A THEOREM ON SIMULTANEOUS REPRESENTATION OF PRIMES AND ITS COROLLARIES*

ARNOLD E. ROSS

1. **Simultaneous representation of primes.** Two numbers m and M are said to be represented simultaneously by a ternary form

$$f = ax^2 + by^2 + cz^2 + 2ryz + 2sxz + 2txy \tag{1}$$

and its reciprocal†

$$F = AX^2 + BY^2 + CZ^2 + 2RYZ + 2SXZ + 2TXY \tag{2}$$

if there exist integers x, y, z and X, Y, Z such that $f(x, y, z) = m$, $F(X, Y, Z) = M$ and $xX + yY + zZ = 0$.

The case of interest is that in which representation is not only simultaneous but also proper.‡ One is usually interested in the existence of such numbers m and M, fulfilling certain conditions, with the view of a suitable normalization of the given form f and its reciprocal F.§

In this paper we will require that m and M be a pair of simultaneously and properly represented distinct odd primes or doubles of such primes and derive a normalized form permitting some interesting applications. We note that the first coefficient a of f and the third coefficient C of F are represented simultaneously and properly and express our result as the following theorem.

THEOREM 1. *If f is a ternary quadratic form with a properly primitive reciprocal and if f is* (i) *properly or* (ii) *improperly primitive, then it is equivalent to a form f' such that* (i) *a' and C' are distinct odd primes not dividing $2\Omega\Delta$, or* (ii) *$a' = 2\alpha$ and α and C' are distinct odd primes not dividing $2\Omega\Delta$. Here a' is the leading coefficient of f', and C' is the third coefficient of the reciprocal F' of f'.*

We note that since F is properly primitive it represents properly an integer prime to any assigned integer and hence to $2\Omega\Delta$. If $\Omega\Delta$ is odd, then F represents properly an integer congruent to 1 (mod 4)

---

* Presented to the Society in part, April 9, 1937, under the title *On certain rational transformations.*

† See Dickson, *Studies in the Theory of Numbers*, University of Chicago Press, p. 12.

‡ Ibid.

§ Dickson, ibid., pp. 15–17 and 54–60; P. Bachman, *Die Arithmetik der quadratischen Formen*, vol. 1, p. 64; H. J. S. Smith, *Collected Works*, vol. 1, pp. 455–509.

and one congruent to 3 (mod 4). Hence we may assume that C is prime to $2\Omega\Delta$ and, if $\Omega\Delta$ is odd,

$$C \equiv \Omega \pmod 4. \tag{3}$$

Then the binary form

$$\psi = ax^2 + 2txy + by^2, \qquad ab - t^2 = \Omega C, \tag{4}$$

is properly or improperly primitive according as f is properly or improperly primitive.

For, in view of a well known property of determinants,

$$aS + tR + sC = 0, \quad tS + bR + rC = 0, \quad sS + rR + cC = \Omega\Delta. \tag{5}$$

The g.c.d. g of a, t, b divides $ab-t^2=\Omega C$ and also the determinant $D=\Omega^2\Delta$ of f. Since C is prime to $2\Omega\Delta$, g divides Ω and is prime to C. Then by (5_1) and (5_2), g divides sC and rC, and hence s and r. Therefore, since g divides Ω, it divides cC and hence c by (5_3). Thus g divides the g.c.d. of the coefficients $a, \cdots, t$ of f, and, since f is primitive, $g=1$. Hence ψ is primitive.

If f is properly primitive, so is ψ. The determinant of f is $abc+2rst-ar^2-bs^2-ct^2=\Omega^2\Delta$. Let $\Omega^2\Delta$ be even. If ψ were improperly primitive, then c would be even by the above and f would be improperly primitive. If $\Omega\Delta$ is odd, $\Omega C\equiv 1 \pmod 4$ by (3), whereas if ψ were improperly primitive, we would have $\Omega C=ab-t^2\equiv -1 \pmod 4$.

If f is improperly primitive, ψ is also improperly primitive since it is primitive.

