193. *A determinant of linear forms*, to appear in Mathematika 18 (1971).
194. *Homogeneous quadratic equations*, to appear in Mathematika 18 (1971).
195. (with D. J. Lewis) *Values of positive definite forms in many variables*, to appear in Acta Arith.

ACTA ARITHMETICA
XVIII (1971)

The least common denominator of the coefficients of a perfect quadratic form

by

G. L. WATSON (London)

1. Introduction. Let n be any positive integer, and f a perfect n-ary quadratic form, with minimum 1. Then, as is well known, the coefficients of f are all rational; we denote their least common denominator by $q(f)$, and prove:

THEOREM 1. *With the foregoing notation*

$$q(f) \leqslant \gamma_n^{\frac{1}{2}n(n+1)} \tag{1.1}$$

where γ_n *is the Hermite constant.*

It is well known that γ_n/n is bounded, so (1.1) implies

$$\log q(f) < \tfrac{1}{2}(1+\varepsilon)n^2 \log n \tag{1.2}$$

for $\varepsilon > 0$ and $n > n_0(\varepsilon)$.

Theorem 1 seems very weak, and indeed it is so for small n. The possibilities for f up to equivalence are all known for $n \leqslant 6$, see [4] and [1], and by looking at them we see that $q(f) = 1$ for $n \leqslant 4$, $q(f) \leqslant 2$ for $n = 5, 6$. If we restrict f further to be absolutely extreme, then $q(f) = 1$ for $n \leqslant 8$, see [2]. Direct proofs of these improvements, or of slightly weaker ones, on (1.1) would be of interest; they might lead to easier proofs of the results of Barnes and Blichfeldt.

I have however failed to find any useful numerical results of this kind; so instead I show that for large n (1.1) is not as weak as it looks. Defining q_n as the supremum of $q(f)$ for given n, we shall see that

$$n^{-\frac{1}{2}} \log q_n \to \infty \quad \text{as} \quad n \to \infty. \tag{1.3}$$

The proof of (1.3) will be such as to suggest the conjecture that the exponent $-\frac{1}{2}$ can be replaced by -1.

2. Lower bounds for q_n. For $n = 1, 2, \ldots,$ we define $Q(n)$ as the (finite) set of positive integer values assumed by $q(f)$, defined above, for perfect n-ary f with minimum 1; whence q_n is the greatest member of $Q(n)$. We shall prove three theorems.

THEOREM 2. *For each odd* $n \geqslant 5$, $\frac{1}{2}(n-1) \in Q(n)$, *whence* $q_n \geqslant \frac{1}{2}(n-1)$.

THEOREM 3. *Let* (h_m, n_m), $m = 1, \ldots, r$, *be any* $r \geqslant 2$ *ordered pairs of positive integers such that*

$$h_m | q_m \quad \text{for some } q_m \in Q(n_m), \quad m = 1, \ldots, r. \tag{2.1}$$

Then for every n *with*

$$n \geqslant n_1 + \ldots + n_r, \tag{2.2}$$

there exists q *with*

$$q \in Q(n) \quad \text{and} \quad h_m | q \quad \text{for} \quad m = 1, \ldots, r; \tag{2.3}$$

whence, trivially, q_n *is not less than the least common multiple of the* h_m.

By taking $r = 2$, $n_1 = n-1$, $n_2 = 1$, $h_1 = q_{n-1}$, and $h_2 = 1$, as we clearly may, we have:

COROLLARY TO THEOREM 3. $q_n \geqslant q_{n-1}$ *for* $n \geqslant 2$.

THEOREM 4. *For* $\varepsilon > 0$ *and* $n > n_0(\varepsilon)$ *we have*

$$\log q_n > (1-\varepsilon)(\tfrac{1}{2} n \log n)^{\frac{1}{2}}, \tag{2.4}$$

implying (1.3).

3. Preliminaries for Theorem 1. Using the notation

$$\boldsymbol{\xi} = \operatorname{col}\{\xi_1, \ldots, \xi_n\} \tag{3.1}$$

for a column vector with n real elements, we define $\boldsymbol{\xi}^*$, with $n^* = \frac{1}{2}n(n+1)$ elements $\xi_i \xi_j$, $1 \leqslant i \leqslant j \leqslant n$, by (3.1) and

$$\boldsymbol{\xi}^* = \operatorname{col}\{\xi_1^2, \xi_1\xi_2, \ldots, \xi_1\xi_n, \xi_2^2, \ldots, \xi_n^2\}. \tag{3.2}$$

Then more generally, if M is an n by s matrix, with jth column m_j, we define M^* as the n^* by s matrix whose jth column is m_j^*. Now if T is any real non-singular n by n^* matrix, we need to know that

$$(TM^*) = UM^*, \quad \text{with} \quad \det U = \pm(\det T)^{n+1}, \tag{3.3}$$

where $U = U(T)$ is a real n^* by n^* matrix.

