Next

$$a_{11}\Phi_1 = \Phi_3 = z_1^2 + \phi_3(z_2, z_3, z_4)$$

where ϕ_3 is given by (2. 02). Let a be the minimum of ϕ_3. Then, it is easily seen that

(2. 32) $$a \leq \beta(a_{11})$$

where $\beta(a_{11})$ may be taken as the least multiple of $2a_{11}$, which is not a square. Proceeding further we see that

$$aa_{11}\Phi_1 = au_1^2 + u_2^2 + \Psi_4(u_3, u_4)$$

where Ψ_4 is given by (2. 12). Let M be the minimum of Ψ_4. Then

(2. 33) $$M \leq \Delta(a_{11}, a)$$

where $\Delta(a_{11}, a)$ may be taken as the least multiple of $2a_{11}a$ which is not represented by $au_1^2 + u_2^2$. Next

$$Maa_{11}\Phi_1 = Mau_1^2 + Mu_2^2 + U_3^2 + (ML - N^2)u_4^2$$

where

(2. 341) $$ML - N^2 = aa_{11}^2D, \qquad D = |\, a_{ij} \,|,$$

and

(2. 342) $$D \leq ML - N^2 \leq B(M, a, a_{11}) \leqq B_2$$

where $B(M, a, a_{11})$ may be taken as a multiple of $2M \cdot a \cdot a_{11}$ which is not represented by

(2. 34) $$Mau_1^2 + Mu_2^2 + U_3^2.$$

We are now ready to prove that B_2 in (2. 342) is an absolute constant.

One may easily verify that $\beta(1) = 2$ and $\beta(2) = 8$. Examining the form $au_1^2 + u_2^2$ we get the following values for $\Delta(a_{11}, a)$ in (2. 33):

a_{11}	1	1	2	2	2	2	2	2	2	2
a	1	2	1	2	3	4	5	6	7	8
$\Delta(a_{11}, a)$	6	20	12	40	24	48	40	48	84	160

To extract the best value of B_2 out of the above inequalities one should determine the best value of $B(M, a, a_{11})$ for each set of values M, a_1, a_{11} permitted by this table. Although this presents no difficulty, the computation is somewhat lengthy and we shall therefore merely prove the existence of such an upper bound. To do this it suffices, in view of the above discussion, to show that in every case the ternary form in (2. 34) will fail to represent a multiple of $2Maa_{11}$. This last follows at once from a result due to Hasse.[3]

3. The canonical form (C_p).

We shall find the following normalization useful in the subsequent discussion.

THEOREM 3. *Every properly primitive classic quaternary quadratic form with integral coefficients and invariants*[4] *o_μ is equivalent to a canonical form*

(3. 01) $$f = \Sigma a_{ij}x_ix_j = x'Ax$$

of determinant $|\, A \,| = |\, a_{ij} \,|$ whose leading principal minors are

$$a_{11} = A_1, \qquad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = o_1A_2, \qquad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = o_1^2o_2A_3$$

[3] Hasse (6a), § 11.

[4] After Minkowski and Smith. We employ the notation of Minkowski.

where

$$(C_p) \qquad A_\mu \text{ or } \tfrac{1}{2}A_\mu \textit{ is an odd prime not dividing } |\,a_{ij}\,|\, A_k A_l$$
$$(\mu, k, l) = (1,2,3),\ (2,1,3),\ (3,1,2).$$

Since our form is properly primitive we may assume at once that a_{11} is an odd prime not dividing $|\,a_{ij}\,|$. Write $o_1{}^2 o_2 A_{ij}$ for the algebraic complement of a_{ij} in $|\,a_{ij}\,|$. Then $F = \Sigma A_{ij} X_i X_j$ is the reciprocal[5] of f. In view of the choice of a_{11} the ternary section $F(0, X_2, X_3, X_4)$ of F is a primitive ternary form of invariants[6]

$$(3.03) \qquad \Omega = o_3 \quad \text{and} \quad \Delta = o_2 a_{11}.$$

This ternary, however, is equivalent to a form whose third coefficient A_{44} $(= A_3)$ and the leading coefficient $(= A_2)$ of whose reciprocal are distinct odd primes not dividing $o_1 o_2 o_3 A_1$ or doubles of such primes.[7] Replacement of the ternary section by this canonical form does not disturb[8] the choice of a_{11}.

4. The associates of a given quadratic form. In this section we assume that our quadratic form (2.01) is a canonical form (C_p). Multiplying through by $a_{11} = A_1$ we obtain

$$(4.01) \qquad A_1 f = X_1{}^2 + o_1 \sum_{i,j=2}^{4} \alpha_{ij}{}^{(1)} x_i x_j,$$

where

$$(4.02) \quad o_1 \alpha_{ij}{}^{(1)} = \begin{vmatrix} a_{11} & a_{1j} \\ a_{i1} & a_{ij} \end{vmatrix} \quad \alpha_{22}{}^{(1)} = A_2, \; X_1 = a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + a_{14}x_4.$$

Next

$$(4.03) \qquad A_2 A_1 f = A_2 X_1{}^2 + o_1 (X_2{}^2 + a_{11} o_2 \sum_{i,j=3}^{4} \alpha_{ij}{}^{(2)} x_i x_j),$$

where, in view of a determinant theorem of Sylvester,

$$(4.04) \quad \begin{vmatrix} \alpha_{22}{}^{(1)} & \alpha_{2j}{}^{(1)} \\ \alpha_{i2}{}^{(1)} & \alpha_{ij}{}^{(1)} \end{vmatrix} = \frac{1}{o_1{}^2} \begin{vmatrix} o_1\alpha_{22}{}^{(1)} & o_1\alpha_{2j}{}^{(1)} \\ o_1\alpha_{i2}{}^{(1)} & o_1\alpha_{ij}{}^{(1)} \end{vmatrix}$$
$$= \frac{a_{11}}{o_1{}^2} \begin{vmatrix} a_{11} & a_{12} & a_{1j} \\ a_{21} & a_{22} & a_{2j} \\ a_{i1} & a_{i2} & a_{ij} \end{vmatrix} = \frac{a_{11} o_1{}^2 o_2 \alpha_{ij}{}^{(2)}}{o_1{}^2} = a_{11} o_2 \alpha_{ij}{}^{(2)}$$

$$(4.05) \qquad \alpha_{33}{}^{(2)} = A_3 \quad \text{and} \quad X_2 = \alpha_{22}{}^{(1)} x_2 + \alpha_{23}{}^{(1)} x_3 + \alpha_{24}{}^{(1)} x_4.$$

Finally

[5] Cf. Dickson (3).

[6] Minkowski (10), Ch. XVIII.

[7] Ross (16). The precise statement of the theorem referred to implies that if Ω, Δ are odd A_2 and A_3 may be taken as odd primes.

[8] Cf. Dickson (3).

$$(4.06) \quad A_3 A_2 A_1 f = A_3 A_2 X_1{}^2 + o_1 A_3 X_2{}^2 + o_1 o_2 A_1 X_3{}^2 + o_1 o_2 o_3 A_1 A_2 X_4{}^2,$$

since

$$(4.07) \quad \begin{vmatrix} \alpha_{33}{}^{(2)} & \alpha_{34}{}^{(2)} \\ \alpha_{43}{}^{(2)} & \alpha_{44}{}^{(2)} \end{vmatrix} = \frac{1}{(o_1{}^2 o_2)^2} \begin{vmatrix} o_1{}^2 o_2 \alpha_{33}{}^{(2)} & o_1{}^2 o_2 \alpha_{34}{}^{(2)} \\ o_1{}^2 o_2 \alpha_{43}{}^{(2)} & o_1{}^2 o_2 \alpha_{44}{}^{(2)} \end{vmatrix}$$
$$= \frac{o_1 \alpha_{22}{}^{(1)}\,|\,A\,|}{o_1{}^4 o_2{}^2} = \frac{A_2 o_1{}^4 o_2{}^2 o_3}{o_1{}^4 o_2{}^2} = o_3 A_2.$$

Here

$$(4.08) \qquad X_3 = \alpha_{33}{}^{(2)} x_3 + \alpha_{34}{}^{(2)} x_4, \quad X_4 = x_4.$$

We now introduce the form

$$(4.09) \quad G(X_1, X_2, X_3, X_4) = A_3 A_2 X_1{}^2 + o_1 A_3 X_2{}^2 + o_1 o_2 A_1 X_3{}^2 + o_1 o_2 o_3 A_1 A_2 X_4{}^2$$

in the independent variables X_1, X_2, X_3, X_4. We shall call G the *associate* of f.

4.1. The form G is of interest by virtue of the following:

THEOREM 4.1. *Let f be a properly primitive quaternary quadratic form. Employ the notation of Theorem 3 and assume that f is in the canonical form of type (C_p). Then if f represents an integer m its associate G in (4.09) represents $A_1 A_2 A_3 m$. Conversely, if the form G represents $A_1 A_2 A_3 m$ and (4.14) and (4.16) hold, then the original form f represents m.*

The first part of the theorem is trivial, for if x_1, x_2, x_3, x_4 are integers, then by (4.02), (4.05), and (4.08), so also are X_1, X_2, X_3, X_4 and $A_1 A_2 A_3 m$ is represented by G in view of (4.06).

Now let $G(X_1, X_2, X_3, X_4) = A_1 A_2 A_3 m$. We seek integers x_1, x_2, x_3, x_4 such that $f(x_1, x_2, x_3, x_4) = m$. We take $x_4 = X_4$. By (4.09),

$$(4.11) \quad A_1 A_2 A_3 m = A_3 A_2 X_1{}^2 + o_1 A_3 X_2{}^2 + o_1 o_2 A_1 X_3{}^2 + o_1 o_2 o_3 A_1 A_2 x_4{}^2,$$

and hence

$$o_1 o_2 A_1 X_3{}^2 + o_1 o_2 o_3 A_1 A_2 x_4 \equiv 0 \pmod{A_3}.$$

But, by (4.07),

$$(4.12) \qquad o_3 A_2 \equiv -[\alpha_{34}{}^{(2)}]^2 \equiv -s^2 \pmod{A_3},$$

whence

$$o_1 o_2 A_1 (X_3{}^2 - s^2 x_4{}^2) \equiv 0 \pmod{A_3}.$$

If

$$(4.14) \qquad (o_1 o_2 A_1, A_3) = 1,$$

then

$$(X_3 - s x_4)(X_3 + s x_4) \equiv X_3{}^2 - s^2 x_4{}^2 \equiv 0 \pmod{A_3},$$

since A_3 is either an odd prime or double such a prime, we have

$$X_3 \equiv s x_4 \quad \text{or} \quad -X_3 \equiv s x_4 \pmod{A_3},$$

whence, replacing s by its value in (4.12), we get

$$\pm X_3 = A_3x_3 + \alpha_{34}{}^{(2)}x_4$$

with integral x_3. Substituting the resulting value of $X_3{}^2$ into (4.11) we get

$$(4.15) \quad A_3A_2A_1m = A_3A_2X_1{}^2 + o_1A_3X_2{}^2 \\ + o_1o_2A_1[(A_3x_3 + \alpha_{34}{}^{(2)}x_4)^2 + o_3A_2x_4{}^2].$$

Replacing o_3A_2 by its value in (4.07), squaring the expression in the parenthesis, combining the similar terms, and dividing both members of (4.15) by the factor A_3 common to all terms, we get

$$(4.151) \qquad A_2A_1m = A_2X_1{}^2 + o_1X_2{}^2 + o_1o_2A_1(\sum_{i,j=3}^{4}\alpha_{ij}{}^{(2)}x_ix_j).$$

This equality, in turn, implies that

$$o_1X_2{}^2 + o_1o_2A_1(\sum_{i,j=3}^{4}\alpha_{ij}{}^{(2)}x_ix_j) \equiv 0 \pmod{A_2}.$$

But, by (4.04),

$$o_2A_1\alpha_{ij}{}^{(2)} \equiv -\alpha_{2i}{}^{(1)}\alpha_{2j}{}^{(1)} \pmod{A_2},$$

and hence

$$o_2A_1\sum_{i,j=3}^{4}\alpha_{ij}{}^{(2)}x_ix_j = o_2A_1(\alpha_{33}{}^{(2)}x_3{}^2 + 2\alpha_{34}{}^{(2)}x_3x_4 + \alpha_{44}{}^{(2)}x_4{}^2) \\ \equiv -[(\alpha_{23}{}^{(1)})^2x_3{}^2 + 2\alpha_{23}{}^{(1)}\alpha_{24}{}^{(1)}x_3x_4 + (\alpha_{24}{}^{(1)})^2x_4{}^2] \\ \pmod{A_2} \\ \equiv -(\alpha_{23}{}^{(1)}x_3 + \alpha_{34}{}^{(1)}x_4)^2 \pmod{A_2}.$$

Thus, (4.151) becomes

$$o_1[X_2{}^2 - (\alpha_{23}{}^{(1)}x_3 + \alpha_{24}{}^{(1)}x_4)^2] \equiv 0 \pmod{A_2}.$$

