REDUCTIONS OF ENUMERATIONS IN HOMOGENEOUS FORMS*

BY E. T. BELL

1. *Introduction.* By carrying out the work in detail for the form $ax^2 + by^2 + cz^2$ we shall derive a useful set of reduction formulas, and illustrate a general process which can easily be applied to the reduction of the number $N(n = f)$ of representations of the integer n in any homogeneous form f of any degree in any number of variables. This set contains implicitly the complete set of corresponding reduction formulas for $Ax^2 + By^2 + Cz^2 + \cdots + Et^2$, in any number of indeterminates $x, y, z, \ldots, t$. The formulas in no case yield by themselves a complete evaluation of $N(n = f)$ for any type of n, but in many instances they materially simplify the problem, either by making the evaluation for f depend upon that for a simpler form, or by reducing the n to be represented to a more tractable type. By means of the process developed here, combined with elliptic function expansions, I have recently obtained several new complete enumerations for special ternary and quinary quadratic forms; the results will be published in other papers.

Before proceeding to the main discussion it will be instructive to glance at what is known concerning $N(n = f)$ in the simplest case (other than f linear), viz., $f \equiv ax^2 + by^2 + \cdots$; when the degree of f exceeds 2 even partial evaluations of $N(n = f)$ are at present unknown. It seems fair to say that the simplest case of all, $N(n = x^2 + by^2)$, $b > 0$, is still far from complete; Dirichlet's well known general theorem† for the number of representations by the totality of a system of representative forms of determinant—b

* Presented to the Society, San Francisco Section, April 5, 1924.

† Cf. Dickson's *History*, vol. 3, p. 19. References to the other citations of this introduction can be found by consulting the index to vol. 3, and running down the references to vol. 2.

does not of itself give a complete solution when the principal genus contains more than one class. For $f \equiv ax^2 + by^2 + cz^2$ there is the complete evaluation of $N(n = f)$ in the case $(a, b, c) = (1, 1, 1)$ by Gauss, an unproved statement of Liouville for $(a, b, c) = (1, 2, 3)$, partial results by Torelli for $(a, b, c) = (1, 1, 2)$, a special case of $(a, b, c) = (1, 2, 2)$ by Stieltjes, and beyond these apparently nothing detailed and specific for this $N(n = f)$. When $f \equiv ax^2 + by^2 + cz^2 + dt^2$, there is Jacobi's $N(n = f)$ for $(a, b, c, d) = (1, 1, 1, 1)$, several theorems of Liouville for $a = 1$ and each of $b, c, d = p^{\alpha}$ ($\alpha = 0, 1$; $p = 3, 5$) times a low power of 2, some similar results by Humbert when $p = 11$, or when $p = 3$, $\alpha = 2$, and Chapelon's evaluations when $p = 5$, $\alpha = 1, 2$. These appear to mark the limit of definite progress in this direction. Complete evaluations of $N(n = ax^2 + by^2 + \cdots)$ for more than 4 indeterminates $x, y, \ldots$ exist only for 5 and 7 squares. These remarks will indicate how far from satisfactory solutions even the simplest problems in the enumerative arithmetic of homogeneous forms still are.

The final formulas of this paper in § 5 have been checked. The nature of the work is such that this verifies all preceding formulas.

2. *Notation.* In all that follows p is prime, the integers n, a, b, c are prime to p, and a, b, c are coprime; k, M, A, B, C are arbitrary integers; $\alpha, \beta, \gamma, \delta$ are integers $\geqq 0$. To simplify the printing we shall write

$$N(p^{\alpha}n = ap^{\delta}x^2 + bp^{\beta}y^2 + cp^{\gamma}z^2) \equiv (\alpha; \delta, \beta, \gamma),$$

in which δ, β, γ (also a, b, c, n) are regarded as given constants. Note that $p^{\alpha}n$ is any integer.

3. *Lemma.* Although it may be obvious that

$$(1) \quad N(kM = kAx^2 + kBy^2 + kCz^2) = N(M = Ax^2 + By^2 + Cz^2),$$

we shall prove it, as upon this depends all that follows. The $\sum$ on the left extending to all integers $x, y, z \gtreqless 0$, that on the right to all integers M,

$$\sum q^{kAx^2 + kBy^2 + kCz^2} \equiv \sum q^{kM} N(kM = kAx^2 + kBy^2 + kCz^2).$$

In this replace q by $\sqrt[k]{q}$:

$$\sum q^{Ax^2+By^2+Cz^2} \equiv \sum q^M N(kM = kAx^2+kBy^2+kCz^2).$$

In the original identity take $k=1$:

$$\sum q^{Ax^2+By^2+Cz^2} \equiv \sum q^M N(M = Ax^2+By^2+Cz^2).$$

By comparing the second identity with the third we get (1).