If T is a diagonal or a permutation matrix, or if premultiplication of $\boldsymbol{\xi}$ by T is equivalent to putting $\xi_1 + \xi_2$ for ξ_1, then (3.3) is easily verified. Factorizing T by elementary row operations, the general case (3.3) follows, as in [5], from these special ones.

If f is a positive-definite n-ary quadratic form we may, by completing the square, write

$$f(\boldsymbol{x}) = f(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i \{x_i + L_i(x_{i+1}, \ldots, x_n)\}^2, \tag{3.4}$$

where the a_i are positive constants and the L_i linear forms (L_n indentically 0). The substitution

$$x_i + L_i(x_{i+1}, \ldots, x_n) = a_i^{-\frac{1}{2}}(a_1 a_2 \ldots a_n)^{1/2n} \xi_i \quad (i = 1, \ldots, n) \tag{3.5}$$

takes $f(\boldsymbol{x})$ into

$$(a_1 a_2 \ldots a_n)^{1/n}(\xi_1^2 + \xi_2^2 + \ldots + \xi_n^2). \tag{3.6}$$

We now restrict f to have minimum $\geqslant 1$, that is, to satisfy

$$f(\boldsymbol{x}) \geqslant 1 \quad \text{for integers } x_1, \ldots, x_n \neq 0, \ldots, 0. \tag{3.7}$$

From (3.4) and (3.7) we have

$$a_1 a_2 \ldots a_n \geqslant \gamma_n^{-n}; \tag{3.8}$$

this implication is essentially the definition of γ_n.

Now clearly there is a T, with $\det T = 1$, such that (3.5) can be expressed as $\boldsymbol{\xi} = T\boldsymbol{x}$, whence, see (3.6), (3.8),

$$\boldsymbol{\xi} = T\boldsymbol{x} \quad \text{and} \quad f(\boldsymbol{x}) = 1 \quad \text{imply} \quad \xi_1^2 + \xi_2^2 + \ldots + \xi_n^2 \leqslant \gamma_n. \tag{3.9}$$

And (3.3), with $\det T = 1$, gives

$$|\det M^*| = |\det(TM)^*| \quad \text{if } M \text{ is } n \text{ by } n^*. \tag{3.10}$$

4. Proof of Theorem 1. Denote by $a_{ij} = a_{ji}$ the coefficient of $x_i x_j$ in f; then since f is perfect, with minimum 1, there are $s \geqslant n^* = \frac{1}{2}n(n+1)$ cases

$$\sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j = 1 \tag{4.1}$$

(with integers x_i) of equality in (3.7). And further, these s linear equations in the a_{ij} determine the a_{ij} uniquely. It is clearly possible to choose a subset of precisely n^* of the equations (4.1) which also determine the a_{ij} uniquely; and to write these equations as

$$(a_{11}, a_{12}, \ldots, a_{1n}, a_{22}, \ldots, a_{nn}) X^*(f) = \operatorname{col}\{1, \ldots, 1\}, \tag{4.2}$$

where $X(f)$ is an n by n^* matrix, with columns $\boldsymbol{x}$ each satisfying (4.1), that is $f(\boldsymbol{x}) = 1$. $X^*(f)$ is n^* by n^* and non-singular, with integral elements. Evidently (4.2) implies that the a_{ij} are all rational, and that their least common denominator $q(f)$ divides $\det X^*(f) \neq 0$, so

$$q(f) \leqslant |\det X^*(f)|. \tag{4.3}$$

Using the T of § 3 with the properties (3.9), (3.10), and putting $M = X(f)$, $Y = TM$, (4.3) gives

$$q(f) \leqslant |\det Y^*| = (\det Y^{*\prime} Y^*)^{\frac{1}{2}}, \tag{4.4}$$

where $Y^{*\prime}$ is the transpose of Y^*. By construction, each column $\boldsymbol{\xi}$ of Y satisfies the inequality in (3.9); and we have $\det Y^* \neq 0$.