If ψ is properly primitive, it represents properly an odd prime a_1 not dividing $2\Omega\Delta C$. If ψ is improperly primitive, it represents properly an integer $a_1=2\alpha$ such that α is an odd prime not dividing $2\Omega\Delta C$.* Hence ψ is equivalent to a form ψ_1 with a_1 as the leading coefficient. A transformation carrying ψ into ψ_1 carries f into $f_1=a_1x^2+\cdots$. The contragredient (defined by the transpose of the reciprocal of its matrix) transformation which carries F into the reciprocal F_1 of f_1, leaves C unaltered.†

The binary section $\Psi=B_1Y^2+2R_1YZ+C_1Z^2$, $(B_1C_1-R_1^2=\Delta a_1)$, of F_1 is properly primitive, since $C_1=C$ is odd and since the g.c.d. g of B_1, R_1, C_1 divides Δa_1 and hence is equal to unity by virtue of the choice of C $(=C_1)$ and a_1. Thus, as above, the properly primitive binary Ψ represents properly on odd prime C' not dividing $\Omega\Delta a_1$.‡

* H. Weber, Mathematische Annalen, vol. 20 (1882), pp. 301–329.

† Dickson, ibid., p. 16.

‡ One could have appealed to a well known result in quadratic form theory and assumed from the beginning that C was a prime.

Thus Ψ is equivalent to a binary form Ψ_1 with C' as the coefficient of Z^2. A transformation carrying Ψ into Ψ_1 carries F_1 into $F' = \cdots + C'Z^2$, and its contragedient transformation carrying f_1 into f', whose reciprocal is F', leaves the leading coefficient a_1 unaltered. Thus $a_1 = a'$, and f' is a form required in Theorem 1.

If the reciprocal F of f is improperly primitive, then f is properly primitive and, by virtue of the symmetry of the relation of reciprocity, Theorem 1 may be applied with f and F interchanged. We obtain thus the following result.

THEOREM 2. *If f is a properly primitive form with an improperly primitive reciprocal, then it is equivalent to a form f' such that $C' = 2\gamma$ and a' and γ are distinct odd primes not dividing $2\Omega\Delta$. Here, as before, a' is the leading coefficient of f' and C' the third coefficient of the reciprocal F' of f'.*

2. **Reduction to sum of squares.** We will assume now that the leading coefficient a of f and the third coefficient C of F are either distinct odd primes not dividing $\Omega\Delta$ or doubles of such primes.

Multiplying both members of (1) by a we obtain

$$af(x, y, z) = (ax + ty + sz)^2 + \Omega Cy^2 - 2\Omega Ryz + \Omega Bz^2, \tag{6}$$

where

$$ab - t^2 = \Omega C, \qquad ac - s^2 = \Omega B, \qquad ar - st = -\Omega R. \tag{7}$$

Next, multiplying both members of (6) by C and noting that by determinant theory

$$BC - R^2 = \Delta a, \tag{8}$$

we get

$$Caf(x, y, z) = C(ax + ty + sz)^2 + \Omega(Cy - Rz)^2 + \Omega\Delta az^2. \tag{9}$$

We now write

$$G(X, Y, Z) = CX^2 + \Omega Y^2 + \Omega\Delta aZ^2 \tag{10}$$

and speak of the so-constructed form G in the independent variables X, Y, Z as a form *associated* with f.

THEOREM 3. *Let f be a primitive ternary quadratic form, and let F be its reciprocal form. Employ the notation of* (1) *and* (2). *Let the leading coefficient a of f and the third coefficient C of F be either odd primes or doubles of such primes. Then if f represents an integer m, the associated form G in* (10) *represents aCm and in case $\Omega \equiv C \equiv 0 \pmod 2$ then*

$Y \equiv Z \pmod 2$. *Conversely if the form* G *represents* aCm *and if* $Y \equiv Z \pmod 2$ *when* $\Omega \equiv C \equiv 0 \pmod 2$, *then* f *represents* m.