If

$$(4.16) \qquad (o_1, A_2) = 1,$$

then

$$(X_2 - \alpha_{23}{}^{(1)}x_3 - \alpha_{24}{}^{(1)}x_4)(X_2 + \alpha_{23}{}^{(1)}x_3 + \alpha_{24}{}^{(1)}x_4) \\ = X_2{}^2 - (\alpha_{23}{}^{(1)}x_3 + \alpha_{24}{}^{(1)}x_4)^2 \equiv 0 \pmod{A_2},$$

and since A_2 is a prime or a double of a prime, we have

$$X_2 = A_2x_2 + \alpha_{23}{}^{(1)}x_3 + \alpha_{24}{}^{(1)}x_4 \quad \text{or} \quad -X_2 = A_2x_2 + \alpha_{23}{}^{(1)}x_3 + \alpha_{24}{}^{(1)}x_4,$$

where x_2 is an integer. Substituting the resulting value of $X_2{}^2$ into (4.151), we get

$$(4.17) \qquad A_2A_1m = A_2X_1{}^2 + o_1(A_2x_2 + \alpha_{23}{}^{(1)}x_3 + \alpha_{24}{}^{(1)}x_4)^2 \\ + o_1o_2A_1(\sum_{i,j=3}^{4}\alpha_{ij}{}^{(2)}x_ix_j).$$

Replacing $A_1o_2\alpha_{ij}{}^{(2)}$ by their values in (4.04), squaring the expression in the

parenthesis, combining similar terms, and dividing both members of (4.17) by the factor A_2 common to all terms, we get

$$(4.171) \qquad A_1m = X_1{}^2 + o_1\sum_{i,j=2}^{4}\alpha_{ij}{}^{(1)}x_ix_j.$$

Again, the last equality implies that

$$(4.172) \qquad X_1{}^2 + o_1\sum_{i,j=2}^{4}\alpha_{ij}{}^{(1)}x_ix_j \equiv 0 \pmod{A_1}.$$

But, by (4.02), $o_1\alpha_{ij}{}^{(1)} \equiv -a_{1i}a_{1j} \pmod{A_1}$ and hence

$$o_1\sum_{i,j=2}^{4}\alpha_{ij}{}^{(1)}x_ix_j \equiv -\sum_{i,j=2}^{4}a_{1i}a_{1j}x_ix_j = -(a_{12}x_2 + a_{13}x_3 + a_{14}x_4)^2 \pmod{A_1}.$$

Thus, (4.172) becomes

$$(X_1 - a_{12}x_2 - a_{13}x_3 - a_{14}x_4)(X_1 + a_{12}x_2 + a_{13}x_3 + a_{14}x_4) \\ \equiv X_1{}^2 - (a_{12}x_2 + a_{13}x_3 + a_{14}x_4)^2 \equiv 0 \pmod{A_1}.$$

Since A_1 is a prime, we have

$$X_1 \text{ or } -X_1 = A_1x_1 + a_{12}x_2 + a_{13}x_3 + a_{14}x_4$$

for an integer x_1. Substituting the resulting value of $X_1{}^2$ into (4.171), we get

$$(4.173) \quad A_1m = (A_1x_1 + a_{12}x_2 + a_{13}x_3 + a_{14}x_4)^2 + o_1\sum_{i,j=2}^{4}\alpha_{ij}{}^{(1)}x_ix_j.$$

Replacing $o_1\alpha_{ij}{}^{(1)}$ by their values in (4.02), squaring the expression in the parenthesis, combining similar terms and dividing both members of (4.173) by the factor A_1 common to all terms, we get

$$m = \sum_{i,j=1}^{4}a_{ij}x_ix_j$$

with integral $x_1, \cdots, x_4$. Thus m is represented by f.

FORMS OF ODD DETERMINANTS.

5. A set of sufficient conditions in terms of generic characters. We shall now restrict ourselves to the study of properly primitive forms (2.01) of odd determinants. We shall assume that such a form f is already in a canonical form of type (C_p). Then, since in this case A_1, o_1, o_2, o_3 are all odd, the conditions (4.14) and (4.16) of Theorem 4.1 hold in view of the choice of A_1, A_2, A_3. Thus if the associate G of f represents the multiple $A_1A_2A_3m$ of m then f represents m. Consequently should G represent all integers $\geq K$, and therefore all multiples $A_1A_2A_3m \geq K$ of $A_1A_2A_3$ then f would represent all integers $m \geq K/A_1A_2A_3$. But the form G is of the type considered by Kloosterman (7). We may therefore apply to the form G Kloosterman's conditions 1°-5° assuring representation of all large integers.[9]

We note that A_1 is an odd prime. The same may be assumed in this case of A_2 and A_3 by the proof of Theorem 3.0. Our choice of A_1, A_2, A_3 implies that 4° and 5° hold. Condition 3° becomes

$$o_1 = 1 \tag{5.1}$$

and, if we write ω_2 for an odd prime factor of o_2, condition 2° becomes

(5.21) $(A_2|\omega_2) = (-1|\omega_2)$ or $(A_2|\omega_2) = (-o_3|\omega_2)$, or both, if $\omega_2{}^2 \nmid o_2$ and $\omega_2 \nmid o_3$;

(5.22) $(A_2|\omega_2) = (-1|\omega_2)$, if either (1) $\omega_2{}^2 | o_2$ or (2) $\omega_2 | o_3$;

(5.23) $(-o_3A_2|A_3) = 1, \ (-o_2A_1A_3|A_2) = 1, \ (-A_2|A_1) = 1.$

The condition (5.23) is satisfied by all forms, for, by virtue of (4.07), (4.02) and (4.04), we have

$$-o_3A_2 \equiv (\alpha_{34}{}^{(2)})^2 (\text{mod } A_3), \quad -A_2 \equiv a_{12}{}^2 \ (\text{mod } A_1),$$
$$-o_2A_1A_3 \equiv (\alpha_{23}{}^{(1)})^2 \ (\text{mod } A_2).$$

The condition (5.1) restricts the value of the first invariant o_1 of f. Next, in view of the choice of A_2 and the definition of the generic characters of f, it is clear that the relations (5.21) and (5.22) are in fact conditions upon the generic characters of f with respect to the odd prime factors of o_2.

The condition (5.21) may be modified by virtue of the following considerations. If $(o_3|\omega_2) = -1$, then $(-1|\omega_2)$ and $(-o_3|\omega_2)$ have opposite signs and $(A_2|\omega_2)$ must be equal to one or to the other, and hence at least one (and, of course, only one) of the relations in (5.21) holds true. If, however, $(o_3|\omega_2) = 1$, then $(-1|\omega_2) = (-o_3|\omega_2)$ and the two relations in (5.21) coincide and, therefore, either both hold true or both fail according as $(A_2|\omega_2) = (-1|\omega_2)$ or $(A_2|\omega_2) = -(-1|\omega_2)$. Thus (5.21) may be replaced by

$$(A_2|\omega_2) = (-1|\omega_2) \text{ if } \omega_2{}^2 \nmid o_2, \ \omega_2 \nmid o_3, \ (o_3|\omega_2) = 1. \tag{5.24}$$

The part[10] $(\mu_a, \mu_b, \mu_c, \mu_d) = (0, 0, 0, 0)$ of the condition 1° is in fact the necessary and sufficient condition in order that a form (1.1) with odd coefficients a, b, c, d should fail to represent zero properly modulo 8. In view of the choice of A_1, A_2, A_3 and the formulae (4.02), (4.05), (4.08), the form f in (3.01) and its associate G in (4.09) either both represent zero properly modulo 8 or both fail to do so. The above mentioned conditions

$$a \equiv b \equiv c \equiv d \ (\text{mod } 4) \quad a + b + c + d \equiv 4 \ (\text{mod } 8) \tag{5.25}$$

as applied to G, yield conditions

$$o_1 \equiv o_3 \ (\text{mod } 8), \ o_3A_2 \equiv 1 \ (\text{mod } 4), \ o_2A_1A_3 \equiv 1 \ (\text{mod } 4). \tag{5.26}$$

For, (5.251) becomes $A_3A_2 \equiv o_1A_3 \equiv o_1o_2A_1 \equiv o_1o_2o_3A_1A_2$ (mod 4), and hence $A_2 \equiv o_1$, $A_3 \equiv o_2A_1$, $1 \equiv o_3A_2$ (mod 4). The first and the third of these last congruences imply $o_1 \equiv o_3$ (mod 4). Moreover, (5.252) becomes

$$A_3(A_2 + o_1) + o_1o_2A_1(1 + o_3A_2) \equiv 4 \ (\text{mod } 8).$$

Since $A_2 + o_1 \equiv 2o_1 \equiv 2$ and $1 + o_3A_2 \equiv 2$ (mod 4), each of the two terms above is double an odd integer and the last congruence together with $A_3 \equiv o_2A_1$ (mod 4) implies $A_3(A_2 + o_1) \equiv o_1A_3(1 + o_3A_2)$ (mod 8). Therefore $A_2 + o_1 \equiv o_1 + o_1o_3A_2$ and $1 \equiv o_1o_3$ (mod 8). It is easily seen that conditions (5.26) imply that G satisfies (5.25).

The conditions (5.262) and (5.263) are equivalent to

$$\Psi = (-1)^{\frac{1}{2}(o_3A_2+1) \cdot \frac{1}{2}(o_2A_1A_3+1)} = -1. \tag{5.27}$$

Since the ternary form $F(0, X_2, X_3X_4)$ in Section **3**, has invariants $\Omega = o_2$ and $\Delta = o_2A_1$, and since A_3 and A_2 are represented simultaneously by this ternary and its reciprocal we have[11]

$$\Psi \cdot (A_3|o'_3)(A_2|o'_2A_1) = (-1)^{\frac{1}{2}(o_3+1) \cdot \frac{1}{2}(o_2A_1+1)}.$$

Here $o_i = o_i'o_i''^2$, and $o_i''^2$ is the largest square dividing o_i. In view of (4.02),

$$(A_2|A_1) = (-o_1|A_1) = (-1)^{[(A_1-1)/2] \cdot [(o_1+1)/2]}(A_1|o_1'),$$

and therefore

$$(A_2|o'_2A_1) = (A_2|o'_2)(A_1|o'_1)(-1)^{\frac{1}{2}(A_1-1)\frac{1}{2}(o_1+1)}.$$

Since (5.261) implies that $\frac{1}{2}(o_3 + 1)\frac{1}{2}(o_3A_1 + 1) + \frac{1}{2}(o_1 + 1)\frac{1}{2}(A_1 - 1) \equiv \frac{1}{2}(o_3 + 1)$ modulo 2, we have

$$(A_3|o'_3)(A_2|o'_2)(A_1|o'_1) = \Psi \cdot (-1)^{\frac{1}{2}(o_3+1)} = -(-1)^{\frac{1}{2}(o_3+1)} \tag{5.28}$$

in view of (5.27).

We see that conditions (5.26) are equivalent to (5.261) and (5.28). In view of the choice of A_1, A_2, A_3 condition (5.28) is a restriction upon the generic characters of f.

[9] (7), Section 4.6, p. 453.

[10] Kloosterman (7), p. 453.

[11] Smith, vol. 1, p. 470.

If (5.1) holds, then, in view of (5.261), (5.28) becomes

$$(5.29) \qquad (A_3 | o'_3)(A_2 | o'_2) = 1.$$

Employing the notation of Minkowski,[10] we may state our conclusions in the following form:

THEOREM 5. *Let ϕ be a properly primitive quaternary form of odd determinant and the invariants o_1, o_2, o_3. Let ω_2 be an odd prime factor of o_2. Let finally*

$$(5.1) \qquad o_1 = 1,$$

$$(5.31) \qquad (\phi_2 | \omega_2) = (-1 | \omega_2) \textit{ for } \omega_2 \textit{ such that } \omega_2^2 \nmid o_2 o_3, \ (o_3 | \omega_2) = 1,$$

$$(5.32) \qquad (\phi_2 | \omega_2) = (-1 | \omega_2) \textit{ for } \omega_2 \textit{ such that } \omega_2^2 | o_2 o_3,$$

$$(5.33) \qquad (\phi_3 | o'_3)(\phi_2 | o'_2) = -1, \textit{ if } o_3 \equiv 1 \pmod 8.$$

Then the form ϕ represents all but a finite number of integers.

The truth of this theorem follows at once from the fact that conditions (5.1), (5.31)-(5.33) imply that (5.1), (5.22)-(5.24) but not (5.26) hold for the associate G of a canonical form f of type (C_p) in the class of ϕ and hence G represents all but a finite number of integers.

6. The necessity of conditions (5.1) and (5.32).

We ask now if the conditions (5.1), (5.31), (5.32), (5.33) are necessary in order that ϕ should represent all integers with but a finite number of exceptions. We find at once that (5.1) and (5.32) are necessary. For, should there be an odd prime divisor $\omega_1 > 1$ of o_1, ϕ would not represent integers m such that

$$(6.1) \qquad (m, \omega_1) = 1, \qquad (m | \omega_1) = -(\phi_1 | \omega_1).$$

(in view of (4.11)). Next, suppose that (5.32) should fail. Then $(\phi_2 | \omega_2) = -(-1 | \omega_2)$. First let $\omega_2^2 | o_2$. Then, in view of (4.11), with $o_1 = 1$, and the choice of A_2, A_1, ϕ would not represent integers m such that

$$(6.2) \qquad m = \omega_2 m_1, \qquad (m_1, \omega_2) = 1.$$

Next let $\omega_2^2 \nmid o_2$, but $\omega_2 | o_3$. Then by (4.11), with $o_1 = 1$, ϕ would not represent integers m such that

$$(6.3) \quad m = \omega_2 m_1, \ (m_1, \omega_2) = 1, \ (m_1 | \omega_2) = -(\phi_3 | \omega_2)(\phi_2 | \omega_2)(\bar{o}_2 | \omega_2),$$

where $o_2 = \omega_2 \bar{o}_2$.