Now $Y^{*\prime}Y^*$ is a positive-definite matrix, and so its determinant does not exceed the product of its diagonal elements. So from (4.4) we have

$$q^2(f) \leqslant \prod_{\xi} (\xi_1^4 + \xi_1^2\xi_2^2 + \ldots + \xi_2^4 + \ldots + \xi_n^4), \tag{4.5}$$

where ξ ranges over the n^* columns of Y.

Crudely, (4.5) gives

$$q(f) \leqslant \prod_{\xi} (\xi_1^2 + \xi_2^2 + \ldots + \xi_n^2), \tag{4.6}$$

whence since the ξ all satisfy the inequality in (3.9) we have (1.1) and the proof of Theorem 1 is complete.

The argument is crude at several steps, so presumably (1.1) is true with a good deal to spare — except when $n = \gamma_n = 1$. A little improvement is possible if we replace (4.5) by

$$q^2(f) \leqslant \gamma_n^{n(n+1)} \prod_{\eta} (\eta_1^4 + \eta_1^2\eta_2^2 + \ldots + \eta_n^4) \tag{4.7}$$

$$= \gamma_n^{n(n+1)} \prod_{\eta} (\tfrac{1}{2} + \tfrac{1}{2}\eta_1^4 + \ldots + \tfrac{1}{2}\eta_n^4),$$

with each η satisfying

$$\eta_1^2 + \eta_2^2 + \ldots + \eta_n^2 = 1. \tag{4.8}$$

Then it is not hard to see that the expression $\frac{1}{2} + \sum \eta_i^4$ in (4.7) may be replaced by its mean over the sphere (4.8), which is $(n+5)/(2n+4)$.

I leave the details of this argument to the reader, since it neither improves on (1.2) for large n nor gives useful numerical results for $n = 6, 7, 8$.

5. Proof of Theorem 2. We write $n = 2k-1$, k an integer $\geqslant 3$, since $n \geqslant 5$ is odd. We write for brevity

$$y_i = \begin{cases} x_1 & \text{for } i = 1, \\ x_1 + kx_i & \text{for } i = 2, \ldots, n, \\ -(y_1 + \ldots + y_n) & \text{for } i = n+1 = 2k. \end{cases} \tag{5.1}$$

We define f by

$$2k(k-1)f(x_1, \ldots, x_n) = y_1^2 + \ldots + y_{2k}^2, \tag{5.2}$$

and it suffices to prove that this makes f perfect, with minimum 1 and with $q(f) = k-1 = \frac{1}{2}(n-1)$. The x_i are all integers if and only if the y_i

are all integers and satisfy

$$y_1 = \ldots = y_{2k} \pmod{k} \tag{5.3}$$

and

$$y_1 + \ldots + y_{2k} = 0. \tag{5.4}$$

We note that (5.3) implies $y_i^2 \equiv y_j^2 \pmod{m}$, with $m = k$ if $2 \nmid k$, $m = 2k$ if $2 | k$. So (5.3) and (5.4) imply

$$y_1^2 + \ldots + y_{2k}^2 \equiv 0 \pmod{2k}. \tag{5.5}$$

We consider the two cases

$$k | y_1, \ldots, y_{2k} \neq 0, \ldots, 0 \tag{5.6}$$

and

$$y_1 \equiv \ldots \equiv y_{2k} \equiv h \pmod{k}, \quad 1 \leqslant h \leqslant \tfrac{1}{2}k, \tag{5.7}$$

with (5.3), (5.4), in either case.

(i) Clearly (5.6) implies that at least two of the $|y_i|$ are positive multiples of k, whence $\sum y_i^2 \geqslant 2k^2$, equality being obviously possible.

(ii) In case (5.7), y_i^2 is least when each y_i is either h or $h-k$. But then, by (5.4), y_i takes these two values for $k-h$, h values of i respectively, and so

$$y_1^2 + \ldots + y_{2k}^2 = 2(k-h)h^2 + 2h(k-h)^2 = 2hk(k-h) \geqslant hk^2.$$

We therefore have

$$y_1^2 + \ldots + y_{2k}^2 \geqslant 2k(k-1)$$

with equality only when $h = 1$.

Now (5.5) and (i), (ii) above show that $(k-1)f$ is an integer-valued and primitive form, with minimum $k-1$ (primitive since by (i) it also takes the value k). So we have proved all that is required, except that f is perfect. We have also established that the only minimum points of f, in terms of the y_i but omitting the redundant y_{2k}, are the permutations of $\pm\mathrm{col}\{1, \ldots, 1, 1-k\}$ and of $\pm\mathrm{col}\{1, \ldots, 1-k, 1-k\}$.

