**3.** For primes $p \equiv 1 \pmod 4$ we have (theorem 3 of the Annals paper)

$$(3) \qquad 4\frac{u}{t}h \equiv -\sum_{1\leqslant n<p} \frac{1}{gn}\left(\frac{n}{p}\right)\left[\frac{gn}{p}\right] \pmod p,$$

where $g$ is a primitive root $(\bmod p)$, $\left(\frac{n}{p}\right)$ is Legendre's symbol, and $[x]$ denotes the greatest integer in $x$.

To the right hand side of (3) we apply Voronoi's theorem (J. V. Uspensky and M. A. Heaslet, *Elementary number theory*, New York and London 1939, p. 261)

$$(4) \qquad (a^{2k}-1)P_k \equiv (-1)^{k-1}2k\cdot a^{2k-1}Q_k \sum_{S=1}^{N-1} S^{2k-1}\left[\frac{Sa}{N}\right] \pmod N.$$

Here $N$ is an arbitrary positive integer, $a$ is prime to $N$, while $P_k$ and $Q_k$ are the numerator and denominator of the $k$-th Bernoulli number $C_k$ (where $C_k$ is our $B_k$ except for sign when $k$ is even) in its lowest terms. We apply (4) to (3) with $N = p$, $a = g$, $k = \frac{1}{4}(p-1) = m$. When $p \equiv 1 \pmod 8$, it follows that

$$(5) \qquad \sum_{S=1}^{p-1} \frac{1}{gS}\left(\frac{S}{p}\right)\left[\frac{gS}{p}\right] \equiv 4C_m \pmod p,$$

on using $S^{2m} \equiv \left(\frac{S}{p}\right) \pmod p$, $g^{2m} \equiv -1 \pmod p$.

From (3) and (5)

$$(6) \qquad \frac{u}{t}h \equiv -C_m \pmod p.$$

Since $p \equiv 1 (8)$, we have $B_m = -C_m$, and (6) becomes (1).

**4.** Combining the result: "$h$ is prime to $p$" of our previous note (Acta Arith. 6 (1960), pp. 145-147) with the result of the present note, we see that *for primes $p \equiv 1 \pmod 4$ we have:*

$$u \equiv 0 \pmod p \quad \textit{if and only if} \quad B_m \equiv 0\ (p),$$

where $m = \frac{1}{4}(p-1)$; this is the extension of Mordell's result (Acta Arith. 6 (1960), pp. 137-144, theorem II) mentioned in paragraph 1 of this paper.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
UNIVERSITY OF NOTRE DAME, INDIANA
MARCH 8, 1961

*Reçu par la Rédaction le 5. 6. 1961*

ACTA ARITHMETICA
VII (1962)

# Note on Weyl's inequality

by

B. J. Birch and H. Davenport (Cambridge)

**1.** Weyl's inequality relates to exponential sums of the form

$$(1) \qquad S = \sum_{x=1}^{P} e(\alpha x^d + \alpha_{d-1}x^{d-1} + \dots),$$

where $\alpha, \alpha_{d-1}, \dots$ are real, and $e(\theta)$ denotes $e^{2\pi i\theta}$. Let $h/q$ be any rational approximation to $\alpha$ satisfying

$$(2) \qquad |\alpha - h/q| < q^{-2}, \qquad (h, q) = 1.$$

The form (see [4]) of Weyl's inequality with which we are concerned asserts that, if $K = 2^{d-1}$, then

$$(3) \qquad |S|^K \ll P^{\varepsilon}(P^{K-1} + P^K q^{-1} + P^{K-d}q)$$

for any $\varepsilon > 0$, where the implied constant depends only on $d$ and $\varepsilon$. In particular, if $P \ll q \ll P^{d-1}$ (this corresponds roughly to $\alpha$ being on the minor arcs in Waring's problem for $d$-th powers) we get