One sees without any difficulty that there are infinitely many integers of any one of the types (6.1), (6.2), and (6.3).

7. The conditions (5.31) and (5.33).

The condition (5.31) differs essentially from (5.1) and (5.32). Its failure does not directly imply that there is an infinity of integers not represented, but rather that *if there is one integer not represented, then there is an infinity of such integers.* More precisely: let ϕ, and therefore f, represent an integer $\omega_2^2 m$ where ω_2 is an odd prime factor of o_2 such that

$$(7.1) \qquad \omega_2^2 \nmid o_2 o_3, \ (o_3 | \omega_2) = 1 \ \text{ and } \ (\phi_2 | \omega_2) = -(-1 | \omega_2).$$

Then the condition (5.31), and hence (5.24), fails and we have

$$(7.11) \qquad (A_2 | \omega_2) = -(-1 | \omega_2) \ \text{ and } \ (A_2 | \omega_2) = -(-o_3 | \omega_2).$$

Since $A_1 A_2 A_3 \omega_2^2 m$ is represented by G we have, in view of (4.11) with $o_1 = 1$,

$$A_3 A_2 X_1^2 + A_3 X^2 \equiv 0 \pmod{\omega_2},$$

and, since $(A_3, w_2) = 1$,

$$A_2 X_1^2 + X_2^2 \equiv 0 \pmod{\omega_2}.$$

Therefore, by (7.11_1) $X_1 \equiv X_2 \equiv 0 \pmod{\omega_2}$. Replacing X_1 and X_2 by $\omega_2 X'_1$ and $\omega_2 X'_2$ respectively, in (4.11), and dividing every term of both members of this equality by ω_2, we see that

$$\bar{o}_2 A_1 X_3^2 + \bar{o}_2 o_3 A_1 A_2 X_4^2 \equiv 0 \pmod{\omega_2},$$

and, since $(\bar{o}_2 A_1, \omega_2) = 1$,

$$X_3^2 + o_3 A_2 X_4^2 \equiv 0 \pmod{\omega_2}.$$

But by (7.11_2), $(-o_3 A_2 | \omega_2) = -1$, and hence $X_3 \equiv X_4 \equiv 0 \pmod{\omega_2}$. Write $X_3 = \omega_2 X'_3$, $X_4 = \omega_2 X'_4$. Then, dividing once more every term of both members of (4.11) by ω_2, we get

$$A_1 A_2 A_3 m = G(X'_1, X'_2, X'_3, X'_4).$$

Thus G represents $A_1 A_2 A_3 m$, and hence f, and therefore ϕ represents m. It follows, therefore, that if a form ϕ should not fulfil condition (5.31) then if it does not represent an integer m it also does not represent $\omega_2^2 m$ and in general $\omega_2^{2\kappa} m$ for every integer κ. This proves the above statement in italics. It is seen then that *such a form ϕ either represents all integers or there are infinitely many integers not represented by ϕ.* We shall speak of the set of integers of the form $\omega_2^{2\kappa} m$ as the *tower* $\omega_2^{2\kappa} m$ or the tower generated by ω_2 and m.

In view of the discussion preceding the statement of Theorem 5, the failure of condition (5.33) implies that if f does not represent an *even* integer

$2m$, then it does not represent the whole tower $2^{2\kappa+1}m$, that is, it does not represent an infinity of integers.

8. Forms representing all large integers and not covered by Theorem 5. Such forms may be divided into two types. Type P_1, for which (5.31) does not hold, and type P_3 for which (5.31) holds true but (5.33) fails to hold.

Forms of type P_3 must represent all even integers. For, if such a form fails to represent an even integer $2m$ then it fails to represent the whole tower $2^{2\kappa+1}m$. In view of Theorem 2.3, the determinant of such a form does not exceed B_2. Thus, there is only a finite number of classes of forms of type P_3.

Forms of type P_1 must represent all integers. For, if such a form fails to represent an integer m then it fails to represent the whole tower $\omega^{2\kappa}m$. Therefore, by Theorem 2.0, the determinant of such a form does not exceed 112.

We shall determine all forms of type P_1. The only odd determinants $D < 112$ which permit such forms are given together with the desired invariants o_2, o_3 ($(o_3|\omega_2) = 1$) by the following table.

(8.01)

D	9	63	25	49
$\omega_2 = o_2$	3	3	5	7
o_3	1	7	1	1

Since every form ϕ under consideration which does not represent 1 also does not represent $\omega_2^{2\kappa}$, we need consider only forms which represent 1. Such forms are equivalent to

$$(8.02)\quad \phi = \xi^2 + ax^2 + by^2 + cz^2 + 2ryz + 2sxz + 2txy = \xi^2 + \mu(x, y, z).$$

If ϕ is a form of one of the determinants given in the table (8.01) and if it possesses the indicated invariants o_2 and o_3 then $\mu(x, y, z)$ is a properly primitive form with invariants $\Omega = o_2$ and $\Delta = o_3$ and odd determinant $\Omega^2\Delta = o_2{}^2 o_3 = D$. Since (7.1) holds, we have

$$(8.03)\qquad (\mu|\omega_2) = -(-1|\omega_2)$$

for the generic character $(\mu|\omega_2)$ of μ. For, if we choose a to be any integer prime to ω_2 and properly represented by μ then, in view of (8.02),

$$(\phi_2|\omega_2) = (a|\omega_2) = (\mu|\omega_2).$$

We may assume next that μ in (8.02) is a reduced form and we need to consider all forms (8.02) in which μ is a reduced form of the above mentioned invariants and genus satisfying (8.03). We list such forms in the following table.

D	$\Omega = \omega_2$	Δ		a	b	c	r	s	t	$(\mu\|\omega_2)$	$(-1\|\omega_2)$
9	3	1	$\mu^{(1)}$	1	3	3	0	0	0	1	-1
25	5	1	$\mu^{(2)}$	2	3	5	0	0	-1	-1	1
49	7	1	$\mu^{(3)}$	1	7	7	0	0	0	1	-1
			$\mu^{(4)}$	2	4	7	0	0	-1		
63	3	7	$\mu^{(5)}$	1	3	21	0	0	0	1	-1
			$\mu^{(6)}$	1	6	12	-3	0	0		
			$\mu^{(7)}$	3	3	7	0	0	0		

We write

$$\phi^{(i)} = \xi^2 + \mu^{(i)} \qquad (i = 1, \cdots, 7).$$

Each of the forms $\phi^{(1)}, \cdots, \phi^{(7)}$ satisfies the conditions (5.1), (5.32), but not the condition (5.31). Hence each of these forms either represents all integers or fails to represent an infinite number of integers (Cf. 7). One sees at once that

$$(8.1)\qquad \phi^{(3)} \neq 3,\quad \phi^{(5)} \neq 6,\quad \phi^{(6)} \neq 3,\quad \phi^{(7)} \neq 2,$$

and therefore these forms belong to the second category, i.e., they do not represent an infinity of integers. The form $\phi^{(1)} = \xi^2 + x^2 + 3y^2 + 3z^2$ as is well known,[12] represents all integers. Consider next the form

$$\phi^{(2)}(\xi, x, y, z) = \xi^2 + 2x^2 + 3y^2 + 5z^2 - 2xy.$$

Its ternary section $\psi = \phi(\xi, x, y, 0) = \xi^2 + 2x^2 + 3y^2 - 2xy$ belongs to a genus of one class[13] of determinant 5. Its invariants are $\Omega = 1$, $\Delta = 5$, and its character is

$$(\Psi|5) = (2|5) = -1 = -(-\Omega|5)$$

where Ψ is the reciprocal of ψ. Therefore[14] integers not represented by ψ are

$$(8.11)\qquad 5^{2\kappa+1}(5n+1),\quad 5^{2\kappa+1}(5n+4).$$

In order to prove that $\phi^{(3)}$ represents all integers we need only prove that it represents all integers of the form (8.11). But these integers are represented by the ternary section $\phi^{(2)}(\xi, x, 0, z) = \xi^2 + 2x^2 + 5z^2$ which represents all integers not of the form[15] $5^{2k+1}(5n+2)$, $5^{2k+1}(5n+3)$ and hence all integers of the form (8.11). Thus $\phi^{(2)}$ represents all integers.

Finally, consider the form

$$\phi^{(4)} = \xi^2 + 2x^2 + 4y^2 + 7z^2 - 2xy.$$

[12] Ramanujan (14), Dickson (4), pp. 111-113.

[13] Jones (6), Borissow (1).

[14] Ross (17), Lemmas 1-3.

[15] Ramanujan (14), Dickson (4), pp. 111-113.

Since $2\phi^{(4)} = 2\xi^2 + (2x - y)^2 + 7y^2 + 14z^2$, the form $\phi^{(4)}$ will represent all integers if

$$\psi^{(4)} = X^2 + 2\xi^2 + 7y^2 + 14z^2$$

will represent all even integers. The ternary section

$$(8.12) \qquad X^2 + 2\xi^2 + 7y^2$$

represents[16] all even integers $\equiv 0$ or $1 \pmod 3$ which are not of the form

$$(8.13) \qquad 7^{2\kappa+1}(14m + R)\,; \qquad R = 10,\ 12, \text{ and } 6.$$

If an integer is $\equiv 0$ or $1 \pmod 3$ and is of the form (8.13), we need concern ourselves only with those of type $L = 7(14m + R)$. Since at least one of the integers

$$L - 14 \cdot 3^2 = 7[14(m-1) + (R-4)]$$

or

$$L - 14 \cdot 6^2 = 7[14(m-5) + (R-2)]$$

is not of the form (8.13) and neither one is $\equiv 2 \pmod 3$, one of them is represented by (8.12), and hence L, and therefore $7^{2\kappa}L$, is represented by $\phi^{(4)}$.

Finally, let an integer be of the form $3n + 2$. If $z \not\equiv 0 \pmod 3$ then $3n + 2 - 14z^2 \equiv 3n + 2 - 2 \equiv 0 \pmod 3$. We may again assume that $7^2 \nmid 3n + 2$. If $(7, 3n + 2) = 1$, then $3n + 2 - 14$ is not of the form (8.13) and hence is represented by (8.12). If $7 | 3n + 2$, then

$$3n + 2 = 7(14m + M), \qquad M \not\equiv 0 \pmod 7.$$

In this case at least one of the integers

$$7(14m + M) - 14 = 7[14m + (M-2)],$$
$$7(14m + M) - 14 \cdot 2^2 = 7[14m + (M-8)],$$

or

$$7(14m + M) - 14 \cdot 4^2 = 7[14(m-2) + (M-4)]$$

is not of the form (8.13). The only numbers for which the above differences are negative, are ≤ 560 and are easily seen to be represented by $\phi^{(4)}$. Thus $\phi^{(4)}$ represents all integers.

We may now supplement Theorem 5 by

THEOREM 8. *Except for forms given in Theorem 5, there is only a finite number of classes of forms of odd determinants representing all large integers. These consist of a finite number of classes of forms of type P_3 and exactly three classes of type P_1, viz., the three classes containing $\phi^{(1)}$, $\phi^{(2)}$ and $\phi^{(4)}$. The classes to which $\phi^{(1)}$ and $\phi^{(2)}$ belong may be completely described by their generic invariants, for they are the only classes in their respective genera.*[17] *This is not true of the class of $\phi^{(4)}$.*

[16] Pall (12).

9. One observes that $\phi^{(3)} = \xi^2 + \mu^{(3)}$ and $\phi^{(4)} = \xi^2 + \mu^{(4)}$ (Cf. the table in **8**) do not represent the same large integers even though they belong to the same genus. For, $\phi^{(4)}$ represents all large integers, whereas $\phi^{(3)}$ does not represent integers in the tower $3 \cdot 7^{2\kappa}$. Similarly the forms $\phi^{(5)}$, $\phi^{(6)}$, $\phi^{(7)}$ do not represent the same large integers in view of (8.1). It appears that when a quaternary form f fails to represent zero properly modulo p^a where $a \geq 2$ and p is a prime, then the behavior of f for large integers depends not only upon the values of its generic invariants but also upon its accidental behavior for small values of the variables. For, should f fail to represent a small integer $p^\nu m$, it would not represent the whole tower $mp^{2\kappa+\nu}$. In our case when $p = \omega_2$ then $\nu = 0$ and when $p = 2$ then $\nu = 1$.

The failure of (5.31) or (5.33) implied that our form was not a zero form modulo $\omega_2{}^2$ or modulo 8 respectively.

ST. LOUIS UNIVERSITY.

BIBLIOGRAPHY.

1. E. Borissow, *Reduction of Positive Ternary Quadratic Forms by Selling's Method, with a Table of Reduced Forms for all Determinants from 1 to 200*, St. Petersburg (1890), pp. 1-108; tables 1-116. (Russian).

2. L. E. Dickson, *American Journal of Mathematics*, vol. 49 (1927), pp. 39-56.

3. ———, *Studies in the Theory of Numbers*, University of Chicago Press, 1930.

4. ———, *Modern Elementary Theory of Numbers*, University of Chicago Press, 1939.

