Aus (2) folgt mit (23) und (24)

$$g^2(2\varepsilon, 2\varepsilon) \geqslant c_{20}^{-1}\varepsilon^{-2}, \qquad \varepsilon \leqslant \varepsilon_{10}(\delta). \tag{25}$$

Mit (25) erhält man aus (22) und (21) die Ungleichung:

$$c_{21}^{-1}\frac{u_0^2}{\varepsilon} \leqslant c_{15}|\log\varepsilon|^2 \quad \text{für} \quad \varepsilon \leqslant \varepsilon_{10}(\delta).$$

Setzt man für u_0 gemäß (6) ein, so gelangt man zu der Ungleichung:

$$\beta \geqslant c_{22}^{-1} \quad \text{für} \quad \varepsilon \leqslant \varepsilon_{10}(\delta). \tag{26}$$

Wählt man $\delta = \frac{1}{2}c_{22}^{-1}$ und $\varepsilon_{11}(\delta)$ so klein, daß für $\varepsilon \leqslant \varepsilon_{11}(\delta)$ gilt:

$$\sqrt{\varepsilon}|\log\varepsilon|^2 \leqslant \tfrac{1}{3}c_{22}^{-1},$$

dann erhält man einen Widerspruch zu (26). Deshalb kann die Annahme (5) nicht gelten, und der angekündigte Satz ist bewiesen.

Zum Schluß sei noch bemerkt, daß die bestechende Einfachheit des Beweises von Erdös und Fuchs deswegen teilweise verlorengeht, weil die Reihen $G(s, s')$ und $T(s, s')$, welche man als Verallgemeinerung der geometrischen Reihe bzw. deren Ableitung im Körper K anzusehen hat, nicht so elementar zu handhaben sind wie in $\boldsymbol{Q}$.

Literaturverzeichnis

[1] R. Courant and D. Hilbert, *Methods of Mathematical Physics*, Vol. I, First English Edition 1953, Interscience Publishers, Inc., New York.

[2] P. Erdös and W. H. J. Fuchs, *On a problem of additive number theory*, J. London Math. Soc. 31 (1956), S. 67–73.

[3] W. Schaal, *Übertragung des Kreisproblems auf reell-quadratische Zahlkörper*, Math. Ann. 145 (1962), S. 273–284.

[4] — *On the expression of a number as the sum of two squares in totally real algebraic number fields*, Proc. Amer. Math. Soc. 16 (1965), S. 529–537.

Eingegangen am 8. 8. 1975 (750)

ACTA ARITHMETICA
XXXII (1977)

A new upper bound for Waring's problem (mod p)

by

J. D. Bovey (Cardiff)

1. Introduction. Let p be a prime and let d and t be positive integers with $p-1 = dt$. The number $\gamma(d, p)$ is defined to be the least positive integer s such that the congruence

$$x_1^d + \ldots + x_s^d \equiv N \pmod{p}$$

has a solution for all integers N. It can be verified readily from the work of Hardy and Littlewood [5] that

$$\gamma(d, p) \leqslant d$$

for all d and p. When $t = 1$ or 2 equality holds, but if we restrict d and p, better bounds can be found. Let ε be any fixed positive number. It is not hard to show, using exponential sum arguments (see [1] or [3]), that for all d, p with $d < p^{1/2-\varepsilon}$

$$\gamma(d, p) = O(1). \tag{1}$$

Dodson [3] has shown that when $d < p^{1/2}$

$$\gamma(d, p) = O(\log d).$$

Heilbronn [6] has conjectured that for $t > t_0(\varepsilon)$

$$\gamma(d, p) = O(d^{\varepsilon})$$

or at least that $\gamma(d, p) = O(d^{1/2})$ for $t > 2$. The best result so far is due to Dodson and Tietäväinen [4] who have proved that

$$\gamma(d, p) = O(d^{1/2+\varepsilon}) \tag{2}$$

for $t > 2$.