$$(4) \qquad |S| \ll P^{1-\frac{1}{K}+\varepsilon}.$$

In a recent paper [1] Chowla and Davenport have shown that this form of Weyl's inequality with $d = 3$ can be extended without loss of precision to double sums of the form

$$(5) \qquad S_2 = \sum_{x=1}^{P}\sum_{y=1}^{Q} e[\alpha f(x, y) + \Phi(x, y)] \qquad (0 < Q \leqslant P)$$

where $f(x, y)$ is a fixed binary cubic form with integral coefficients and non-zero discriminant, and $\Phi(x, y)$ is any real polynomial of degree 2 at most. In the present note we give an extension to a class of forms of degree $d$ in $n$ variables. We prove:

THEOREM. *Let $f(x_1, \dots, x_n)$ be any form of degree $d$ in $n$ variables with integral coefficients which is expressible as a sum of $n$ $d$-th powers of linear* *forms with real or complex coefficients and non-zero determinant. Let* $\Phi(x_1, \ldots, x_n)$ *be any real polynomial of degree less than d. Let*

$$S_n = \sum_{x_1=1}^{P_1} \ldots \sum_{x_n=1}^{P_n} e[af(x_1, \ldots, x_n) + \Phi(x_1, \ldots, x_n)], \tag{6}$$

*where* $0 < P_j \leqslant P$ $(j = 1, \ldots, n)$. *Then, subject to* (2),

$$|S_n|^K \ll P^\varepsilon [P^{K-1} + P^K q^{-1} + P^{K-d} q]^n. \tag{7}$$

This includes the result mentioned above, since a binary cubic form whose discriminant does not vanish is expressible over a quadratic extension as the sum of the cubes of two linear forms with non-vanishing determinant.

The homogeneous forms of degree $d$ and order $n$ may be considered as points of an affine space of dimension $(n+d-1)!/(n-1)!\,d!$; the forms satisfying the conditions of the theorem form a Zariski open set, $\Sigma$ say, of this space. In particular, if $d = 2$ (quadratic forms) or $d = 3$, $n = 2$ (binary cubics), $\Sigma$ is the whole space except for certain subvarieties. If $d = 4$, $n = 2$ (binary quartics) or if $d = 3$, $n = 3$ (ternary cubics) $\Sigma$ has codimension 1. Thus a binary quartic will generally satisfy the conditions of the theorem if its invariant $J$ is 0 ([2], p. 268), and a ternary cubic will generally satisfy the conditions if its invariant $S$ is 0 ([2], p. 377).

Our inequality may be applied in the usual way to prove new results of Waring type about the solution of Diophantine equations. However, in this sort of problem really sharp results are more often gained from better estimates for the number of solutions of equations (perhaps giving mean value theorems like those of Hua and Vinogradov) than from improvements of the Weyl inequality.

**2.** From now on, we suppose that $f(x_1, \ldots, x_n)$ is expressible as a sum of $n$ $d$-th powers of linear forms, say

$$f(x_1, \ldots, x_n) = L_1^d + \ldots + L_n^d, \tag{8}$$

where

$$L_r(x) = \sum_s \lambda_{rs} x_s. \tag{9}$$

We can suppose that all the coefficients $\lambda$ are in a finite algebraic extension $\Omega$ of the rationals.

For $d-1$ sets $\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(d-1)}$ of $n$ variables, write

$$M_s(\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(d-1)}) = \sum_{r=1}^{n} L_r(\boldsymbol{x}^{(1)}) \ldots L_r(\boldsymbol{x}^{(d-1)})\, \lambda_{rs}. \tag{10}$$



LEMMA 1.

$$|S|^K \ll P^{n(K-d)} \sum_{\boldsymbol{x}^{(1)}} \ldots \sum_{\boldsymbol{x}^{(d-1)}} \prod_{s=1}^{n} \min[P, \|d!\,\alpha M_s\|^{-1}], \tag{11}$$