5. Jaçobi, *Werke*, vol. 6, pp. 281-302.

6. B. W. Jones, *A Table of Eisenstein—reduced Positive Ternary Quadratic Forms of determinant* $\leqq 200$, (1935), Bulletin No. 97 of the National Research Council.

6a. H. Hasse, "Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen," *Journal für Mathematik*, vol. 152 (1923), pp. 205-224.

7. H. D. Kloosterman, *Acta Mathematica*, vol. 49 (1926), pp. 454-464.

8. J. L. Lagrange, *Oeuvres*, vol. 3 (1869), pp. 189-201.

9. J. Liouville. See, for example, *Journal de Mathématiques* (2), vol. 1 (1856), p. 230.

[17] Townes (20).

10. H. Minkowski, "Grundlagen für eine Theorie der quadratischen Formen," *Werke*, Bd. 1, pp. 3-144.

11. D. C. Morrow, *University of Chicago Thesis*, 1928.

12. G. Pall, *Bulletin of the American Mathematical Society*, vol. 46 (1940), p. 291.

13. T. Pepin, *Atti Accad. Pont. Nuovi Lincei*, vol. 38 (1884-5), pp. 171-196, and elsewhere.

14. S. Ramanujan, *Proceedings of the Cambridge Philosophical Society*, vol. 19, I. (1916), pp. 11-21. Also *Collected Papers*, pp. 169-178. Cf. also Dickson (4), pp. 104-5. It was first pointed out by Dickson that one of the 55 forms originally listed by Ramanujan was not universal.

15. A. E. Ross, *Proceedings of the National Academy of Sciences*, vol. 18 (1932), pp. 600-608.

16. ———, *Bulletin of the American Mathematical Society*, vol. 45 (1939), pp. 899-906.

17. ———, *American Journal of Mathematics*, vol. 55 (1933), pp. 293-302.

18. H. J. S. Smith, *Collected Papers*.

19. W. A. Tartakowsky, *Bull. Ak. Sc. U. R. S. S.*, vol. 7 (1929), pp. 111-122, 165-196.

20. S. B. Townes, *Annals of Mathematics*, vol. 41 (1940), pp. 57-58.

21. H. W. Turnbull, *The Theory of Determinants, Matrices, and Invariants.*

THE COMPLETION OF A PROBLEM OF KLOOSTERMAN.*

By Gordon Pall.

1. Introduction. The Euler-Lagrange proof of the theorem that every positive integer is a sum of four squares employed the fact that the form $x^2 + y^2 + z^2 + t^2$ is multiplicative. Hence Liouville [1] [1] examined the multiplicative forms $x^2 + ay^2 + bz^2 + abt^2$, and found the positive integers a, b, for which these forms represent all positive integers. Ramanujan [2] examined in similar fashion the forms

$$(1) \qquad f = (a, b, c, d) = ax^2 + by^2 + cz^2 + dt^2,$$

where a, b, c, d are positive integers, and $a \leqq b \leqq c \leqq d$. He found that there are 54 such forms which represent all positive integers; actually he had 55, and Dickson later pointed out his error [3]. More recently, Halmos found the 88 such forms which represent all positive integers with one exception [4].

Ramanujan, in the spirit of the analytic number theory which was then becoming popular, proposed and partly solved the more interesting problem of determining all forms (1) which represent all but a finite number of positive integers. Kloosterman [5] later solved this problem of Ramanujan, save that he was unable to decide whether the four forms

$$(2) \qquad (1, 2, 11, 38), \quad (1, 2, 17, 34), \quad (1, 2, 19, 22), \quad (1, 2, 19, 38)$$

represent all positive integers. In **11-13** we shall complete the problem by showing that these four forms do in fact represent all large integers. The technique used for this purpose is based on the fact that quadratic forms in the same genus have rational transformations into one another, which can be employed in particular cases to investigate the numbers represented integrally by the individual forms. Earlier similar attempts by the writer (6) failed because he did not then realize that Kloosterman's asymptotic formula could be adapted to settle the problem for numbers involving a limited power of 2, so that it is only necessary to consider, say, multiples of 4.

However, the most interesting feature of this paper consists in the elegant formulation of the conditions for a form to represent all large integers. This

* Received July 17, 1945.

[1] Numbers in square brackets refer to the references at the end of the paper.

formulation we owe largely to reading a manuscript of Arnold E. Ross, in which he considers the extension of Kloosterman's results to non-diagonal forms. Also, whereas much earlier work on quadratic forms is complicated by many cases involving the numerous invariants of the forms, we obtain our results here directly and simply by appealing to the arithmetical properties of the forms themselves. Although our Theorems 1, 2, and 4 are true, precisely as stated, for non-diagonal forms as well, this will not be proved here.

2. The pertinent properties of f. If f is to represent all large integers, then evidently the congruence $f \equiv n \pmod{k}$ must be solvable in integers x, y, z, t, for every pair of integers n and k, $k \neq 0$. If p is any prime we shall say that f *is p-adically universal,* when

$$ax^2 + by^2 + cz^2 + dt^2 \equiv n \pmod{p^r}, \tag{3}$$

is solvable in integers x, y, z, and t, for every n and r, $r \geqq 0$. Hence a necessary condition for f to represent all large integers is that f be p-adically universal for every p.

We shall later (Lemma 1) give precise criteria for such universality, as also (Lemma 2) for p-adic representation of zero.

We shall say that f *fails to represent zero p-adically,* if

$$ax^2 + by^2 + cz^2 + dt^2 \equiv 0 \pmod{p^r} \tag{4}$$

implies, for some r, that $x \equiv y \equiv z \equiv t \equiv 0 \pmod{p}$. If, however, (4) is solvable for every positive integer r in integers x, y, z, t not all divisible by p, we say that f *represents zero p-adically.* The connection with our problem is this. If f fails to represent zero p-adically for some p, suppose for a certain s, that $f \equiv 0 \pmod{p^s}$ implies $x \equiv y \equiv z \equiv t \equiv 0 \pmod{p}$. Then the number of representations of $p^{s+2k}n$ is the same as that of $p^s n$ in f, for every positive integer k. Hence *if* f does not represent one integer of the form $p^s n$, f does not represent infinitely many integers. And in any case the number of representations of the *large* number p^{s+2k} is bounded, so that, in the asymptotic formula soon to be encountered, $\chi(p, p^{s+2k})$ is near zero when k is large.

3. The principal theorems. Kloosterman's results are expressed in rather complicated fashion in terms of conditions on the coefficients of f. Interpreting his results by means of the notions of **2**, and using Lemmas 1 and 2, we get the following two theorems.

THEOREM 1. *If* (a) *f is p-adically universal for every p, and* (b) *f represents zero p-adically for every p, then f represents all sufficiently large integers.*

It will be observed that (a) is a necessary, and (b) is not a necessary condition.

THEOREM 2. *Of the forms f which are p-adically universal for every p, there are only a finite number of forms which fail to represent zero p-adically for some prime p_1, and yet represent all large integers.*

We shall in fact prove

THEOREM 3. *There are precisely* 199 *forms which fail to represent zero p-adically for some p_1, and yet represent all large integers. They are as follows, the first two having $p_1 = 3$ and 5, the others $p_1 = 2$:*

(A) $(1, 1, 3, 3)$;
(B) $(1, 2, 5, 10)$;
(C) $(1, 1, 5, 5)$, *and* $(1, 1, 1, t)$ $(t = 1, 9, 17, 25)$;
(D) $(1, 4, 5, 5)$, $(1, 1, 5, 20)$, $(1, 1, 4, t)$, $(1, 1, 1, 4t)$;
(E) $(1, 1, 10, 10)$, $(2, 2, 5, 5)$, $(1, r, 2, 2t)$, $(1, 17, 2, 2s)$, *and* $(1, 25, 2, 2r)$, $(r = 1, 9;\ s = 1, 9, 17)$;
(F) $(1, 1, 10, 40)$, $(5, 5, 2, 8)$, $(1, r, 2, 8t)$, $(1, r, 8, 2t)$, $(1, 17, 2, 8s)$, $(1, 17, 8, 2s)$, $(1, 25, 2, 8r)$, $(1, 25, 8, 2r)$;
(G) $(1, 4, 10, 10)$, $(2, 2, 5, 20)$, $(1, 4r, 2, 2t)$, $(4, r, 2, 2t)$, $(1, 68, 2, 2s)$, $(4, 17, 2, 2s)$, $(1, 100, 2, 2r)$, $(4, 25, 2, 2r)$;
(H) $(1, 4, 10, 40)$, $(2, 8, 5, 20)$, $(1, 4r, 2, 8t)$, $(1, 4r, 8, 2t)$, $(4, r, 2, 8t)$, $(4, r, 8, 2t)$, $(1, 68, 2, 8s)$, $(1, 68, 8, 2s)$, $(4, 17, 2, 8s)$, $(4, 17, 8, 2s)$, $(1, 100, 2, 8r)$, $(1, 100, 8, 2r)$, $(4, 25, 2, 8r)$, $(4, 25, 8, 2r)$;
(I) $(1, u, 2, 2v)$, $u, v = 3, 11$, *and* 19;
(J) $(1, 4u, 2, 2v)$, $(4, u, 2, 2v)$;
(K) $(1, u, 2, 8v)$, $(1, u, 8, 2v)$;
(L) $(1, 4u, 2, 8v)$, $(1, 4u, 8, 2v)$, $(4, u, 2, 8v)$, $(4, u, 8, 2v)$.

Furthermore, we shall give in **4** a surprisingly easy proof of a theorem of which Theorem 1 is obviously a corollary:

THEOREM 4. *Let n denote any integer such that $f \equiv n \pmod{k}$ is solvable for every modulus k. For each prime p such that f fails to represent zero p-adically, impose an upper bound to the power of p in n. Then f represents every sufficiently large n (> 0) thus restricted.*

3a. Modification of the asymptotic formula. Kloosterman's formula [7] for the number of representations $f(n)$ of n by f is

$$(5) \qquad f(n) = \frac{\pi^2}{(abcd)^{1/2}} nS(n) + O(n^{17/18+\epsilon}).$$

To prove that $f(n) > 0$ for n large, it suffices to show that

$$(6) \qquad S(n) > K/\log\log n,$$

where K is a positive constant depending only on f and the positive number ϵ. Kloosterman expresses $S(n)$ as a product over all primes p, namely

$$(7) \qquad S(n) = \prod_p \chi(p),$$

$$(8) \qquad \chi(p) = \chi(p, n) = 1 + A(p) + A(p^2) + \cdots,$$

$$(9) \qquad p^{4r}A(p^r) = \sum_h \sum_{x,y,z,t} \exp[2\pi i h(ax^2 + by^2 + cz^2 + dt^2 - n)/p^r],$$

where x, y, z, t range over all residues mod p^r, and h over all such residues prime to p. To put $\chi(p)$ into a more significant form, note that if $r \geqq 1$, the right member of (9) is

$$\begin{aligned} &\sum_{h,x,y,z,t \bmod p^r} \exp[2\pi i h(ax^2 + by^2 + cz^2 + dt^2 - n)/p^r] \\ &\qquad - p^4 \sum_{h_1,x,y,z,t \bmod p^{r-1}} \exp[2\pi i h_1(ax^2 + by^2 + cz^2 + dt^2 - n)/p^{r-1}] \\ &\qquad = p^r f(n, p^r) - p^{r+3} f(n, p^{r-1}), \end{aligned}$$

where $f(n, k)$ denotes the number of solutions of

$$(10) \qquad f(x, y, z, t) \equiv n \pmod k.$$

Hence

$$(11) \qquad \chi(p) = \lim_{r \to \infty} p^{-3r} f(n, p^r),$$

where it should be observed that if p^δ is the precise power of p in the determinant of f, $p^{-3r}f(n, p^r)$ is independent of r if $r \geqq \delta + 3$ [8]. This interesting form of expression for $\chi(p)$ will be found in a paper by Tartakowsky [9], and in the work of Siegel.

We note that it is easy to prove by (11) that

$$(12) \qquad \text{if } p \nmid 2abcd, \qquad \chi(p) = (1 - \epsilon_1 p^{-2}) \sum_{j=0}^{\nu} \epsilon_1^j p^{-j},$$

where $\epsilon_1 = (abcd \mid p)$, $n = p^\nu n_1$, n_1 prime to p.

A sketch of Kloosterman's application of (5) is now in order. He proves easily that the product of the $\chi(p)$ over all primes save the finite number dividing $2abcd$, exceeds $K/\log\log n$ [10]. He then narrows the problem to forms whose coefficients satisfy certain conditions. Comparison with our Lemma 1 will show that these are the conditions for f to be universal for every p. Next, confining himself to such forms, he shows that for primes of a special kind, which by our Lemma 2 we now recognize as those for which f fails to represent zero p-adically, $\chi(p)$ is so near zero when n is divisible by a high power of p that (6) will not hold. This is to be expected from the last observation of **2**.