In this paper we obtain an upper bound for $\gamma(d, p)$ which is about as good as is possible in its dependence on d, but is spoilt by the factor $\varphi(t)$ (where φ is Euler's function). We then use this upper bound to obtain a new proof of the result of Dodson and Tietäväinen (2).

THEOREM 1. *Let q be any positive integer. Then there exist positive numbers $c(q)$ and $t_0(q)$ such that if p is a prime with $p-1 = dt$ we have*

$$\gamma(d, p) \leqslant c(q)\varphi(t)d^{1/q} \quad \text{when} \quad t > t_0$$

and

$$\gamma(d, p) \leqslant c(q)d^{1/\varphi(t)} \quad \text{when} \quad t \leqslant t_0.$$

It is evident that these estimates are more effective than an unpublished estimate of Heilbronn's ([6], Theorem 8) which asserts that for $t \geqslant 2$ there exists a constant a_t such that

$$\gamma(d, p) < a_t p^{1/\varphi(t)}.$$

The method used in this paper works better on the "Easier" Waring's problem. We denote by $\delta(d, p)$ the least s such that the congruence

$$\varepsilon_1 x_1^d + \ldots + \varepsilon_s x_s^d \equiv N (\operatorname{mod} p),$$

where each coefficient ε_i, $i = 1, \ldots, s$ can assume the values $+1$ or -1, has a solution for all integers N. Clearly $\delta(d, p) \leqslant \gamma(d, p)$ for all d and p. In § 2 we show that

$$\gamma(d, p) \ll \log d\, \delta(d, p)$$

and then in § 3 we prove the main results.

2. Let m be any positive integer and A a subset of Z_m, the additive group of residues modulo m. We write

$$A - A = \{a_1 - a_2 |\ a_1, a_2 \in A\}$$

and

$$(k)A = \{a_1 + \ldots + a_k |\ a_i \in A, i = 1, \ldots, k\}.$$

The following lemma is due to Jackson and Rehman [7] but we include a simple proof here.

LEMMA 1. *Let m be any positive integer and let A be a subset of Z_m such that $A - A = Z_m$. Then*

$$([\log m/\log 2] + 1)A = Z_m.$$

Proof. We prove by induction on n that if $A - A = Z_m$ then $(n)A$ has at least 2^n consecutive residue classes. Plainly if $A - A = Z_m$ then $(1)A$ has 2 consecutive residue classes. Suppose inductively that $(n)A$ contains 2^n consecutive residue classes $r+1, \ldots, r+2^n$ for some $r \in Z_m$. As 2^n is contained in $A - A$, $a + 2^n \in A$ for some $a \in A$. Hence $(n+1)A$ contains the 2^{n+1} consecutive residue classes

$$a+r+1, \ldots, a+r+2^n, a+2^n+r+1, \ldots, a+2^n+r+2^n$$

which establishes the desired induction. The lemma now follows on putting $n = [\log m/\log 2] + 1$.

LEMMA 2. *For all p and d*

$$\gamma(d, p) \ll \log d\, \delta(d, p).$$

Proof. Let A be the set of residue classes (mod p) that can be written as the sum of $\delta(d, p)$ dth powers. Clearly $A - A = Z_p$ and Lemma 1 gives

$$\gamma(d, p) \leqslant ([\log p/\log 2] + 1)\,\delta(d, p).$$

By (1) we can assume that $d > p^{1/3}$ say, and the result follows.

3. The main result. Let R be a primitive tth root of $1 (\operatorname{mod} p)$ and let $r = \varphi(t)$ where φ is Euler's function. The r-tuples of integers $(a_1, \ldots, a_r)$ which satisfy

$$a_1 + a_2 R + \ldots + a_r R^{r-1} \equiv 0 \ (\operatorname{mod} p)$$

form an additive subgroup of Z^r with index p. They form hence a lattice (in the "Geometry of Numbers" sense) which we call Λ. If $\boldsymbol{x} = (x_1, \ldots, x_r)$ is a vector in R^r then we use the standard notation

$$\|\boldsymbol{x}\|_1 = \sum_{i=1}^{r} |x_i|.$$

We need the following elementary lemma.