*where the sum is over* $n(d-1)$ *integers satisfying*

$$|x_r^{(\nu)}| < P \quad (1 \leqslant r \leqslant n,\ 1 \leqslant \nu \leqslant d-1). \tag{12}$$

Proof. The result is obtained by repeatedly squaring and using Cauchy's inequality, on the lines of the usual proofs (see e.g. [3]) for a polynomial in one variable. After the $k$-th stage one obtains an exponential sum containing a polynomial whose terms of highest degree in $\boldsymbol{x}$ are of degree $d-k$ in $\boldsymbol{x}$ and of degree 1 in each of $\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(k)}$. At the next stage this polynomial, say $F(\boldsymbol{x})$, is replaced by $F(\boldsymbol{x}+\boldsymbol{x}^{(k+1)}) - F(\boldsymbol{x})$. Finally, when $k = d-1$, we get a polynomial

$$d! \sum_{r=1}^{n} L_r(\boldsymbol{x}^{(1)}) \ldots L_r(\boldsymbol{x}^{(d-1)}) L_r(\boldsymbol{x}) + \text{terms not involving } \boldsymbol{x}.$$

The coefficient of $x_s$ in this is $d!\,M_s$. Estimating the separate sums over $x_1, \ldots, x_n$, we get the result.

LEMMA 2. *There exist* $n$ *independent linear forms*

$$\sum_{s=1}^{n} \Lambda_{rs} m_s \tag{13}$$

*with the following properties: if* $m_1, \ldots, m_n$ *are such that none of the forms* (13) *vanish, then the equations*

$$M_s(\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(d-1)}) = m_s \quad (s = 1, \ldots, n) \tag{14}$$

*have* $\ll P^\varepsilon$ *solutions in integers* $x_r^{(\nu)}$ *of absolute value less than* $P$. *If* $m_1, \ldots, m_n$ *make just* $g$ *of the forms* (13) *vanish, the number of solutions of* (14) *is* $\ll P^{\varepsilon + g(d-2)}$.

Proof. By (10), the equations (14) are $n$ linear equations for the $n$ products $L_r(\boldsymbol{x}^{(1)}) \ldots L_r(\boldsymbol{x}^{(d-1)})$, and their determinant is $\det \lambda_{rs} \neq 0$. Hence they are equivalent to

$$L_r(\boldsymbol{x}^{(1)}) \ldots L_r(\boldsymbol{x}^{(d-1)}) = \sum_{s=1}^{n} \Lambda_{rs} m_s \quad (1 \leqslant r \leqslant n), \tag{15}$$

where $\det \Lambda_{rs} \neq 0$. The right hand sides of (15) are the forms (13) postulated in the lemma.

The $\Lambda_{rs}$ are in $\Omega$ and the $L_r(\boldsymbol{x}^{(\nu)})$ are numbers in $\Omega$ with bounded denominators. If the $r$-th form (13) is non-zero, then factorisation of the corresponding equation (15) gives $\ll P^{\varepsilon}$ possibilities, each of the form

$$L_r(\boldsymbol{x}^{(1)}) = \xi_r^{(1)}\varepsilon_r^{(1)}, \ldots, L_r(\boldsymbol{x}^{(d-1)}) = \xi_r^{(d-1)}\varepsilon_r^{(d-1)},$$

where the $\xi_r^{(\nu)}$ are particular numbers in $\Omega$ and the $\varepsilon_r^{(\nu)}$ are units in $\Omega$ with fixed product. For each $\nu$, $|L_r(\boldsymbol{x}^{(\nu)})|$ is bounded by a multiple of $P$, so there are $\ll (\log P)^h$ possibilities for $\varepsilon_r^{(\nu)}$, where $h$ is the number of fundamental units in $\Omega$. Thus each equation (15) with non-zero right hand side determines the factors on the left with $\ll P^{2\varepsilon}$ possibilities.