If the representation of aCm *by* G *is proper, then that of* m *by* f *is likewise proper. The converse of the last statement holds with reservation; namely, if a proper representation* x, y, z *of* m *by* f *is given, then the related representation* X, Y, Z *of* aCm *by* F *is also proper if* a *and* C *are prime to* m.*

The first part of the theorem is obvious in view of (9). We assume next that G represents aCm. There exist, therefore, integers X, Y, Z such that

$$aCm = CX^2 + \Omega Y^2 + \Omega\Delta a Z^2. \tag{11}$$

It follows from (11) that $\Omega Y^2 + \Omega\Delta a Z^2 \equiv 0 \pmod C$. But by (8), $\Delta a \equiv -R^2 \pmod C$. Thus $\Omega(Y^2 - R^2 Z) \equiv 0 \pmod C$, and, multiplying through by -1 and factoring, we get $\Omega(RZ + Y)(RZ - Y) \equiv 0 \pmod C$. Since C is an odd prime not dividing Ω or a double of such a prime, since $Y \equiv Z \pmod 2$ if $C \equiv \Omega \equiv 0 \pmod 2$ by hypothesis, and since R is odd in the latter case in view of the choice of a, we have either $RZ + Y \equiv 0$ or $RZ - Y \equiv 0 \pmod C$. Thus, there exists an integer y such that either

$$RZ + Y = Cy \tag{12_1}$$

or

$$RZ - Y = Cy, \tag{12_2}$$

that is, such that

$$\pm Y = Cy - RZ. \tag{13}$$

Substituting $(Cy - RZ)^2$ for Y^2 in (11), we get, in view of (8),

$$\begin{aligned} aCm &= CX^2 + \Omega(Cy - RZ)^2 + \Omega(BC - R^2)Z^2 \\ &= CX^2 + \Omega C^2 y^2 - 2\Omega CRyZ + \Omega CBZ^2, \end{aligned}$$

whence

$$am = X^2 + \Omega C y^2 - 2\Omega RyZ + \Omega BZ^2. \tag{14}$$

From (14) it follows that

$$X^2 + \Omega C y^2 - 2\Omega RyZ + \Omega BZ^2 \equiv 0 \pmod a, \tag{15}$$

* For any particular m this condition may be fulfilled (save possibly for a factor 2) by a suitable choice of a and C.

and since, in view of (7), $\Omega C \equiv -t^2$, $\Omega R \equiv ts$, $\Omega B \equiv -s^2 \pmod{a}$, we have

$$X^2 - t^2y^2 - 2tsyZ - s^2Z^2 \equiv 0 \pmod{a}, \quad X^2 - (ty + sZ)^2 \equiv 0 \pmod{a}.$$

Since a is an odd prime or a double of such a prime, either $X - ty - sZ \equiv 0$ or $-X - ty - sZ \equiv 0 \pmod{a}$. Thus, there exists an integer x such that either

$$X - ty - sZ = ax \tag{16$_1$}$$

or

$$-X - ty - sZ = ax, \tag{16$_2$}$$

that is, such that

$$\pm X = ax + ty + sZ. \tag{17}$$

Substituting $(ax+ty+sz)^2$ for X^2 in (14) we obtain, in view of (7),

$$am = (ax + ty + sZ)^2 + (ab - t^2)y^2 + 2(ar - st)yZ + (ac - s^2)Z^2,$$

whence

$$m = ax^2 + by^2 + cZ^2 + 2ryZ + 2sxZ + 2txy.$$

We now let

$$z = Z. \tag{18}$$

Then $f(x, y, z) = m$, and, since x and y determined by (12) and (16) are integers and Z is one by assumption, the integer m is represented by f.

From (13), (17) and (18) it follows that every common prime factor p of x, y, z divides X, Y, Z. Therefore if X, Y, Z are relatively prime, then so are x, y, z. The converse of the first statement is true for every prime p not dividing either a or C. For, if such a prime p divides X, Y, Z, then by (13) it divides y, by (17) it divides x, and by the choice of z in (18) it divides z. Thus if x, y, z are relatively prime, then the only possible common factors of X, Y, Z are divisors of a or C. But by virtue of (11) and the choice of a and C such common factors divide m. Hence the reservation of the converse of the second part of the theorem is sufficient.