4. Proof of Theorem 4. We shall formulate the proof so as to apply to any m-ary quadratic form f for which a formula like (5) holds; $\chi(p)$ is then $\lim p^{-(m-1)r} f(n, p^r)$. Except possibly when $p = 2$ (see below) any f can be expressed modulo p^r as a sum of terms $p^{\alpha_i} a_i x_i^2$, say

$$(13) \qquad \begin{aligned} &f \equiv p^{\alpha_1} a_1 x_1^2 + \cdots + p^{\alpha_m} a_m x_m^2, \\ &0 \leqq \alpha_1 \leqq \alpha_2 \leqq \cdots \leqq \alpha_m, \qquad a_1 \cdots a_m \text{ prime to } p. \end{aligned}$$

To prove the theorem it is evidently sufficient to show that $\chi(p)$ is bounded away from zero for all large n, for each prime p dividing the determinant of f, and for the prime $p = 2$.

Case 1. Suppose n to be such that $f \equiv n \pmod{p^{\alpha_m+3}}$ is solvable with some x_i prime to p. We shall prove that $\chi(p) \geqq p^{-(m-1)(\alpha_m+3)}$. For, proceeding by induction, suppose $r \geqq \alpha_m + 3$ and that $f \equiv n \pmod{p^r}$ is solvable with, say, x_3 prime to p. The residues $x_1, x_2, x_4, \cdots, x_m \pmod{p^r}$ expand into p^{m-1} sets of residues mod p^{r+1}. For each of these we can choose h so that if x_3 is replaced by $x_3 + p^{r-\alpha_3}h$ if $p > 2$, or by $x_3 + 2^{r-\alpha_3-1}h$ if $p = 2$, then $f \equiv n \pmod{p^{r+1}}$ [11]. By repetitions of this process we see that $f \equiv n \pmod{p^r}$ has at least $p^{(m-1)(r-\alpha_m-3)}$ solutions, if $r \geqq \alpha_m + 3$. Hence $\chi(p) \geqq p^{-(m-1)(\alpha_m+3)}$.

Case 2. Let the power p^ν of p in n be bounded. Then if $f \equiv n \pmod{p^r}$ has p^ρ dividing every x_i but not $p^{\rho+1}$, then $2\rho \leqq \nu$ and the number of solutions of $f \equiv n \pmod{p^r}$ is $p^{m\rho}$ times the number of solutions of $f \equiv n/p^{2\rho} \pmod{p^{r-2\rho}}$. Hence by Case 1,

$$f(n, p^r) \geqq p^{m\rho} p^{(m-1)(r-2\rho-\alpha_m-3)}, \qquad \chi(p) \geqq p^{-\frac{1}{2}(m-2)\nu-(m-1)(\alpha_m+3)}.$$

Case 3. Finally, let f represent zero p-adically. The fact that $\chi(p)$ is bounded away from zero follows from Case 2 if $p^{a_m+3} \nmid n$. Let then $p^{a_m+3} | n$ Now, $f \equiv 0 \pmod{p^{a_m+3}}$ is solvable with an x_i prime to p. Hence $f \equiv n \pmod{p^{a_m+3}}$ is similarly solvable, and Case 1 applies.

Although not needed in this article the remaining case with $p = 2$ will be resolved. We then have $f \equiv 2^a(jx_1^2 + x_1x_2 + jx_2^2) +$ terms in other variables $(\text{mod } 2^r)$, and $j = 0$ or 1. Hence, if $f \equiv n \pmod{2^r}$ is solvable with (say) x_1 odd, and $s \geqq \alpha + 1$, we can replace x_1 by $x_1 + 2^{s-a}h$ and x_2 by $x_2 + 2^{s-a}k$, and obtain $f \equiv n \pmod{2^{s+1}}$ if $2^sQ + 2^s(hx_2 + kx_1) \equiv 0 \pmod{2^{s+1}}$, where Q denotes an integer; i. e. with arbitrary h and unique k mod 2; thus again there are 2^{m-1} times as many solutions of $f \equiv n \pmod{2^{s+1}}$ as of $f \equiv n \pmod{2^s}$, with *any* x_i odd; and $\chi(2) \geqq 2^{-(m-1)(a+1)}$.

This completes the proof of Theorem 4, hence of Theorem 1.

5. The criteria for p-adic universality and representation of zero. For any prime p we can number the variables so that (13) holds, with $m = 4$. Detailed proofs of the following three lemmas will be found in a forthcoming book by the author. Since their verification is not difficult we leave it to the reader, noting merely that the easiest proof of Lemma 2 amounts to a direct application of the conditions of Hasse [12] for p-adic representation of zero in rationals x_i.

LEMMA 1. *If $p > 2$, f is p-adically universal if and only if*

$$(14) \quad \alpha_1 = \alpha_2 = 0; \textit{ and either } \alpha_3 = 0 \textit{ or } (-a_1a_2|p) = 1 \textit{ or } \alpha_3 = \alpha_4 = 1.$$

If $p = 2$, the necessary and sufficient condition is:

$$(15) \qquad \alpha_1 = 0,\ \alpha_2 = 0 \textit{ or } 1,\ \alpha_3 - \alpha_2 = 0 \textit{ or } 1;$$

$$(16) \qquad \textit{if } \alpha_2 = 0, \textit{ then either } \alpha_4 - \alpha_3 \leqq 2 \textit{ or } c^*_2 = 1;$$

$$(16) \qquad \textit{if } \alpha_2 = 1, \textit{ then either } \alpha_4 - \alpha_3 \leqq 1 \textit{ or } c^*_2 = 1.$$

Here c^*_2 denotes the unit

$$c^*_2 = (2|a_1a_2)^{a_3}(2|a_1a_3)^{a_2}(-1)^{\frac{1}{2}(a_1a_2+1)\cdot\frac{1}{2}(a_1a_3+1)}.$$

We may observe that c^*_2 is the invariant Ψ of Smith [13], or the invariant c_2 of Hasse, for the ternary form $g = a_1x_1^2 + 2^{a_2}a_2x_2^2 + 2^{a_3}a_3x_3^2$. It has the property that if $c^*_2 = 1$, then g represents zero 2-adically, and f does likewise.

LEMMA 2. *If $p > 2$ and (14) holds, then f fails to represent zero p-adically, if and only if*

$$(17) \quad \alpha_1 = \alpha_2 = 0,\ \alpha_3 = \alpha_4 = 1,\ (-a_1a_2|p) = -1 = (-a_3a_4|p).$$

If $p = 2$ and (15) holds, then f fails to represent zero p-adically if and only if $a_1a_2a_3a_4 \equiv 1 \pmod 8$ and any of the following cases (18)-(23) holds:

$$(18) \quad \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0, \quad a_1 \equiv a_2 \equiv a_3 \equiv a_4 \pmod 4;$$

$$(19) \quad \alpha_1 = \alpha_2 = 0,\ \alpha_3 = \alpha_4 = 1, \textit{ and}$$

either (i) $a_1 \equiv a_2$, $a_3 \equiv a_4 \pmod 8$, $a_1 \equiv a_3 \pmod 4$,
or (ii) $a_1 \equiv 5a_2$, $a_3 \equiv 5a_4 \pmod 8$, $a_1 \equiv -a_3 \pmod 4$,
or (*iii*) $a_1 \equiv 3a_2$, $a_3 \equiv 3a_4 \pmod 8$;

$$(20) \quad \alpha_1 = \alpha_2 = \alpha_3 = 0,\ \alpha_4 = 2,\ a_1 \equiv a_2 \equiv a_3 \equiv a_4 \pmod 4;$$

$$(21) \quad \alpha_1 = \alpha_2 = 0,\ \alpha_3 = 1,\ \alpha_4 = 3, \textit{ and three cases as in } (19);$$

$$(22) \quad \alpha_1 = 0,\ \alpha_2 = \alpha_3 = 1,\ \alpha_4 = 2, \textit{ and the three cases of } (19) \textit{ with subscripts in the order } 1423;$$

$$(23) \quad \alpha_1 = 0,\ \alpha_2 = 1,\ \alpha_3 = 2,\ \alpha_4 = 3, \textit{ and the three cases of } (19) \textit{ with subscripts in the order } 1324.$$

The least index s for which, in the cases of Lemma 2, $f \equiv 0 \pmod{p^s}$ implies that all x_i are divisible by p, is given as follows.

LEMMA 3. *When (17) holds, $f \equiv 0 \pmod{p^2}$ implies that p divides every x_i. If $p = 2$ and $a_1a_2a_3a_4 \equiv 1 \pmod 8$, then $f \equiv 0 \pmod{2^s}$ implies every x_i even, as follows: when $s = 3$ in (18), when $s = 4$ in (19), when $s = 5$ in (20), when $s = 6$ in (21)-(23).*

6. The forms which fail to represent zero p-adically for an odd p, and yet represent all large integers. By Lemma 3, if f does not represent n it does not represent $p^{2k}n$. Hence such forms f must represent all integers. By (17), f has the form

$$a_1x_1^2 + a_2x_2^2 + p(a_3x_3^2 + a_4x_4^2), \qquad (-a_1a_2|p) = -1 = (-a_3a_4|p),$$

and we can suppose $a_1 \leqq a_2$, $a_3 \leqq a_4$, $p \geqq 3$. In order that f shall represent 1 and 2, $a_1 = 1$ and $a_2 = 1$ or 2. If $p \geqq 7$, f cannot represent 6. If $p = 3$, $(-a_1a_2|p) = -1$ implies that $a_2 = 1$; then if f represents 3,

$a_3 = 1$ and $a_4 \equiv 1 \pmod 3$; if f represents 6, $a_4 = 1$. There remains form (A) of Theorem 3, which is known to represent all positive integers. If $p = 5$ then $a_2 = 2$ in order that $(-a_1a_2|p) = -1$; $a_3 = 1$ if f represents 5, and $a_4 \equiv 2$ or 3 (mod 5); $a_4 = 2$ if f represents 10. We thus obtain the form (B), which was overlooked by Kloosterman, and represents all positive integers.

7. The forms satisfying (18) which represent all large integers. By Lemma 3 such forms must represent all even positive integers. Let

$$f = (a_1, a_2, a_3, a_4), \quad a_1 \equiv a_2 \equiv a_3 \equiv a_4 \pmod 4), \quad a_1 \cdots a_4 \equiv 1 \pmod 8),$$
$$a_1 \leqq a_2 \leqq a_3 \leqq a_4.$$

If $a_1 > 1$, or if $a_1 = 1$ and $a_2 \geqq 5$, then $f \neq 2$. If $a_1 = a_2 = 1$ and $a_3 \geqq 9$ $f \neq 6$. If $a_1 = a_2 = 1$, $a_3 = 5$, $a_4 \geqq 9$, then $f \neq 12$. If $a_1 = a_2 = a_3 = 1$ and $a_4 \geqq 33$, then $f \neq 28$. There remain forms (C), treated in **10.**

8. The forms of type (20). We need only consider the forms (C) with a coefficient multiplied by 4, thus getting the nine distinct forms (D). By Lemma 3 it suffices to prove that these represent all multiples of 8. Since the forms (C) represent all large integers, their products by 4 represent all large multiples of 4. Hence the forms (D) represent all large multiples of 4; but none of these forms can fail to represent a number $8n$, since it would then not represent the large numbers $4^k \cdot 8n$. Hence the forms (D) represent all large integers.

9. Further cases in Lemma 2. Next, consider case (19), (i). We use ? to indicate that no multiple of 4 less than 200 is not represented:

$$\begin{gathered}(1, 1, 2, 2t)\ ?\ ;\ (1, 1, 2, \geqq 66) \neq 56;\ (1, 1, 10, 10)\ ?\ ;\\ (1, 1, 10, \geqq 26) \neq 24;\ (1, 1, \geqq 18, \geqq 18) \neq 12;\ (1, 9, 2, 2t)\ ?\ ;\\ (1, 9, 2, \geqq 66) \neq 56;\ (1, \geqq 9, \geqq 10, \geqq 10) \neq 8;\\ (1, 17, 2, 2s)\ ?\ \text{ if } s = 1, 9, 17;\ (1, 17, 2, \geqq 50) \neq 40;\\ (1, 25, 2, 2r)\ ?\ \text{ if } r = 1, 9;\ (1, 25, 2, \geqq 34) \neq 20;\\ (1, \geqq 33, 2, \geqq 2) \neq 28;\ (\geqq 3, \geqq 3, \geqq 2, \geqq 6) \neq 4;\\ (5, 5, 2, 2)\ ?\ ;\ (\geqq 5, > 5, 2, 2) \neq 12.\end{gathered}$$

There remain the 15 forms (E), treated in **10-12.**

Case (21) (i) is got by multiplying one of the even coefficients in the preceding case by 4, yielding the 24 distinct forms (F). To represent all large numbers they need only represent all multiples of 16, and the fact that they do so follows, much as in **8**, from their connection with (E).

Cases (i) of (22) and (23) lead similarly to the $24 + 39$ forms (G) and (H), which represent all large numbers.

Next, take the case of (19) (ii):

$$(1, \geqq 5, \geqq 6, \geqq 14) \neq 8; \qquad (\geqq 3, \geqq 7, \geqq 2, \geqq 10) \neq 4.$$

Hence no such form represents all large integers. The same conclusion follows for cases (ii) of (21)-(23).

Lastly, consider cases (iii). By (19) we have: the nine forms (I) to be treated in **10-13**;

$$\begin{gathered}(1, u, 2, \geqq 54) \neq 40; \quad (1, \geqq 3, \geqq 6, \geqq 10) \neq 8;\\ (1, \geqq 27, 2, \geqq 6) \neq 20; \quad (\geqq 3, \geqq 3, \geqq 2, \geqq 6) \neq 4.\end{gathered}$$

Extending these to (21)-(23) we get the 72 forms (J), (K), and (L).