By the notation explained in § 2, the evaluation of $N(M = Ax^2+By^2+Cz^2)$ is equivalent to that of $(\alpha;\ \delta,\ \beta,\ \gamma)$. By the lemma, if $\alpha < \delta, \beta, \gamma, (\alpha;\ \delta, \beta, \gamma) = 0$; if $\alpha \geqq \delta, (\alpha;\ \delta, \delta, \delta) = (\alpha - \delta;\ 1, 1, 1)$; while if $\delta,\ \beta,\ \gamma$ are unequal, one of them, say δ, is not greater than either of the others, and if $\alpha \geqq \delta,\ (\alpha;\ \delta,\ \beta+\delta,\ \gamma+\delta) = (\alpha-\delta;\ 0,\ \beta,\ \gamma)$.

Hence the evaluation of $N(M = Ax^2+By^2+Cz^2)$ is reduced to that of $(\alpha;\ 0,\ \beta,\ \gamma)$, in which, without loss of generality, we may assume $\gamma \geqq \beta$. Evidently the inequality $\gamma \geqq \beta$ (by the definitions of $\beta,\ \gamma$ in § 2) can be eliminated by replacing γ by $\gamma+\beta$ wherever γ occurs. Eliminations of this kind simplify the final formulas. The further evaluation of $N(M = Ax^2+By^2+Cz^2)$ is now reduced to that of $(\alpha;\ 0,\ \beta,\ \beta+\gamma)$.

4. *Preliminary Reductions.* Let $s \geqq 0$ be an integer such that $\alpha - 2s,\ \beta - 2s \geqq 0$, and therefore also $\beta+\gamma-2s \geqq 0$. Suppose for a moment that for some $s > 0$ we have $\alpha - 2s$, $\beta - 2s > 0$. If $(\alpha;\ 0,\ \beta,\ \beta+\gamma) > 0$, then must $x \equiv 0 \bmod p$, and therefore by s applications of the Lemma (§ 3),

$$(2) \qquad (\alpha;\ 0,\ \beta,\ \beta+\gamma) = (\alpha-2s;\ 0,\ \beta-2s,\ \beta+\gamma-2s),$$

which obviously remains true when $s=0$ and when $(\alpha;\ 0,\ \beta,\ \beta+\gamma) = 0$. Choose for s the lesser of $[\alpha/2]$, $[\beta/2]$, where $[t]$ is the greatest integer $\leqq t$; when $\alpha = \beta$, take $s = [\beta/2]$. Clearly the reductions (2) can be performed precisely s times, s being as just chosen. Separating out the cases of (2) for even and odd values of β we get

(1. 1) $\alpha \leqq \beta,\ (2\alpha;\ 0, 2\beta, 2\beta+\gamma) = (0;\ 0,\ 2\beta-2\alpha,\ 2\beta+\gamma-2\alpha)$;

(1. 2) $\alpha \geqq \beta,\ (2\alpha;\ 0,\ 2\beta,\ 2\beta+\gamma) = (2\alpha-2\beta;\ 0,\ 0,\ \gamma)$;

$$(1.3)\ \alpha \leqq \beta,\ (2\alpha+1;\ 0,\ 2\beta,\ 2\beta+\gamma) = (1;\ 0,\ 2\beta-2\alpha,\ 2\beta+\gamma-2\alpha);$$

$$(1.4)\ \alpha \geqq \beta,\ (2\alpha+1;\ 0, 2\beta, 2\beta+\gamma) = (2\alpha+1-2\beta;\ 0, 0, \gamma);$$

and the complementary set,

$$(2.1)\ \alpha \leqq \beta,\ (2\alpha;\ 0,\ 2\beta+1,\ 2\beta+\gamma+1) = (0;\ 0,\ 2\beta+1-2\alpha,\ 2\beta+\gamma+1-2\alpha);$$