3. **Application to universal forms.** Universal ternary quadratic forms were studied by Dickson,* who found the necessary and sufficient conditions that a form

$$\Phi = ex^2 + gy^2 + hz^2 \tag{19}$$

* Dickson, ibid., p. 21. Also this Bulletin, vol. 35 (1929), pp. 55–59.

should represent all integers, by Oppenheim* who studied forms with cross products and their equivalence to certain type forms, and by the present author,† who obtained conditions for universality of a ternary form in terms of its generic characters.

In this section we propose to show how by means of Theorem 3 and the normalization in §1, the criteria for universality for general forms with cross product terms may be deduced directly from the information available for forms of type (19).

The universality criteria in terms of generic characters run as follows.‡

THEOREM A. *Let f be a properly primitive, indefinite, classic,§ ternary, quadratic form with reciprocal F and determinant D. The necessary and sufficient conditions that f be universal are*

$$D = 2k + 1 \quad \text{or} \quad 2(2k + 1), \qquad \Omega = \pm 1 \tag{20}$$

where k is an integer, and, for every odd prime p dividing $\Delta = D$

$$(F \mid p) = (-\Omega \mid p). \tag{21}$$

THEOREM B. *Let f_1 be a primitive, indefinite, non-classic, ternary, quadratic form. Consider an improperly primitive form $f = 2f_1$. Let F be the reciprocal and Ω, Δ the invariants of f. Then f_1 is universal if and only if $f = 2f_1$ satisfies the following conditions*:

$$\Omega = \pm 1, \tag{22}$$

the characters of f are

$$(-1)^{(F-1)/2} = (-1)^{(\Omega+1)/2}, \qquad (F \mid p) = (-\Omega \mid p) \tag{23}$$

for every odd prime p dividing $\Delta = D$, and, in case 4 divides Δ,

$$(-1)^{(F^2-1)/8} = 1. \tag{24}$$

Noticing that conditions of Theorem A and relations (8) and (7_1) imply that the conditions of the above mentioned theorem of Dickson are fulfilled for the associated form G of f (see (10)), we may at once conclude that these conditions are sufficient.

To achieve the same for Theorem B, however, we need some addi-

* Oppenheim, Quarterly Journal of Mathematics (Oxford), vol. 1 (1930), pp. 179–185.

† Quarterly Journal of Mathematics, vol. 4 (1933), pp. 147–158.

‡ Ibid., pp. 147–148. There was a misprint in the statement of condition (1.51), our (23_1).

§ A classic form is one in which the coefficients of the cross products are all even. A form is non-classic if some or all of these coefficients are odd.

tional information about the form Φ in (19). We will proceed therefore to study forms of the type (19) and procure information permitting us not only to draw the conclusions of Theorem B, but also those of Theorem A. The procedure will be somewhat simplified by taking advantage of the fact that when the necessary conditions are imposed upon f the associated form G is of type (19) with $g=1$.

We first prove the following lemma.

LEMMA 1. *Consider a form*

$$\Phi(x, y, z) = ex^2 + y^2 + hz^2 = y^2 + \phi(x, z), \qquad eh = d, \tag{25}$$

such that

(26) $eh<0$ *and* $(e, h)=1$,

(27) $-h$ *and* $-e$ *are quadratic residues of* e *and* h *respectively.*

Then

$$\Phi \sim \Phi_1 = 2xy + y^2 - dz^2. \tag{28}$$

From (26) and (27), in view of a theorem due to Legendre* it follows that there exist integers λ, μ, ν relatively prime in pairs such that $\Phi(\lambda, \mu, \nu)=0$. Hence, by (25), $\phi(\lambda, \nu)=-\mu^2$, $(\lambda, \nu)=1$. Therefore, there exists a transformation carrying ϕ into an equivalent form

$$\phi(x, z) = (-\mu^2, M, N), \qquad M^2 + N\mu^2 = -eh = -d. \tag{29}$$

Henceforth the proof proceeds as in a similar lemma proved elsewhere.†

If we let $z=0$, $y=1$ or 2 in (28), we get

$$\Phi_1 = 2x + 1 \quad \text{or} \quad 4(x + 1). \tag{30}$$

Next if $d\equiv 2 \pmod 4$, take $z=1$, $y=2$. Then $\Phi_1=4(x+1)+d$. If d is odd take $z=1$, $y=1$ and $x=2u$ or $2u+1$ according as $d=4h-1$ or $4h+1$. Then $\Phi_1=4(u-h)+2$. In both cases Φ_1 is equal to any $4l+2$ by choice of y and u respectively. We thus obtain a second lemma.