To prove perfection, it suffices to show that any form which vanishes at all these minimum points must vanish identically. Let

$$g = g(y_1, \ldots, y_n) = \sum b(i,j) y_i y_j$$

be such a form; with summation over $1 \leqslant i \leqslant j \leqslant n$ (but, for convenience, with $b(i,j) = b(j,i)$ when $i > j$). Then the $b(i,j)$ have to satisfy a system of equations got by permuting the coordinates in $g(1, \ldots, 1, 1-k) = 0$ and in $g(1, \ldots, 1, 1-k, 1-k) = 0$. And we must deduce that the $b(i,j)$ all vanish.

If we permute and add the two equations just written it is not difficult to see that $\sum b(i,i) = 0$ and $\sum_{i<j} b(i,j) = 0$. Then the two equations can be written more simply as

$$(5.8)\qquad kb(n,n) = b(1,n)+\ldots+b(n-1,n),$$

$$(5.9)\qquad kb(n,n)+kb(n,n-1)+kb(n-1,n-1) = \sum_{i\leq n-2}\{b(i,n)+b(i,n-1)\}.$$

Interchange n and $n-1$ in (5.8), then add the result to (5.8) as it stands, and subtract from (5.9); this gives $b(n-1,n) = 0$. Now by symmetry $b(i,j) = 0$ for $i\neq j$; (5.8) gives $b(n,n) = 0$, and symmetry gives $b(i,i) = 0$. This completes the proof.

6. Proof of Theorem 3. We notice first that $1\in Q(1)$ (consider the perfect form x_1^2); so, by putting in $n-\sum n_m$ ordered pairs $(1,1)$, we see that it suffices to consider the case in which equality holds in (2.2); that is, $n = n_1+\ldots+n_r$.

We next note that if the case $r = 2$ has been proved then for $r\geqslant 3$ we can replace the two pairs $(h_1,n_1),(h_2,n_2)$ by (h', n_1+n_2), with h' a common multiple of h_1, n_1. So the case $r\geqslant 3$ can be dealt with by induction on r. We therefore suppose $r = 2$. For convenience, we write $n_1 = \nu$; the $n_2 = n-n_1 = n-\nu$. We choose two perfect forms f_1, f_2, each with minimum 1, in ν, $n-\nu$ variables respectively, with

$$(6.1)\qquad h_1|q(f_1),\qquad h_2|q(f_2).$$

And we consider the disjoint form

$$(6.2)\qquad f_1(x_1,\ldots,x_\nu)+f_2(x_{\nu+1},\ldots,x_n).$$

The following well known result is proved in substance in [6], pp. 105–107:

Lemma. *Let $f = f(x_1,\ldots,x_n)$ be a positive-definite n-ary quadratic form with minimum 1 which is not perfect. Then there exists an n-ary quadratic form g such that:*

(i) *$f+g$ is perfect, with minimum 1;*

(ii) *$g(x_1,\ldots,x_n) = 0$ whenever the x_i are integers satisfying $f(x_1,\ldots,x_n) = 1$.*

By definition, f, with minimum 1, is perfect if every g having property (ii) above is identically 0. Now we take f to be the form (6.2), and apply the Lemma. By (ii), $g_1 = g(x_1,\ldots,x_\nu,0,\ldots,0) = 0$ for every set of integers $x_1,\ldots,x_\nu$ satisfying $f_1(x_1,\ldots,x_\nu) = 1$. So, by the definition of perfection, g_1 is identically 0. Similarly, $g_2 = g(0,\ldots,0,x_{\nu+1},\ldots,x_n)$ is identically 0.

Hence we may write $g = b(x_1,\ldots,x_\nu; x_{\nu+1},\ldots,x_n)$, where b is a bilinear form in the two sets of ν, $n-\nu$ variables. And the form $f+g$, which by (i) is perfect with minimum 1, is of the shape

$$(6.3)\qquad f_1(x_1,\ldots,x_\nu)+b(x_1,\ldots,x_\nu;x_{\nu+1},\ldots,x_n)+f_2(x_{\nu+1},\ldots,x_n).$$

Call this form Φ and let $a_{ij} = a_{ji}$ be the coefficent of x_ix_j in Φ. The theorem follows, by (6.1), if we prove that $q(f_1)$ and $q(f_2)$ are divisors of $q(\Phi)$. But this is trivial; we have $q(f_1)|q(\Phi)$ by considering only the a_{ij} with $i,j\leqslant\nu$, which are the coefficients of f_1, and similarly for f_2.

So the theorem is proved; and we observe that we might do better if we had some control over the coefficients of b.