LEMMA 3. *Let Λ be defined as above and let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_r$ be r linearly independent vectors contained in Λ. Then*

$$\delta(d, p) \leqslant \tfrac{1}{2} \sum_{i=1}^{r} \|\boldsymbol{b}_i\|_1.$$

Proof. Let N be any integer. Clearly we can solve

$$(N, 0, \ldots, 0) \equiv c_1 \boldsymbol{b}_1 + \ldots + c_r \boldsymbol{b}_r \ (\operatorname{mod} \Lambda)$$

where the c_i are real numbers with $|c_i| \leqslant \frac{1}{2}$ for $i = 1, \ldots, r$. If we write

$$(a_1, \ldots, a_r) = \boldsymbol{a} = c_1 \boldsymbol{b}_1 + \ldots + c_r \boldsymbol{b}_r$$

then the a_i are integers

$$a_1 + a_2 R + \ldots + a_r R^{r-1} \equiv N \ (\operatorname{mod} p)$$

and

$$|a_1| + \ldots + |a_r| \leqslant \tfrac{1}{2}(\|\boldsymbol{b}_1\|_1 + \ldots + \|\boldsymbol{b}_r\|_1)$$

by the triangle inequality. As the R^i are all dth powers (mod p) the result is proved.

Let ϱ be a primitive tth root of 1 and let $Z[\varrho]$ be the ring of cyclotomic integers of order t. Let $f\colon Z^r \to Z[\varrho]$ be given by

$$f(a_1, \ldots, a_r) = a_1 + a_2\varrho + \ldots + a_r\varrho^{r-1}.$$

LEMMA 4. *$f(\Lambda)$ is an ideal of $Z[\varrho]$.*

Proof. As $p \equiv 1 \pmod t$ the prime p splits completely in $Z[\varrho]$. The kernel of the homomorphism $g\colon Z[\varrho] \to Z_p$ which sends $a_1 + a_2\varrho + \ldots \ldots + a_r\varrho^{r-1}$ to the residue class $a_1 + a_2R + \ldots + a_rR^{r-1} \pmod p$ is $f(\Lambda)$ which proves the lemma.

Let $\Phi_t(x)$ be the cyclotomic polynomial of order t and let $A(t)$ be the least upper bound of the absolute values of the coefficients of $\Phi_t(x)$. We can prove the following upper bound for $\delta(d, p)$.

LEMMA 5. *If n is a positive integer with $n \leqslant \varphi(t)$ then*

$$\delta(d, p) \leqslant n\big(A(t)+1\big)^n \varphi(t) p^{1/n}.$$

Proof. Consider the $([p^{1/n}]+1)^n$ numbers

$$a_1 + a_2R + \ldots + a_nR^{n-1}, \quad 0 \leqslant a_i \leqslant [p^{1/n}]; \quad i = 1, \ldots, n.$$

As there are more than p of them at least two must be congruent $\pmod p$ and we can solve

$$c_1 + c_2R + \ldots + c_nR^{n-1} \equiv 0 \pmod p \quad \text{with} \quad |c_i| < p^{1/n}, \quad i = 1, \ldots, n.$$

If we write $\boldsymbol{c} = (c_1, \ldots, c_n, 0, \ldots, 0)$ then $\boldsymbol{c} \in \Lambda$ and $\|\boldsymbol{c}\|_1 < np^{1/n}$. We now define

$$\boldsymbol{b}_i = f^{-1}\big(\varrho^{i-1} f(\boldsymbol{c})\big), \quad i = 1, \ldots, r.$$

Clearly the $\boldsymbol{b}_i$ are linearly independent and by Lemma 4 they are contained in Λ. For $1 \leqslant i \leqslant r-n$, $\boldsymbol{b}_i$ is just $\boldsymbol{c}$ shifted $i-1$ places to the right, i.e.