If none of the right hand sides vanish we get the first part of the lemma. Now suppose that exactly $g$ of them vanish, for definiteness say the first $g$. For each $\nu = 1, \ldots, d-1$, suppose that $g_\nu$ of the $L_r(\boldsymbol{x}^{(\nu)})$ vanish, then

$$g_1 + \ldots + g_{d-1} \geqslant g.$$

This leaves $\ll P^{g-g_\nu}$ possibilities for those of $L_1(\boldsymbol{x}^{(\nu)}), \ldots, L_g(\boldsymbol{x}^{(\nu)})$ that don't vanish, so for given values of the $L_r(\boldsymbol{x}^{(\nu)})$ for $r > g$ there are $\ll P^{g-g_\nu}$ possibilities for $\boldsymbol{x}^{(\nu)}$. Altogether the number of solutions is

$$\ll P^{\varepsilon+(g-g_1)+\ldots+(g-g_{d-1})} \ll P^{\varepsilon+(d-2)g}.$$

**3. Proof of the theorem.** For $s = 1, \ldots, n$, write $m_s$ for the value taken by $d!M_s$ in (11); then each $m_s \ll P^{d-1}$. For given $m_1, \ldots, m_n$ the number of values of the $x_s^{(\nu)}$ for which $d!M_s = m_s$ $(s = 1, \ldots, n)$ is estimated by Lemma 2; here we have to distinguish the cases $g = 0, 1, \ldots, n$. Thus

$$|S|^K \ll P^{n(K-d)} \sum_{g=0}^{n} \sum_{m_1,\ldots,m_n}^{(g)} P^{\varepsilon+(d-2)g} \prod_{s=1}^{n} \min[P, ||\alpha m_s||^{-1}],$$

where $\sum^{(g)}$ denotes that $n-g$ of $m_1, \ldots, m_n$ are independent variables each $\ll P^{d-1}$, and the others are functions of them, determined by the vanishing of $g$ of the linear forms (13). (If $g = n$, then $m_1 = \ldots = m_n = 0$.) Suppose for simplicity that $m_1, \ldots, m_{n-g}$ are the independent variables. Then

$$\sum_{m_1,\ldots,m_n}^{(g)} P^{\varepsilon+(d-2)g} \prod_{s=1}^{n} \min[P, ||\alpha m_s||^{-1}]$$
$$\ll P^{\varepsilon+(d-2)g} P^{g} \sum_{m_1,\ldots,m_{n-g}} \prod_{s=1}^{n-g} \min[P, ||\alpha m_s||^{-1}]$$
$$\ll P^{\varepsilon+g(d-1)} \cdot \Big( \sum_{|m| \ll P^{d-1}} \min[P, ||\alpha m||^{-1}]\Big)^{n-g}.$$

It is well known (see Chowla and Davenport [1], Lemma 3) that the inner sum is

$$\ll (P^{d-1}q^{-1}+1)(P+q\cdot\log q).$$



Since this expression is $\gg P^{d-1}$, we can estimate the previous sum as

$$\ll P^{\varepsilon}[(P^{d-1}q^{-1}+1)(P+q\cdot\log q)]^{n}.$$

This gives the result of the theorem, namely (7), on recalling that we can suppose $\log q \ll P^{\varepsilon}$, since otherwise the desired result is trivial.

## References

[1] S. Chowla and H. Davenport, *On Weyl's inequality and Waring's Problem for cubes*, Acta Arith. 6 (1960), pp. 505-521.

[2] E. B. Elliott, *Algebra of Quantics*, Oxford 1913.

[3] E. Landau, *Vorlesungen über Zahlentheorie* I, Leipzig 1927, Sätze 264-267.

[4] I. M. Vinogradov, *Izvestiya Akad. Nauk SSSR* 21 (1927), 567-578.

TRINITY COLLEGE
CAMBRIDGE

*Reçu par la Rédaction le 19. 6. 1961*