$$(2.2)\ \alpha \geqq \beta,\ (2\alpha;\ 0,\ 2\beta+1,\ 2\beta+\gamma+1) = (2\alpha-2\beta;\ 0,\ 1,\ \gamma+1);$$

$$(2.3)\ \alpha \leqq \beta,\ (2\alpha+1;\ 0,\ 2\beta+1,\ 2\beta+\gamma+1) = (1;\ 0,\ 2\beta+1-2\alpha,\ 2\beta+\gamma+1-2\alpha);$$

$$(2.4)\ \alpha \geqq \beta,\ (2\alpha+1;\ 0,\ 2\beta+1,\ 2\beta+\gamma+1) = (2\alpha+1-2\beta;\ 0,\ 1,\ \gamma+1).$$

Only those on the right having a pair of zeros in the symbol are irreducible. The further reduction of the rest is effected in a similar way, first powers of the prime p, instead of second, being now successively eliminated. The process is seen by examining the right of (1. 3), (2. 3). When $\alpha < \beta$ we have $2\beta-2\alpha \geqq 2$, $2\beta+\gamma-2\alpha \geqq 2$, and since pn is the number represented in the right of (1. 3), it follows that $x \equiv 0 \bmod p$. Applying the lemma, we get

$$(1;\ 0,\ 2\beta-2\alpha,\ 2\beta+\gamma-2\alpha) = (0;\ 1,\ 2\beta-2\alpha-1,\ 2\beta+\gamma-2\alpha-1),$$

and this evidently vanishes (when $\alpha < \beta$). Similarly for (2. 3), and we have

$$(1.31)\ \alpha < \beta,\ (2\alpha+1;\ 0,\ 2\beta,\ 2\beta+\gamma) = 0;$$

$$(2.31)\ \alpha < \beta,\ (2\alpha+1;\ 0,\ 2\beta+1,\ 2\beta+\gamma+1) = 0,$$

which may replace (1. 3), (2. 3), since the cases $\alpha = \beta$ are included in (1. 4), (2. 4).

Similarly, provided that $\alpha-2s$, $\gamma-2s+1 \geqq 0$, we get

$$(\alpha;\ 0,\ 1,\ \gamma+1) = (\alpha-2s;\ 0,\ 1,\ \gamma+1-2s),$$

and, provided that $\alpha-1-2s$, $\gamma-2s \geqq 0$,

$$(\alpha;\ 0,\ 1,\ \gamma+1) = (\alpha-1-2s;\ 1,\ 0,\ \gamma-2s).$$

Upon separation of cases according to even, odd γ, these yield the formulas which enable us to complete the reduction of (1. 1)—(2. 4). It is unnecessary to preserve the very simple calculations. We find

(3. 1) $\alpha \leqq \gamma+1$, $(2\alpha;\ 0, 1, 2\gamma+2) = (0;\ 0, 1, 2\gamma+2-2\alpha)$;
(3. 2) $\alpha \geqq \gamma+1$, $(2\alpha;\ 0, 1, 2\gamma+2) = (2\alpha-2\gamma-2;\ 0, 1, 0)$;
(3. 3) $\alpha \leqq \gamma$, $(2\alpha+1;\ 0, 1, 2\gamma+2) = (0;\ 1, 0, 2\gamma+1-2\alpha)$;
(3. 4) $\alpha \geqq \gamma+1$, $(2\alpha+1;\ 0, 1, 2\gamma+2) = (2\alpha-2\gamma-1;\ 0, 1, 0)$,

and the complementary set

(4. 1) $\alpha \leqq \gamma$, $(2\alpha;\ 0, 1, 2\gamma+1) = (0;\ 0, 1, 2\gamma+1-2\alpha)$;
(4. 2) $\alpha \geqq \gamma+1$, $(2\alpha;\ 0, 1, 2\gamma+1) = (2\alpha-2\gamma-1;\ 1, 0, 0)$;
(4. 3) $\alpha \leqq \gamma$, $(2\alpha+1;\ 0, 1, 2\gamma+1) = (0;\ 1, 0, 2\gamma-2\alpha)$;
(4. 4) $\alpha \geqq \gamma$, $(2\alpha+1;\ 0, 1, 2\gamma+1) = (2\alpha-2\gamma;\ 1, 0, 0)$,

all of which are further irreducible. Note that since γ may take the value zero, $(\alpha;\ 0, 1, 2\gamma)$ is not necessarily reducible, while the type considered, $(\alpha;\ 0, 1, 2\gamma+2)$, is.