$$\boldsymbol{c} = \boldsymbol{b}_1 = (c_1, \ldots, c_n, 0, \ldots, 0),$$
$$\boldsymbol{b}_2 = (0, c_1, \ldots, c_{n-1}, c_n, 0, \ldots, 0),$$
$$\boldsymbol{b}_{r-n} = (0, \ldots, 0, c_1, \ldots, c_n)$$

and we have

$$\|\boldsymbol{b}_1\|_1 + \ldots + \|\boldsymbol{b}_{r-n}\|_1 = (r-n)\|\boldsymbol{c}\|_1 < (r-n)np^{1/n}. \tag{3}$$

We now write

$$\Phi_t(x) = a_0 + a_1x + \ldots + a_{r-1}x^{r-1} + x^r$$

and define $\boldsymbol{a} = (a_0, \ldots, a_{r-1})$. If $\boldsymbol{x} = (x_1, \ldots, x_r)$ is any element of Z^r we use the standard definition

$$\|\boldsymbol{x}\|_\infty = \sup_{1 \leqslant i \leqslant r} |x_i|.$$

It is easily verified that

$$f^{-1}\big(\varrho f(\boldsymbol{x})\big) = (0, x_1, \ldots, x_{r-1}) - x_r\boldsymbol{a}$$

and so

$$\big\|f^{-1}\big(\varrho f(\boldsymbol{x})\big)\big\|_\infty \leqslant \|\boldsymbol{x}\|_\infty + |x_r|\,\|\boldsymbol{a}\|_\infty \leqslant \big(A(t)+1\big)\|\boldsymbol{x}\|_\infty.$$

Applying this to $\boldsymbol{b}_{r-n+i}$ for $i = 1, \ldots, n$ we get

$$\|\boldsymbol{b}_{r-n+i}\|_\infty \leqslant \big(A(t)+1\big)^i \|\boldsymbol{b}_{r-n}\|_\infty \leqslant \big(A(t)+1\big)^i p^{1/n}, \quad i = 1, \ldots, n$$

and so

$$\sum_{i=1}^{n} \|\boldsymbol{b}_{r-n+i}\|_1 \leqslant rp^{1/n} \sum_{i=1}^{n} \big(A(t)+1\big)^i \leqslant rnp^{1/n}\big(A(t)+1\big)^n,$$

as $A(t) \geqslant 1$. Adding this estimate to (3) we get

$$\sum_{i=1}^{r} \|\boldsymbol{b}_i\|_1 \leqslant 2rn\big(A(t)+1\big)^n p^{1/n},$$

and combining this with Lemma 3 we get the required result.

Proof of Theorem 1. We choose t_0 to be large enough to ensure that, if $t > t_0$ then t has a factor, t' say, such that $t' > 3q$ and $A(t') = 1$. We can do this by choosing t' to be, say, the largest prime power divisor of t. If we write $d' = (p-1)/t'$ then, as every d'th power is also a dth power, we have

$$\delta(d, p) \leqslant \delta(d', p).$$

When $t > t_0$ putting $n = 3q$ in Lemma 4 gives

$$\delta(d, p) \leqslant \delta(d', p) \ll q2^{3q}\varphi(t')p^{1/3q}$$

which with Lemma 2 gives

$$\gamma(d, p) \ll q8^q\varphi(t)\log p\, p^{1/3q}.$$

Combining this with (1) gives the first inequality.

If we put $n = \varphi(t)$ in Lemma 5 we get

$$\delta(d, p) \leqslant 2\varphi(t)^2\big(A(t)+1\big)^{\varphi(t)} t^{1/\varphi(t)} d^{1/\varphi(t)}.$$

Since $-1 \equiv R + R^2 + \ldots + R^{t-1} \pmod p$, it follows that $\gamma(d, p) \leqslant (t-1) \times \delta(d, p)$. The second inequality of the theorem will therefore hold if we choose $c(q)$ to satisfy

$$c(q) \geqslant \sup_{t \leqslant t_0}\Big((t-1)\varphi(t)^2\big(A(t)+1\big)^{\varphi(t)} t^{1/\varphi(t)}\Big).$$

Finally we prove the estimate (2). First we assume that $t < d^{1/2}$. Let $q > \varepsilon^{-1}$ be a fixed positive integer. The condition $t > 2$ implies $\varphi(t) \geqslant 2$ and so if $t \leqslant t_0(q)$ the theorem gives

$$\gamma(d, p) \ll d^{1/\varphi(t)} \ll d^{1/2}.$$

If $t > t_0$ then $\gamma(d, p) \ll \varphi(t) d^{1/q} \ll d^{1/2+\varepsilon}$ as required.