10. The method of ternary sections. To complete the proof of Theorem 3 we need only prove that the forms in (A), (B), (C), (E), (I) represent all large integers. The investigation of such problems is usually made to depend on a knowledge of the numbers represented by a ternary section, obtained by putting one of the variables equal to zero. We know the numbers represented by a genus of ternary quadratic forms, and (with a few exceptions) it is only when a ternary form belongs to a genus of one class that we can tell precisely what numbers it represents. For example, the forms (1, 1, 3), (1, 2, 5), (1, 1, 5), (1, 1, 1), (1, 1, 2), (1, 2, 2), (1, 2, 3), (1, 2, 6), (needed in (A), (B), (C), (E), and (I)), are in genera of one class, and so are known to represent all positive integers except those of the respective forms $3^{2k}(9q + 6)$, $5^{2k}(25q + 10$ or $15)$, $4^k(8q + 3)$, $4^k(8q + 7)$, $4^k(16q + 14)$, $4^k(8q + 7)$, $4^k(16q + 10)$, and $4^k(8q + 5)$. The forms (1, 1, 10), (2, 2, 5), (1, 2, 9), and (1, 2, 18) (needed in (E)) are not in genera of one class. However, (1, 1, 10) represents $2n$ if (1, 1, 5) represents n; (1, 2, 9) represents $2n$ if $g_0 = y^2 + 2x^2 - 2xz + 5x^2$ (in a genus of one class, representing all $\neq 4^k(8q + 7)$) represents n; (2, 2, 5) represents $4n$ if (1, 1, 5) represents n; (1, 2, 18) represents $4n$ if g_0 represents n. Only the forms in (2) and (1, 2, 11, 22) fail to succumb, by means of these facts, to the following treatment which we illustrate by the form (1, 25, 2, 18).

The form (1, 25, 2, 18) must be shown to represent all multiples of 4. Now (1, 2, 18) represents all multiples of 4 except $4^{k+1}(8q + 7)$. Also, $4^{k+1}(8q + 7) - 4^{k+1} \cdot 25 = 4^{k+1}(8q - 18)$, and this is represented by (1, 2, 18) unless $q = 0$, 1, or 2. Finally, (1, 25, 2, 18) is verified as representing 28, 60, and 92.

11. The forms (1, 2, 11, 22), (1, 2, 11, 38), and (1, 2, 19, 22). The form (1, 2, 11) represents $2n$ if $g_1 = y^2 + 2x^2 - 2xz + 6z^2$ represents n. Now g_1 is in a genus of one class and represents all positive integers not of the form $4^k(8q + 5)$. Hence (1, 2, 11) represents all evens $\neq 4^k(16q + 10)$. Also, $4^{k+1}(16q + 10) - 22 \cdot 4^k = 4^k(64q + 18)$, which is represented by (1, 2, 11). Again, $4^{k+1}(16q + 10) - 38 \cdot 4^k = 4^k(64q + 2)$, also represented by (1, 2, 11). Hence the forms (1, 2, 11, 22) and (1, 2, 11, 38) represent all large multiples of 4; that they represent all large numbers not divisible by 4 follows from Theorem 4. Similarly, (1, 2, 22) represents every $4n \neq 4^{k+1}(8q + 5)$; hence (1, 2, 22, 19) represents every $4n$.

12. The form (1, 2, 17, 34). The form $x^2 + 2y^2 + 17z^2$ represents $2n$ if $g_2 = y^2 + 2x^2 - 2xz + 9z^2$ represents n. Now g_2 is not in a genus of one class, but is in a genus of two classes, the other class containing the form $h_2 = x^2 + y^2 + 17z^2$. Together, g_2 and h_2 represent all positive integers $\neq 4^k(8q + 7)$. However, the identity

$$(24) \qquad x^2 + y^2 + 17z^2 = x^2 + 2(3z)^2 - 2(3z)(y + z)/3 + 9[(y + z)/3]^2$$

shows that if n is represented in h_2 with either $y + z$ or $x + z$ divisible by 3, then n is represented also in g_2. This can be arranged unless $x^2 \equiv y^2 \not\equiv z^2 \pmod 3$, whence $n \equiv 2 \pmod 3$. Thus:

g_2 represents every $3s$ and $3s + 1$ not of the form $4^k(8q + 7)$.

Hence (1, 2, 17) represents every $6s$ and $6s + 2$ not of the form $4^k(16q + 14)$. In view of Theorem 4 we need consider only multiples of 4. If $6s$ or $6s + 2 = 4^{k+1}(16q + 14)$, then $6s - 34 \cdot 4^k = 4^k(64q + 22) \equiv 2 \pmod 6$, or $6s + 2 - 34 \cdot 9 \cdot 4^k = 4^k(64q - 250) \equiv 2 \pmod 6$, and thus is represented in (1, 2, 17); except, in the last case when $q = 0$ or 3. But (1, 2, 17, 34) represents 56 and 248.

Finally, there remains $6s + 4 = 4(3s_1 + 1)$, say. Subtracting 34 we get $12s_1 - 30$, which has the form $4^k(16q + 14)$ only if $s_1 = 4s_2 + 1$, whence $4(3s_1 + 1) = 4^2(3s_2 + 1)$. We proceed by induction. If $4^h(3s_h + 1) - 34 \cdot 2^{2h-2}$ or $4^{h-1}(12s_h - 30)$ is of the excluded form, then $s_h = 4s_{h+1} + 1$; and so on. If $4^{h-1}(12s_h - 30)$ is negative, s_h is 0, 1, or 2, and $4^h(3s_h + 1)$ is 4^h, 4^{h+1}, or $4^h \cdot 7$, all of which are evidently represented by (1, 2, 17) if $h \geqq 1$.

13. The form (1, 2, 19, 38). The form (1, 2, 19) represents $2n$ if $g_3 = x^2 + 2y^2 + 2yz + 10z^2$ represents n. Also, g_3 and $h_3 = 2x^2 + 2y^2 + 7z^2 + 2yz + 2zx + 2xy$ constitute a genus, representing all positive integers $\neq 4^k(8q + 5)$. This time, transformations of denominator 3, as in (24), do not suffice, and we use denominator 5. The transformations with the matrices $T/5$, where

$$T = \begin{pmatrix} 6 & 4 & -3 \\ 1 & 4 & 7 \\ 1 & -1 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 6 & 2 & 9 \\ 1 & -3 & -6 \\ 1 & 2 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 4 & -2 & 7 \\ -4 & -3 & 3 \\ 1 & 2 & 3 \end{pmatrix},$$

replace g_3 by h_3. Hence if $n = 2x^2 + 2y^2 + 7z^2 + 2yz + 2zx + 2xy$ in integers x, y, z, then g_3 also represents n if any of the following congruences holds:

$$\begin{aligned} &x - y + 2z \equiv 0, \quad x + 2y - z \equiv 0, \quad x + 2y - 2z \equiv 0, \\ &x - y - 2z \equiv 0, \quad 2x + y - z \equiv 0, \quad 2x + y - 2z \equiv 0, \pmod 5, \end{aligned}$$

the last three being got by interchanging x and y. Introducing $X = y + z$, $Y = z + x$, $Z = x + y$, we see that these conditions reduce to

$$(25) \qquad 2X \equiv Y \text{ or } Z, \text{ or } 2Y \equiv Z \text{ or } X, \text{ or } 2Z \equiv X \text{ or } Y \pmod 5.$$

If $n \equiv 0$, 1, or 4 (mod 5), then $h_3 = n$ implies $X^2 + Y^2 + Z^2 \equiv 0$, 1, or 4, whence (X, Y, Z) is a permutation of the following residues mod 5: $(0, 0, 0)$, $(0, 0, \pm 1)$, $(0, 0, \pm 2)$, $(0, \pm 1, \pm 2)$, $(\pm 1, \pm 1, \pm 2)$, $(\pm 1, \pm 2, \pm 2)$. In all cases, (25) is seen to hold (e. g. $2 \cdot 2 \equiv -1$, $2 \cdot 1 \equiv 2$). Hence:

g_3 represents every $5s + 0, 1, 4$ not of the form $4^k(8q + 5)$;

and (1, 2, 19) represents every $10s + 0, 2, 8$ not of the form $4^k(16q + 10)$.

If $10s = 4^{k+1}(16q + 10)$, then $10s - 38 \cdot 4^k = 4^k(64q + 2)$ and is represented by (1, 2, 19). If $10s + 2 = 4^{k+1}(16q + 10)$, then according as k is odd or even, $10s + 2 - 38 \cdot 4^k = 4^k(64q + 2) \equiv 0 \pmod{10}$, or $10s + 2 - 38 \cdot 4^{k+1} = 4^{k+2}(4q - 7) \equiv 0 \pmod{10}$; in the last case q cannot be 0 or 1. Similar results hold if $10s + 8 = 4^{k+1}(16q + 10)$ with k even or odd.

Finally, we have $4(5s_1 \pm 1)$ to consider. Now $4(5s_1 \pm 1) - 38 = 4^k(16q + 10)$ only if $s_1 \equiv \mp 1 \pmod 4$ respectively. Then $4(5s_1 \pm 1) = 4^2(5s_2 \mp 1)$. We proceed by induction and have $4^h(5s_h \pm 1) - 38 \cdot 4^{h-1} = 4^{h-1}(20s_h \pm 4 - 38)$ of the form $4^k(16q + 10)$ only if $s_h = 4s_{h+1} \mp 1$; and so on. If $20s_h \pm 4 - 38$ is negative, then s_h is 0, 1, or 2; and we see that (1, 2, 19, 38) represents 4, 16, 24, 36, and 44.

McGill University.

REFERENCES.

1. J. Liouville, *Journal de Mathématiques*, Ser. 2, vol. 1 (1856), p. 230.

2. S. Ramanujan, *Proceedings of the Cambridge Philosophical Society*, vol. 19 (1917), pp. 11-21; *Collected Papers*, 169-178.

3. L. E. Dickson, *Bulletin of the American Mathematical Society*, vol. 33 (1927), pp. 63-70; Dickson gives proofs of Ramanujan's results on ternary forms.

4. P. R. Halmos, *Bulletin of the American Mathematical Society*, vol. 44 (1938), pp. 141-144. See also A. E. Ross, *Bulletin of the American Mathematical Society*, vol. 49 (1943), p. 362.

5. H. D. Kloosterman, *Acta Mathematica*, vol. 49 (1926), pp. 407-464.

6. Compare G. Pall, *Bulletin of the American Mathematical Society*, vol. 46 (1940), p. 291.

7. Kloosterman, *loc. cit.*, p. 409.

8. C. L. Siegel, *Annals of Mathematics*, vol. 36 (1935), pp. 527-606.

9. W. Tartakowsky, *Bulletin of the Russian Academy of Sciences*, (7), 2 (1929), pp. 111-122.

10. Kloosterman, *loc. cit.*, p. 449.

11. This is of course merely an adaptation of the well-known stepping-up process. Compare Dickson's *Introduction to the Theory of Numbers*, p. 13.

12. H. Hasse, *Journal für Mathematik*, vol. 152 (1923), pp. 129-148 (Theorems 10, 11).

13. H. J. S. Smith, *Collected Mathematical Papers*, I, p. 464.

AN EXTENSION OF A PROBLEM OF KLOOSTERMAN.*

By Arnold E. Ross and Gordon Pall.

1. Introduction. In the previous article [1],[1] Kloosterman's problem of determining all the positive quaternary forms $ax^2 + by^2 + cz^2 + dt^2$ which represent all large integers was completely solved. Ross [2] has proved the following lemma, which makes it possible to extend the solution to cover the general positive integral quaternary form $\Sigma a_{ij}x_ix_j$ in which the a_{ii} and $2a_{ij}$ $(i, j = 1, \cdots, 4)$ are integers.

Lemma 1. *The determinant of any positive integral quaternary quadratic form which represents all positive integers cannot exceed a certain constant R_1.*

We make use also of an extension to a general positive m-ary form $(m \geqq 4)$ of Kloosterman's asymptotic formula [3] for the number of representations of n. Such a formula has been given by W. Tartakowsky [4], who used the Hardy-Littlewood method. It is interesting to see (2) how easily this extension can be made directly from Kloosterman's special case, by induction, making use of Ross's [5] technique of employing primes represented by a primitive form, and the fact that every primitive form in two or more variables represents infinitely many primes.

References to the preceding article will be prefixed by P. The definitions of the terms "f is universal for p," and "f represents zero p-adically," given near $P(3)$ and $P(4)$ evidently extend to any integral forms f. Once the asymptotic formula (1) is established, Lemma 2 and the proof of Theorem $P1$ yield

Theorem 1. *Let f be any positive integral m-ary quadratic form, $m \geqq 4$. Let n be such that $f(x_1, \cdots, x_m) \equiv n \bmod p^r$ is solvable for every p and r. For edch prime p (if any) such that f fails to represent zero p-adically impose an upper bound to the power of p which may divide n. Then f represents every such n sufficiently large.*

It should be observed that if $m \geqq 5$, every f represents zero p-adically for every $p \mid 6$. Hence we can conclude (as Tartakowsky did) that all forms in a

* Received July 17, 1945.