Apply (3. 1)—(4. 4) to (2. 2), (2. 4) after having first eliminated the condition $\alpha \geqq \beta$ by replacing α wherever it occurs by $\beta+\alpha$. The results are:

(5. 1) $\alpha \leqq \gamma$, $(2\beta+2\alpha;\ 0, 2\beta+1, 2\beta+2\gamma+1)$
$= (0;\ 0, 1, 2\gamma+1-2\alpha)$;
(5. 2) $\alpha \geqq \gamma+1$, $(2\beta+2\alpha;\ 0, 2\beta+1, 2\beta+2\gamma+1)$
$= (2\alpha-2\gamma-1;\ 1, 0, 0)$;
(5. 3) $\alpha \leqq \gamma$, $(2\beta+2\alpha+1;\ 0, 2\beta+1, 2\beta+2\gamma+1)$
$= (0;\ 1, 0, 2\gamma-2\alpha)$;
(5. 4) $\alpha \geqq \gamma$, $(2\beta+2\alpha+1;\ 0, 2\beta+1, 2\beta+2\gamma+1)$
$= (2\alpha-2\gamma;\ 1, 0, 0)$;

and the complementary set,

(6. 1) $\alpha \leqq \gamma+1$, $(2\beta+2\alpha;\ 0, 2\beta+1, 2\beta+2\gamma+2)$
$= (0;\ 0, 1, 2\gamma+2-2\alpha)$;
(6. 2) $\alpha \geqq \gamma+1$, $(2\beta+2\alpha;\ 0, 2\beta+1, 2\beta+2\gamma+2)$
$= (2\alpha-2\gamma-2;\ 0, 1, 0)$;
(6. 3) $\alpha \leqq \gamma$, $(2\beta+2\alpha+1;\ 0, 2\beta+1, 2\beta+2\gamma+2)$
$= (0;\ 1, 0, 2\gamma+1-2\alpha)$;
(6. 4) $\alpha \geqq \gamma+1$, $(2\beta+2\alpha+1;\ 0, 2\beta+1, 2\beta+2\gamma+2)$
$= (2\alpha-2\gamma-1;\ 0, 1, 0)$.

Examining (1. 1)—(2. 4) and (5. 1)—(6. 4) we see it is necessary to consider only

$$(7)\qquad N(p^\alpha n = ax^2 + bp^{2\beta}y^2 + cp^{2\beta+\gamma}z^2) \equiv N_1(p^\alpha n),$$

$$(8)\qquad N(p^\alpha n = ax^2 + bp^{2\beta+1}y^2 + cp^{2\beta+2\gamma+1}z^2) \equiv N_2(p^\alpha n),$$

$$(9)\qquad N(p^\alpha n = ax^2 + bp^{2\beta+1}y^2 + cp^{2\beta+2\gamma+2}z^2) \equiv N_3(p^\alpha n),$$

in order, by the reductions in § 3, to obtain a complete set of reduction formulas for

$$(10)\qquad N(M = Ax^2 + By^2 + Cz^2).$$

That the three sets in § 5 are exhaustive is evident by inspection on referring to the notation in § 2.

5. *Final Formulas.* For the N_i $(i = 1, 2, 3)$ see (7), (8), (9). From (1. 1)—(1. 4) and (1. 31), by eliminating the condition $\alpha \geqq \beta$, we find

(I) *Form* $\qquad ax^2 + bp^{2\beta}y^2 + cp^{2\beta+\gamma}z^2$:

$$\begin{aligned}
\alpha \leqq \beta,\ & N_1(p^{2\alpha}n) = (0;\ 0,\ 2\beta - 2\alpha,\ 2\beta + \gamma - 2\alpha);\\
\alpha < \beta,\ & N_1(p^{2\alpha+1}n) = 0;\\
& N_1(p^{2\beta+\alpha}n) = (\alpha;\ 0,\ 0,\ \gamma).
\end{aligned}$$

From (2. 1), (2. 31) with γ replaced by 2γ, and from (5. 1)—(5. 4) we find upon eliminating $\alpha \geqq \gamma + 1$, $\alpha \geqq \gamma$.