Tietäväinen [8] has shown that if $2d$ different residue classes can be represented as the sum of w dth powers, then

$$\gamma(d, p) \ll w \log d.$$

It follows easily from the Cauchy–Davenport Theorem ([2] or [8]) that we can represent $2d$ residue classes as the sum of $2d/t$ dth powers and thus

$$\gamma(d, p) \ll dt^{-1} \log d.$$

This proves the result at once for $t \geqslant d^{1/2}$.

I am grateful to Dr. Maurice Dodson for suggesting a number of improvements in the presentation of this paper.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, 1966.

[2] H. Davenport, *On the addition of residue classes*, J. London Math. Soc. 10 (1935), pp. 30–32.

[3] M. M. Dodson, *Homogeneous additive congruences*, Philos. Trans. Roy. Soc. London, Ser. A, 261 (1967), pp. 163–210.

[4] M. M. Dodson and A. Tietäväinen, *A note on Waring's problem in* GF[p], Acta Arith. 30(1976), pp. 159–167.

[5] G. H. Hardy and J. E. Littlewood, *Some Problems of 'Partitio Numerorum' VIII. The number $\Gamma(k)$ in Waring's Problem*, Proc. London Math. Soc. 28 (1927), pp. 518–542.

[6] H. Heilbronn, *Lecture notes on additive number theory* mod p, California Institute of Technology, 1964.

[7] T. H. Jackson and F. Rehman, *Note on difference-covers that are not k-sum covers*, Mathematika 21 (1974), pp. 107–109.

[8] A. Tietäväinen, *Note on Waring's problem* (mod p), Ann. Acad. Sci. Fenn. AI 554 (1973).

Received on 23. 8. 1975
and in revised form on 15. 10. 1975 (755)

ACTA ARITHMETICA
XXXII (1977)

Elementary methods in the theory of L-functions, V
The theorems of Landau and Page

by

J. Pintz (Budapest)

1. Landau [4] proved in 1918 that if the L-functions belonging to real primitive characters $\chi_1 \pmod{D_1}$ and $\chi_2 \pmod{D_2}$ $(\chi_1 \neq \chi_2)$ respectively, have $1-\delta_1$ and $1-\delta_2$ real zeros, respectively, then

$$\max(\delta_1, \delta_2) > \frac{c}{\log D_1 D_2}, \tag{1.1}$$

where c is an absolute constant. This fact was used by Landau only to prove that the negative fundamental discriminants for which the class number $h(-D)$ of the imaginary quadratic field belonging to the discriminant $-D$

$$h(-D) = o\left(\frac{\sqrt{D}}{\log D}\right) \tag{1.2}$$

are very rare. Namely combining Hecke's theorem (see also Landau [4]) with (1.1) one has immediately the inequality

$$\max\left(\frac{h(-D_1)}{\sqrt{D_1}}, \frac{h(-D_2)}{\sqrt{D_2}}\right) > \frac{c'}{\log D_1 D_2}. \tag{1.3}$$

Page [6] proved (1.1) for the case $\chi_1 = \chi_2$, i.e. he showed that an L-function belonging to a real non-principal character $\chi \pmod D$ has at most one, simple zero in the interval

$$\left[1 - \frac{c''}{\log D}, 1\right] \tag{1.4}$$

where c'' is an absolute constant.

The mentioned results of Page and Landau concerning the real zeros of real L-functions together with the results — concerning the zeros of complex L-functions and the complex zeros of real L-functions — of Gronwall [3] and Titchmarsh [9] were used by Page [6] to get better results for the distribution of primes in arithmetic progressions.