LEMMA 2. *If* d *in* (28) *is odd or a double of an odd integer, then the form* Φ_1 *represents all integers. Should* $d\equiv 0 \pmod 4$, Φ_1 *would not be universal but would still represent all multiples of* 4 *by* (30_2).

We are ready now for the proof of Theorems A and B.

It is not difficult to see that the conditions (20)–(21) and (22)–(24) are necessary.‡

* For exposition see Dickson, *Introduction to the Theory of Numbers*, chap. 8.

† Quarterly Journal of Mathematics, vol. 4 (1933), §3, p. 150.

‡ Ibid., §§ 4 and 7.

We modify slightly the following portion of the proof just referred to.

If $\Delta \equiv 4 \pmod 8$, the only residues of $\Omega\Delta az^2$ modulo 64 are 0, $\Omega\Delta a$, 32, where $\Omega\Delta a \equiv 8 \pmod{16}$. If $C \equiv -\Omega+4 \pmod 8$ holds, we show as before that $CX^2+\Omega Y^2 \not\equiv 8, 24, 32, 40, 56 \pmod{64}$. Then the only possible residues modulo 64 which are congruent to 0 (mod 8) are 0, 16, 48 and those obtained by adding to them 0, 32, and $\Omega\Delta a$. But in this manner we obtain only seven residues 0, 16, 48, 32, $\Omega\Delta a$, $16+\Omega\Delta a$, $48+\Omega\Delta a$ which are congruent to 0 (mod 8) out of the possible eight. Therefore, $C \equiv -\Omega \pmod 8$ and (24) holds.

The sufficiency of the conditions (20)–(21) and (22)–(24) follows at once from the two lemmas of this section, in view of Theorem 3 and Theorems 1 and 2.

If f is universal, so is $-f$, and if conditions (20)–(21) or (22)–(24) hold for one, they also hold for the other. One of these has $\Delta < 0$, $\Omega > 0$. We may assume then that $\Omega = +1$. Then (10) becomes

$$G(X, Y, Z) = CX^2 + Y^2 + \Delta aZ^2. \tag{31}$$

Thus G is of type (25). Since f is indefinite, we have (26_1). Condition (26_2) holds by the choice of a and C. Next, condition (27) holds in view of (8), and (27_2) holds by (7_1), (20_1)–(21) or (23)–(24), according as f is properly or improperly primitive. Therefore, by Lemma 1, $G \sim \Phi_1$. If f is properly primitive, then $d = \Delta aC$ is odd or double an odd integer and hence (Lemma 2) Φ_1 and thus G represents all integers and therefore all multiples of aC. Then, by Theorem 3, f represents all integers.

If f is improperly primitive, $d = \Delta aC \equiv 0 \pmod 4$. By Lemma 2, Φ_1 represents all multiples of 4. That is, Φ_1 and therefore G represents all even multiples of aC. Then, by Theorem 3, f represents all even integers, and hence $f/2$ is universal.

In closing, it may be of interest to mention a theorem first conjectured and proved by Dickson:*

THEOREM C. *Every universal, classic or non-classic, ternary quadratic form is a zero form.*

A proof of this theorem in a more general setting was given by Albert.†

ST. LOUIS UNIVERSITY

* L. E. Dickson, *Studies in the Theory of Numbers*, Chicago, 1930, p. 17. Also cf. Dickson, *Modern Elementary Theory of Numbers*, Chicago, 1939, chap. 8.

† A. A. Albert, this Bulletin, vol. 39 (1933), pp. 585–588.