(II) *Form* $\qquad ax^2 + bp^{2\beta+1}y^2 + cp^{2\beta+2\gamma+1}z^2$:

$$\begin{aligned}
\alpha \leqq \beta,\ & N_2(p^{2\alpha}n) = (0;\ 0,\ 2\beta + 1 - 2\alpha,\ 2\beta + 2\gamma = 1 - 2\alpha);\\
\alpha < \beta,\ & N_2(p^{2\alpha+1}n) = 0;\\
\alpha \leqq \gamma,\ & N_2(p^{2\beta+2\alpha}n) = (0;\ 0,\ 1,\ 2\gamma + 1 - 2\alpha);\\
& N_2(p^{2\beta+2\gamma+2\alpha+2}n) = (2\alpha + 1;\ 1,\ 0,\ 0);\\
\alpha \leqq \gamma,\ & N_2(p^{2\beta+2\alpha+1}n) = (0;\ 1,\ 0,\ 2\gamma - 2\alpha);\\
& N_2(p^{2\beta+2\gamma+2\alpha+1}n) = (2\alpha;\ 1,\ 0,\ 0).
\end{aligned}$$

From (2. 1), (2. 31) with γ replaced by $2\gamma + 1$, and from (6. 1)—(6. 4) upon elimination of $\alpha \geqq \gamma + 1$ we find

(III) *Form* $\qquad ax^2 + bp^{2\beta+1}y^2 + cp^{2\beta+2\gamma+2}z^2$:

$$\begin{aligned}
\alpha \leqq \beta,\ & N_3(p^{2\alpha}n) = (0;\ 0,\ 2\beta + 1 - 2\alpha,\ 2\beta + 2\gamma + 2 - 2\alpha);\\
\alpha < \beta,\ & N_3(p^{2\alpha+1}n) = 0;
\end{aligned}$$

$\alpha \leqq \gamma + 1,\ N_3(p^{2\beta+2\alpha}n) = (0;\ 0,\ 1,\ 2\gamma + 2 - 2\alpha);$

$N_3(p^{2\beta+2\gamma+2\alpha+2}n) = (2\alpha;\ 0,\ 1,\ 0);$

$\alpha \leqq \gamma,\ N_3(p^{2\beta+2\alpha+1}n) = (0;\ 1,\ 0,\ 2\gamma + 1 - 2\alpha);$

$N_3(p^{2\beta+2\gamma+2\alpha+3}n) = 2\alpha + 1;\ 0,\ 1,\ 0).$

In all of the above no further reduction is possible.

6. *Successive Reductions.* Let D be the greatest common divisor of B, C in (10), and assume without loss of generality (§ 3) that M, A, B, C are relatively prime in their totality. Let $M = M'p^\alpha$, where p is any prime divisor of D, and M' is prime to p. Apply (I)—(III) of § 5. Repeat the process on the results for each remaining prime divisor of D, obtaining finally a system of formulas analogous to (I)—(III) in which (10), for its several possible cases according to the prime factors of D, is replaced by a corresponding $N(M'p^{\alpha'} = A'x^2 + B'y^2 + C'z^2)$ in which no further reduction with respect to B', C' is possible. This system of formulas may conveniently be written as a set of equalities between r-rowed matrices, where r is the number of distinct prime factors of D. To each pair of A, B, C in (10) will correspond such a system of equalities, and all three together give the complete reduction of (10). It would be of interest to discuss this set.

7. (IV) *Form* $Ax^2 + By^2 + Cz^2 + \cdots + Et^2$. As in § 3 the reduction for this form is referred to that of

$$N(p^\alpha n = x^2 + p^\beta y^2 + p^{\beta+\gamma}z^2 + \cdots + p^{\beta+\gamma+\cdots+\varepsilon}\ t^2),$$

where $\beta, \gamma, \ldots, \varepsilon$ are integers $\geqq 0$, and a precisely similar argument shows immediately that this N is reduced when $N(p^\alpha n = x^2 + p^\beta y^2 + p^{\beta+\gamma}z^2)$ is reduced. The complete set of reduction formulas can be written down from § 5.

8. *General Form.* When the degree of f is $3 + \alpha$, the process of reducing $N(n = f)$ is evident from the foregoing; the discussion now depends upon $[k/(3 + \alpha)]$ instead of $[k/2]$.

THE UNIVERSITY OF WASHINGTON