[1] Numbers in square brackets refer to the references at the end of the paper.

genus of positive quadratic forms in five or more variables represent the same sufficiently large numbers. If $m = 4$, f can fail to represent zero p-adically only for a few primes appearing in its determinant (the conditions [6] are easily applied and are given partly in our Lemma 4).

It follows that if f is universal for every p, and represents zero p-adically for every p, then if $m \geqq 4$, f represents every sufficiently large positive integer n. In **4** we shall, using Lemma 1, obtain

THEOREM 2. *The number of integral positive quaternary quadratic forms which represent all large numbers, and yet fail to represent zero p-adically for some prime p_1, is finite. In fact the determinant of any such form cannot exceed R_1 if $p_1 > 2$, $256R_1$ if $p_1 = 2$.*

Theorem 1 does not extend to $m = 2$, since binary classes in the same genus, which are neither properly nor improperly equivalent, do not represent the same primes 7. The theorem does not extend without modification to $m = 3$, as was shown by an example in 1939 [8]. The example consists of the forms

$$f = x^2 + y^2 + 16z^2, \qquad g = 2x^2 + 2y^2 + 5z^2 - 2xz - 2yz,$$

which are easily seen to represent equally often every positive integer not an odd square. If s is odd, a result of Jacobi's [9] shows that

$$f(s^2) - g(s^2) = (-1)^{\frac{1}{2}(s-1)}4s,$$

where $f(n)$ denotes the number of representations of n by f. Also,

$$f(s^2) + g(s^2) = 4\Pi\psi(p, a),$$

where

$$\psi(p, a) = (p^{a+1} - 1)/(p - 1) - (-1 \mid p)(p^a - 1)/(p - 1),$$

and the product ranges over the prime-power decomposition $s = \Pi p^a$. From this it is easily seen that $g(s^2) = 0$ if every prime p in s satisfies $p \equiv 1 \bmod 4$. This example is especially interesting in that f and g are two forms in the same genus, and we are able to give exact simple formulas for the number of representations of any number in either form.

However, the theorem is true when $m = 3$ for a large variety of forms [10]; and, if we may make a conjecture, it is probably true for squarefree numbers n and every ternary f.

2. The asymptotic formula for the number of representations of n in f.

THEOREM 3. *Let $m \geqq 4$. For any positive integral m-ary form $f = \Sigma a_{ij}x_ix_j$ where a_{ii} and $2a_{ij}$ $(i, j = 1, \cdots, m)$ are integers, the number of representations $f(n)$ of n by f is given by the formula*

$$(1) \qquad \frac{\pi^{\frac{1}{2}m}n^{\frac{1}{2}m-1}S(n)}{\Gamma(\frac{1}{2}m)\Delta^{\frac{1}{2}}} + O(n^{\frac{1}{2}m-1-1/18+\epsilon}),$$

where Δ denotes the determinant $\mid a_{ij} \mid$ of f,

$$(2) \quad S(n) = \prod_{p=2,3,5,7,\ldots} \chi(p), \qquad \chi(p) = \chi(p, f, n) = \lim_{r\to\infty} p^{-(m-1)r}f(n, p^r),$$

and $f(n, p^r)$ denotes the number of solutions $x_1, \cdots, x_m$ mod p^r *of $f \equiv n$* mod p^r.

Proof. We can write $f = b_1x_1^2 + \cdots + b_{s-1}x_{s-1}^2 + d_1\phi(x_s, \cdots, x_m)$, where ϕ is primitive. Let Δ_1 denote the determinant of ϕ; then $\Delta = b_1 \cdots b_{s-1}d_1^{m-s+1}\Delta_1$. Suppose, then, that (1) is known to be true if $s_1 \leqq s \leqq m$. Kloosterman's case is of course $s_1 = m$. Now let $s = s_1 - 1$. Let q denote an odd prime represented by ϕ and not dividing Δ. We can write $\phi = \sum_{i,j=s}^{m} a_{ij}x_ix_j$, $a_{ss} = q$.

Case I: the a_{sj} all integers. By completing squares we have the identity

$$(3) \qquad qf = qb_1x_1^2 + \cdots + qb_{s-1}x_{s-1}^2 + d_1(qx_s + \sum_{j=s+1}^{m} a_{sj}x_j)^2 + d_1\psi,$$

where $\psi(x_{s+1}, \cdots, x_m) = \sum_{i,j=s+1}^{m} (qa_{ij} - a_{is}a_{sj})x_ix_j$. We introduce two forms:

$$(4) \qquad f_1 = qb_1y_1^2 + \cdots + qb_{s-1}y_{s-1}^2 + d_1y_s^2 + d_1\psi(y_{s+1}, \cdots, y_m),$$

and the form f_2 got from f_1 by changing the coefficient of y_s^2 to q^2d_1. Now for every representation of qn in f_1 we have

$$y_s^2 \equiv -\psi(y_{s+1}, \cdots, y_m) \equiv \sum_{i,j=s+1}^{m} a_{is}y_i \cdot a_{sj}y_j \equiv (\sum_{j=s+1}^{m} a_{sj}y_j)^2 \pmod q.$$

Hence: $y_s \equiv \Sigma a_{sj}y_j \bmod q$ holds only by choice of sign of y_s if $q \nmid y_s$, and always if $q \mid y_s$. Accordingly,

$$\begin{aligned} f(n) = N(n = f) = N(qn = qf) &= N(qn = f_1;\ y_s \equiv \Sigma a_{sj}y_j \bmod q) \\ &= \tfrac{1}{2}\{N(qn = f_1) - N(qn = f_2)\} + N(qn = f_2), \text{ that is,} \end{aligned}$$

$$(5) \qquad f(n) = \tfrac{1}{2}f_1(qn) + \tfrac{1}{2}f_2(qn).$$

If $p \neq q$, f_1 and f_2 are derived from qf by transformations of determinants prime to p, whence $f(n, p^r) = f_1(qn, p^r) = f_2(qn, p^r)$. Hence

$$(6) \qquad \chi(p, f, n) = \chi(p, f_1, qn) = \chi(p, f_2, qn), \text{ if } p \neq q.$$

If $p = q$, we have (counting solutions of the congruences with care):

$$\begin{aligned} f(n, q^r) &= q^{-m} f(qn, q^{r+1}) = q^{-m+1} N(qn \equiv f_1 \bmod q^{r+1};\ y_s \equiv \Sigma a_{sj} y_j \bmod q) \\ &= q^{-m+1} \tfrac{1}{2} \{ N(qn \equiv f_1 \bmod q^{r+1}) - q^{-1} N(qn \equiv f_2 \bmod q^{r+1}) \} \\ &\quad + q^{-m+1} q^{-1} N(qn \equiv f_2 \bmod q^{r+1}), \end{aligned}$$

whence

$$(7) \qquad f(n, q^r) = q^{-m+1} \{ \tfrac{1}{2} f_1(qn, q^{r+1}) + \tfrac{1}{2} q^{-1} f_2(qn, q^{r+1}) \},$$

$$(8) \qquad \chi(q, f, n) = \tfrac{1}{2} \chi(q, f_1, qn) + \tfrac{1}{2} q^{-1} \chi(q, f_2, qn).$$

Hence as (1) holds for f_1 and f_2, we have by (5),

$$f(n) \doteq \{\Gamma(\tfrac{1}{2}m)\}^{-1} \pi^{\frac{1}{2}m} \Delta^{-\frac{1}{2}} n^{\frac{1}{2}m-1} \prod_{p \neq q} \chi(p) \cdot \lambda + O((qn)^{\frac{1}{2}m-1-1/18+\epsilon}),$$

where

$$\lambda = \tfrac{1}{2} (q^{m-2})^{-\frac{1}{2}} q^{\frac{1}{2}m-1} \chi(q, f_1, qn) + \tfrac{1}{2} (q^m)^{-\frac{1}{2}} q^{\frac{1}{2}m-1} \chi(q, f_2, qn) = \chi(q, f, n),$$

by (8). The induction is thus complete for Case I.

Case II: some coefficient $2a_{sj}$ is odd. We now use the identity

$$4qf = 4qb_1 x_1^2 + \cdots + 4qb_{s-1} x_{s-1}^2 + d_1(2qx_s + \Sigma 2a_{sj} x_j)^2 + d_1 \psi,$$

where $\psi = \Sigma(4qa_{ij} - 4a_{is}a_{sj}) x_i x_j$. Besides the two forms

$$(9) \qquad f_k = 4qb_1 y_1^2 + \cdots + 4qb_{s-1} y_{s-1}^2 + q^{2k-2} d_1 y_s^2 + d_1 \psi(y_{s+1}, \cdots, y_m), \quad k = 1, 2,$$

we shall require the form f'_k obtained from f_k by changing y_s to $2y_s$, the form f_k'' obtained from f_k by expressing the condition that $\Sigma 2a_{sj} y_j$ is even (e. g. if $2a_{sm}$ is odd by replacing y_m in ψ by $2a_{s,s+1} y_{s+1} + \cdots + 2a_{s,m-1} y_{m-1} + 2y_m$), and the form f_k''' obtained by both the preceding operations.

If $4qn$ is represented in f_1, we now have only $y_s^2 \equiv (\Sigma 2a_{sj} y_j)^2 \bmod q$. Hence for any integer n,

$$\begin{aligned} f(n) &= N(4qn = 4qf) = N(4qn = f_1;\ y_s \equiv \Sigma 2a_{sj} y_j \bmod 2q) \\ &= \tfrac{1}{2} N(4qn = f_1, y_s \equiv \Sigma 2a_{sj} y_j \bmod 2) + \tfrac{1}{2} N(4qn = f_2, y_s \equiv \Sigma 2a_{sj} y_j \bmod 2). \end{aligned}$$

Hence it is easily seen that

$$(10) \qquad f(n) = \sum_{k=1}^{2} \{ \tfrac{1}{2} f_k(4qn) - \tfrac{1}{2} f_k'(4qn) - \tfrac{1}{2} f_k''(4qn) + f_k(4qn) \}.$$

If $p \neq q$ and $p \neq 2$, we obviously have

$$f(n, p^r) = f_1(4qn, p^r) = f_1'(4qn, p^r) = \cdots = f_2'''(4qn, p^r),$$

whence $\chi(p)$ is the same in all cases. Evidently also $\chi(2)$ is the same for f_1 as for f_2, for f_1' as for f_2', for f_1'' as for f_2'', for f_1''' as for f_2'''; and $\chi(q)$ is the same for all four forms f_1, f_1', f_1'', f_1''', and again for the forms f_2, f_2'; f''_2, f_2'''. Next,

$$\begin{aligned} f(n, q^r) &= q^{-m} f(4qn, q^{r+1}) = q^{1-m} N(f_1 \equiv 4qn \bmod q^{r+1};\ y_s \equiv \Sigma 2a_{sj} y_j \bmod q) \\ &= q^{1-m} \{ \tfrac{1}{2} f_1(4qn, q^{r+1}) + \tfrac{1}{2} q^{-1} f_2(4qn, q^{r+1}) \}; \end{aligned}$$

$$(11) \qquad \chi(q, f, n) = \tfrac{1}{2} \chi(q, f_1, 4qn) + \tfrac{1}{2} q^{-1} \chi(q, f_2, 4qn).$$

Also, $f(n, 2^r) = 4^{-m} N(4qf \equiv 4qn \bmod 2^{r+2}) = 2^{1-2m} N(f_1 \equiv 4qn \bmod 2^{r+2};$ $y_s \equiv \Sigma 2a_{sj} y_j \bmod 2) = 2^{1-2m} f_1(4qn, 2^{r+2}) - N(f_1 \equiv 4qn, y_s \text{ even})$ $- N(f_1 \equiv 4qn, \Sigma 2a_{sj} y_j \text{ even}) + 2N(f_1 \equiv 4qn, y_s \text{ and } \Sigma 2a_{sj} y_j \text{ even})$ whence

$$\begin{aligned} (12) \qquad \chi(2, f, n) = \tfrac{1}{2} \chi(2, f_1, 4qn) - \tfrac{1}{4} \chi(2, f_1', 4qn) - \tfrac{1}{4} \chi(2, f_1'', 4qn) \\ + \tfrac{1}{4} \chi(2, f_1''', 4qn). \end{aligned}$$

Substituting in (10) we obtain the required formula for $f(n)$ in this case also.

3. Proof of Theorem 1. This proceeds exactly as in *P* **3**. We have only to convert f into a convenient form-residue mod p^r: cf. Lemma 2 [11]. Corresponding to $P(12)$, with Δ in place of *abcd*, we can use known formulas [12] for $f(n, p^r)$ in the cases where $p \nmid 2\Delta$ to prove that $\chi(p) \geqq 1 - p^{-\frac{1}{2}m}$ if $p \nmid n$ and m is even, $\chi(p) \geqq (1 - p^{-\frac{1}{2}m})(1 - p^{-1})$ if $p | n$ and m is even, and $\chi(p) \geqq 1 - p^{1-m}$ if m is odd. Hence the product of the $\chi(p)$ for all odd primes not dividing Δ is easily seen to exceed $K/\log \log n$. The additional discussion for cases (14)-(17) will be found in *P*, **3**.