7. Proof of Theorem 4. We suppose $\varepsilon > 0$ given (and < 1) and n large. We denote the mth prime by p_m and note that

$$(7.1)\qquad p_m\sim m\log m\quad\text{as}\quad m\to\infty.$$

This (see [3], 10, Theorem 8*), is a simple consequence of the prime number theorem.

We choose a large $r = r(n)$ so that

$$(7.2)\qquad n\geqslant 2(p_1+p_2+\ldots+p_r)+r.$$

Taking r as large as we can, so that (7.2) becomes false if r is replaced by $r+1$, we find by (7.1) that (for n large enough) we have

$$(7.3)\qquad n < (1+\tfrac{1}{4}\varepsilon)r^2\log r,$$

whence

$$(7.4)\qquad \log r > \tfrac{1}{2}(1-\tfrac{1}{4}\varepsilon)\log n.$$

Now by (7.2) and Theorem 2, the hypotheses of Theorem 3 can be satisfied by taking $h_m = p_m$, $n_m = 2p_m+1$. Then the least common multiple of the h_m is their product, so Theorem 3 gives $q_n\geqslant p_1\ldots p_r$. With (7.1) this gives

$$(7.5)\qquad \log q_n > (1-\tfrac{1}{4}\varepsilon)r\log r.$$

From (7.3)–(7.5) we have

$$(\log q_n)^2 > (1-\tfrac{1}{2}\varepsilon)(r\log r)^2$$
$$> \tfrac{1}{2}(1-\tfrac{3}{4}\varepsilon)r^2(\log r)(\log n) > \tfrac{1}{2}(1-\varepsilon)n\log n,$$

whence we have (2.4) and (1.3), and Theorem 4 is proved.

Now, by the remark at the end of § 6, we have, in effect, constructed an n-ary perfect form, and of its $\frac{1}{2}n(n+1)$ coefficients the number we have used is

$$\tfrac{1}{2}\sum n_m(n_m+1)\sim 2\sum p_m^2.$$

The ratio of this expression to $\frac{1}{2}n(n+1)$ is asymptotic to $2/3r < n^{\varepsilon-1/2}$. This is the foundation for the conjecture stated at the end of § 1.

References

[1] E. S. Barnes, *The complete enumeration of extreme senary forms*, Philos. Trans. Roy. Soc., London, Ser. A, 249 (1957), pp. 461–506.
[2] H. F. Blichfeldt, *The minimum values of positive quadratic forms in six, seven and eight variables*, Math. Zeitschr. 39 (1935), pp. 1–15.
[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, first edition, Oxford 1938.
[4] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. 11 (1877), pp. 242–292.
[5] R. A. Rankin, *On the minimal points of perfect quadratic forms*, Math. Zeitschr. 84 (1964), 228–232.
[6] G. Voronoi, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. Reine Angew. Math. 133 (1908), pp. 97–178.

UNIVERSITY COLLEGE
London, England

Received on 15. 9. 1969

ACTA ARITHMETICA
XVIII (1971)

Some elliptic function identities

by

J. W. S. Cassels (Cambridge)

Harold Davenport in memoriam

0. Introduction. In the course of some calculations about elliptic curves defined over finite fields I was led to identities about the coefficients of classical elliptic functions. These appear to be new, although they are entirely in the spirit of 19th century analysis. In this introduction I shall first enunciate the complex function identities and then describe the application to finite fields. The proofs will be given in the remainder of the paper.

I am grateful to Mr. A. D. McGettrick for some useful discussions and in particular for his contribution to § 6.

As we shall want to specialize mod p later, we must be rather more pedantic in the discussion of the complex function identities than would otherwise be appropriate.

Let x, A, B be independent indeterminates over some field k of characteristic 0 and define y by

$$y^2 = x^3+Ax+B. \tag{0.1}$$

We regard y as a formal series in $x^{-1/2}$:

$$y = x^{3/2}\{1+Ax^{-2}+Bx^{-3}\}^{1/2} = x^{3/2}\Big\{1+\sum_{j>0}\binom{\frac{1}{2}}{j}(Ax^{-2}+Bx^{-3})^j\Big\}. \tag{0.2}$$

There is a sequence of polynomials

$$L_j \in k[x, y, A, B] \tag{0.3}$$

uniquely defined by the properties

$$L_0 = 1, \quad L_1 = 0, \tag{0.4}$$

and

$$\sum_{j=0}^{r}\binom{r}{j} L_j x^{(r-j)/2} = O(1) \quad (r = 2, 3, \ldots) \tag{0.5}$$