LEMMA 2. *Every integral quaternary form f is equivalent* mod p^r, *by a transformation of determinant prime to p, to a form of the type*

$$(13) \qquad p^{\alpha_1} a_1 x_1^2 + \cdots + p^{\alpha_4} a_4 x_4^2, \quad \bmod p^r,$$

$$0 \leqq \alpha_1 \leqq \alpha_2 \leqq \alpha_3 \leqq \alpha_4, \quad a_1 a_2 a_3 a_4 \textit{ prime to } p,$$

if $p > 2$. If $p = 2$, f is equivalent mod 2^r *either to* (13), *or to a form with one of the following residues* mod 2^r:

$$2^{\alpha_1}a_1x_1^2 + 2^{\alpha_2}a_2x_2^2 + 2^{\alpha_3}(2jx_3^2 + 2x_3x_4 + 2jx_4^2), \tag{14}$$

$$2^{\alpha_1}a_1x_1^2 + 2^{\alpha_2}(2jx_2^2 + 2x_2x_3 + 2jx_3^2) + 2^{\alpha_4}a_4x_4^2, \tag{15}$$

$$2^{\alpha_1}(jx_1^2 + x_1x_2 + jx_2^2) + 2^{\alpha_3}a_2x_3^2 + 2^{\alpha_4}a_4x_4^2, \tag{16}$$

$$2^{\alpha_1}(jx_1^2 + x_1x_2 + jx_2^2) + 2^{\alpha_3}(kx_3^2 + x_3x_4 + kx_4^2). \tag{17}$$

Here all a_i are odd, $j, k = 0$ or 1. *Also, in* (14), $0 \leqq \alpha_1 \leqq \alpha_2 < \alpha_3$; *in* (15), $0 \leqq \alpha_1 < \alpha_2 < \alpha_4$; *in* (16), $0 \leqq \alpha_1 \leqq \alpha_3 \leqq \alpha_4$; *and in* (17), $0 \leqq \alpha_1 \leqq \alpha_3$.

4. Proof of Theorem 2. We first extend Lemmas $P1$ and $P2$ as follows:

LEMMA 3. *The conditions that f be universal for p are as stated in Lemma $P1$ if f has the residue* (13). *If $p = 2$ and f has a residue* (14) *or* (15), *f is not universal for p. If $p = 2$ and f has a residue* (16) *or* (17), *f is universal for p if and only if, respectively:*

$$\alpha_1 = 0, \text{ and either } j = 0 \text{ or } \alpha_3 = 0 \text{ or } \alpha_3 = 1 \geqq \alpha_4 - 2; \tag{18}$$

$$\alpha_1 = 0, \text{ and either } j = 0 \text{ or } \alpha_3 = 0 \text{ or } \alpha_3 = 1. \tag{19}$$

LEMMA 4. *If f is universal for p, and f has a residue* (13), *the condition that f fail to represent zero p-adically is given in Lemma $P2$. If* (16) *and* (18), *or* (17) *and* (19), *hold, then f fails to represent zero p-adically if and only if, respectively:*

$$\alpha_1 = 0,\ j = 1,\ \alpha_3 = 1,\ \alpha_4 = 1 \text{ or } 3, \text{ and } a_3a_4 \equiv 3 \bmod 8; \tag{20}$$

$$\alpha_1 = 0,\ j = 1,\ \alpha_3 = 1,\ k = 1. \tag{21}$$

Again, Lemma $P3$ extends to the cases coming under (13). Also,

LEMMA 5. $2^s | f$ *implies* $2 | $ *all* x_i, *if* $s = 3 + \alpha_4$ *in* (20), *if* $s = 2$ *in* (21).

If $p > 2$, or if $p = 2$ and the cases corresponding to (21) hold, then if f does not represent one number n, f will not represent $p^{2k}n$, by Lemmas 5 and $P3$. Hence if f represents all large integers, $\det f \leqq R_1$.

Let $p = 2$ and f be given by (13). (a) If $P(18)$ holds and f represents all large integers it must represent every $2n$, by Lemma $P3$. Now if $f = 2n$, Σx_i is even. Hence the transformation $x_1 = y_1$, $x_2 = y_2$, $x_3 = y_3$, $x_4 = y_1 + y_2 + y_3 + 2y_4$ replaces f by $2g$, where g is an integral form and g represents every n; by Lemma 1, $\det g \leqq R_1$, $\det f \leqq 4R_1$. (b) If $P(20)$ holds, f is obtainable (by changing x_4 to $2x_4$) from a form under case (a). Hence $\det f \leqq 16R_1$. (c) If $P(19)$ holds, and f represents all large integers, f represents every $4n$. In subcases (i) and (ii), $f = 4n$ implies $x_1 = y_1 + y_2$, $x_2 = y_1 - y_2$, $x_3 = y_3$, $x_4 = y_1 + y_2 + y_3 + 2y_4$ where the y_i are integers; and f becomes $4g$ where g represents all n; hence $\det f \leqq 16R_1$. In subcase (iii), $x_1 = y_1 + y_2$, $x_2 = y_1 - y_2$, $x_3 = y_3 + y_4$, $x_4 = y_3 - y_4$ yields the same result. (d) As in case (b), forms coming under $P(21)$-(23) lead to $\det f \leqq 64R_1$, $64R_1$, $256R_1$ respectively.

Next let $p = 2$ and f correspond to (20) with $\alpha_4 = 1$. Then f must represent every $4n$. If $f = 4n$, $x_1 = 2y_1$, $x_2 = 2y_2$, $x_3 = y_3 + y_4$, $x_4 = y_3 - y_4$, and we get $\det f \leqq 4R_1$. Finally, if $\alpha_4 = 3$ instead, $\det f \leqq 16R_1$.

ST. LOUIS UNIVERSITY,
McGILL UNIVERSITY.

REFERENCES.

1. G. Pall, *American Journal of Mathematics*, vol. 68 (1946), pp. 47-58.
2. A. E. Ross, *American Journal of Mathematics*, vol. 68 (1946), pp. 29-46.
3. H. D. Kloosterman, *Acta Mathematica*, vol. 49 (1926), pp. 407-464.
4. W. Tartakowsky, *Bull. Acad. Sci. Leningrad* (7) 2 (1929), pp. 111-122, 165-196.
5. A. E. Ross, *loc. cit.*
6. H. Hasse, *Journal für Mathematik*, vol. 152 (1923), pp. 129-148.
7. E. g., G. Pall, *Mathematische Zeitschrift*, vol. 36 (1933), pp. 321-343, (329).
8. B. W. Jones and G. Pall, *Acta Mathematica*, vol. 70 (1939), pp. 165-191 (181).
9. Cf. Dickson's *History of the Theory of Numbers*, vol. II, pp. 261-263.
10. U. V. Linnik, *Bull. Acad. Sci. URSS. Ser. Math.*, vol. 4 (1940), pp. 363-402; a correction promised in *C. R. Acad. Sci. URSS.*, sometime in 1943.
11. Cf. B. W. Jones, *Duke Mathematical Journal*, vol. 9 (1942), pp. 723-756 (726-727).
12. E. g., C. L. Siegel, *Annals of Mathematics*, vol. 36 (1935), pp. 527-606, (Lemma 16).

$$(14)\qquad 2^{\alpha_1}a_1x_1^2 + 2^{\alpha_2}a_2x_2^2 + 2^{\alpha_3}(2jx_3^2 + 2x_3x_4 + 2jx_4^2),$$

$$(15)\qquad 2^{\alpha_1}a_1x_1^2 + 2^{\alpha_2}(2jx_2^2 + 2x_2x_3 + 2jx_3^2) + 2^{\alpha_4}a_4x_4^2,$$

$$(16)\qquad 2^{\alpha_1}(jx_1^2 + x_1x_2 + jx_2^2) + 2^{\alpha_3}a_2x_3^2 + 2^{\alpha_4}a_4x_4^2,$$

$$(17)\qquad 2^{\alpha_1}(jx_1^2 + x_1x_2 + jx_2^2) + 2^{\alpha_3}(kx_3^2 + x_3x_4 + kx_4^2).$$

Here all a_i are odd, $j, k = 0$ or 1. *Also, in* (14), $0 \leqq \alpha_1 \leqq \alpha_2 < \alpha_3$; *in* (15), $0 \leqq \alpha_1 < \alpha_2 < \alpha_4$; *in* (16), $0 \leqq \alpha_1 \leqq \alpha_3 \leqq \alpha_4$; *and in* (17), $0 \leqq \alpha_1 \leqq \alpha_3$.

4. Proof of Theorem 2. We first extend Lemmas $P1$ and $P2$ as follows:

LEMMA 3. *The conditions that f be universal for p are as stated in Lemma $P1$ if f has the residue* (13). *If $p = 2$ and f has a residue* (14) *or* (15), *f is not universal for p. If $p = 2$ and f has a residue* (16) *or* (17), *f is universal for p if and only if, respectively:*

$$(18)\qquad \alpha_1 = 0, \text{ and either } j = 0 \text{ or } \alpha_3 = 0 \text{ or } \alpha_3 = 1 \geqq \alpha_4 - 2;$$

$$(19)\qquad \alpha_1 = 0, \text{ and either } j = 0 \text{ or } \alpha_3 = 0 \text{ or } \alpha_3 = 1.$$

LEMMA 4. *If f is universal for p, and f has a residue* (13), *the condition that f fail to represent zero p-adically is given in Lemma $P2$. If* (16) *and* (18), *or* (17) *and* (19), *hold, then f fails to represent zero p-adically if and only if, respectively:*

$$(20)\qquad \alpha_1 = 0,\ j = 1,\ \alpha_3 = 1,\ \alpha_4 = 1 \text{ or } 3, \text{ and } a_3a_4 \equiv 3 \bmod 8;$$

$$(21)\qquad \alpha_1 = 0,\ j = 1,\ \alpha_3 = 1,\ k = 1.$$

Again, Lemma $P3$ extends to the cases coming under (13). Also,

LEMMA 5. *$2^s | f$ implies $2 | $ all x_i, if $s = 3 + \alpha_4$ in* (20), *if $s = 2$ in* (21).

If $p > 2$, or if $p = 2$ and the cases corresponding to (21) hold, then if f does not represent one number n, f will not represent $p^{2k}n$, by Lemmas 5 and $P3$. Hence if f represents all large integers, $\det f \leqq R_1$.

Let $p = 2$ and f be given by (13). (a) If $P(18)$ holds and f represents all large integers it must represent every $2n$, by Lemma $P3$. Now if $f = 2n$, Σx_i is even. Hence the transformation $x_1 = y_1$, $x_2 = y_2$, $x_3 = y_3$, $x_4 = y_1 + y_2 + y_3 + 2y_4$ replaces f by $2g$, where g is an integral form and g represents every n; by Lemma 1, $\det g \leqq R_1$, $\det f \leqq 4R_1$. (b) If $P(20)$ holds, f is obtainable (by changing x_4 to $2x_4$) from a form under case (a). Hence $\det f \leqq 16R_1$. (c) If $P(19)$ holds, and f represents all large integers, f represents every $4n$. In subcases (i) and (ii), $f = 4n$ implies $x_1 = y_1 + y_2$, $x_2 = y_1 - y_2$, $x_3 = y_3$, $x_4 = y_1 + y_2 + y_3 + 2y_4$ where the y_i are integers; and f becomes $4g$ where g represents all n; hence $\det f \leqq 16R_1$. In subcase (iii), $x_1 = y_1 + y_2$, $x_2 = y_1 - y_2$, $x_3 = y_3 + y_4$, $x_4 = y_3 - y_4$ yields the same result. (d) As in case (b), forms coming under $P(21)$-(23) lead to $\det f \leqq 64R_1$, $64R_1$, $256R_1$ respectively.

Next let $p = 2$ and f correspond to (20) with $\alpha_4 = 1$. Then f must represent every $4n$. If $f = 4n$, $x_1 = 2y_1$, $x_2 = 2y_2$, $x_3 = y_3 + y_4$, $x_4 = y_3 - y_4$, and we get $\det f \leqq 4R_1$. Finally, if $\alpha_4 = 3$ instead, $\det f \leqq 16R_1$.

ST. LOUIS UNIVERSITY,
MCGILL UNIVERSITY.

REFERENCES.

1. G. Pall, *American Journal of Mathematics*, vol. 68 (1946), pp. 47-58.
2. A. E. Ross, *American Journal of Mathematics*, vol. 68 (1946), pp. 29-46.
3. H. D. Kloosterman, *Acta Mathematica*, vol. 49 (1926), pp. 407-464.
4. W. Tartakowsky, *Bull. Acad. Sci. Leningrad* (7) 2 (1929), pp. 111-122, 165-196.
5. A. E. Ross, *loc. cit.*
6. H. Hasse, *Journal für Mathematik*, vol. 152 (1923), pp. 129-148.
7. E. g., G. Pall, *Mathematische Zeitschrift*, vol. 36 (1933), pp. 321-343, (329).
8. B. W. Jones and G. Pall, *Acta Mathematica*, vol. 70 (1939), pp. 165-191 (181).
9. Cf. Dickson's *History of the Theory of Numbers*, vol. II, pp. 261-263.
10. U. V. Linnik, *Bull. Acad. Sci. URSS. Ser. Math.*, vol. 4 (1940), pp. 363-402; a correction promised in *C. R. Acad. Sci. URSS.*, sometime in 1943.
11. Cf. B. W. Jones, *Duke Mathematical Journal*, vol. 9 (1942), pp. 723-756 (726-727).
12. E. g., C. L. Siegel, *Annals of Mathematics*, vol. 36 (1935), pp. 527-606, (Lemma 16).