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

\( g^2(2c, 2e) \geq c_2^{-1} c^{-2} \), \( e \leq e_1(\delta) \).

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

\[ c_1^{-1} \frac{c^2}{e} \leq c_{14} \log e^{-2} \quad \text{für} \quad e \leq e_{14}(\delta). \]

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

\[ \beta \geq c_1 \quad \text{für} \quad e \leq e_{14}(\delta). \]

Wählt man \( \delta = \frac{1}{4} c_2^2 \) und \( e_{11}(\delta) \) so klein, daß für \( e \leq e_{11}(\delta) \) gilt:

\[ \sqrt{e} \log e^{-1} \leq \frac{1}{4} c_2^2, \]

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 bestehende 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 \( Q \).

**Literaturverzeichnis**


_Eingegangen am 5. 8. 1973_ (760)
THEOREM 1. Let \( q \) be any positive integer. Then there exist positive numbers \( c(q) \) and \( t(q) \) such that if \( p \) is a prime with \( p-1 = dt \) we have
\[
\gamma(d, p) \leq c(q)p(t)\sigma(t) \quad \text{when} \quad t > t_0
\]
and
\[
\gamma(d, p) \leq c(q)d^{t_0} \quad \text{when} \quad t \leq t_0.
\]

It is evident that these estimates are more effective than an unpublished estimate of Heilbronn’s ([16], Theorem 8) which asserts that for \( t \geq 2 \) there exists a constant \( \alpha \) such that
\[
\gamma(d, p) < \alpha d^{t_0}.
\]

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
\[
e_1a_1^2 + \cdots + e_sa_s^2 = \bar{N} \quad \text{(mod} \quad p),
\]
where each coefficient \( e_i \), \( i = 1, \ldots, s \) can assume the values \( +1 \) or \( -1 \), has a solution for all integers \( N \). Clearly \( \delta(d, p) \leq \gamma(d, p) \) for all \( d \) and \( p \). In §2 we show that
\[
\gamma(d, p) \leq \log d \delta(d, p)
\]
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
\[
A - A = \{a_1 - a_2 \mid a_1, a_2 \in A\}
\]
and
\[
(k)A = \{a_1 + \cdots + a_k \mid a_i \in A, \ i = 1, \ldots, k\}.
\]
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 \( n = \lfloor \log m/\log 2 \rfloor + 1 \).

**Lemma 2.** For all \( p \) and \( d \)
\[
\gamma(d, p) \leq \log d \delta(d, p).
\]

Proof. Let \( A \) be the set of residue classes (mod \( p \)) that can be written as the sum of \( \delta(d, p) \) \( d \)-th powers. Clearly \( A - A = Z_p \) and Lemma 1 gives
\[
\gamma(d, p) \leq (\lfloor \log p/\log 2 \rfloor + 1) \delta(d, p).
\]
By (1) we can assume that \( d > p^{10} \) say, and the result follows.

3. The main result. Let \( R = \{a_1, \ldots, a_r\} \) be a primitive \( r \)-th root of \( 1 \) (mod \( p \)) and let \( r = \phi(t) \) where \( \phi \) is Euler’s function. The \( r \)-tuples of integers \( (a_1, \ldots, a_r) \) which satisfy
\[
a_1 + a_2R + \cdots + a_rR^{r-1} = 0 \quad \text{(mod} \quad p)\]
form an additive subgroup of \( Z^r \) with index \( p \). They form hence a lattice (in the “Geometry of Numbers” sense) which we call \( \Lambda \). If \( \mathbf{x} = (x_1, \ldots, x_r) \) is a vector in \( R^r \) then we use the standard notation
\[
\|\mathbf{x}\|_1 = \sqrt{\sum_{i=1}^{r} |x_i|^2}.
\]
We need the following elementary lemma.

**Lemma 3.** Let \( A \) be defined as above and let \( b_1, \ldots, b_r \) be \( r \) linearly independent vectors contained in \( A \). Then
\[
\delta(d, p) \leq \frac{1}{r} \sum_{i=1}^{r} \|b_i\|_1.
\]

Proof. Let \( N \) be any integer. Clearly we can solve
\[
(N, 0, \ldots, 0) = a_1b_1 + \cdots + a_r b_r \quad \text{(mod} \quad A)\]
where the \( c_i \) are real numbers with \( |c_i| \leq \frac{1}{2} \) for \( i = 1, \ldots, r \). If we write
\[
(a_1, \ldots, a_r) = a = c_1b_1 + \cdots + c_r b_r
\]
then the \( c_i \) are integers
\[
a_1 + a_2R + \cdots + a_rR^{r-1} = N \quad \text{(mod} \quad p)\]
and
\[
|a_1| + \cdots + |a_r| \leq \frac{1}{r} \left( \|b_1\|_1 + \cdots + \|b_r\|_1 \right)
\]
by the triangle inequality. As the \( R^r \) are all \( d \)-th powers (mod \( p \)) the result is proved.
Let \( q \) be a primitive 4th root of 1 and let \( Z[q] \) be the ring of cyclotomic integers of order \( t \). Let \( f: Z' \to Z[q] \) be given by
\[
f(a_1, \ldots, a_r) = a_1 + a_2 q + \cdots + a_r q^{r-1}.
\]

**Lemma 4.** \( f(A) \) is an ideal of \( Z[q] \).

**Proof.** As \( p = 1 \pmod{t} \) the prime \( p \) splits completely in \( Z[q] \). The kernel of the homomorphism \( f: Z[q] \to \mathbb{Z}_p \) which sends \( a_1 + a_2 q + \cdots + a_r q^{r-1} \) to the residue class \( a_1 + a_2 E + \cdots + a_r E^{r-1} \pmod{p} \) is \( f(A) \) which proves the lemma.

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

**Lemma 5.** If \( n \) is a positive integer with \( n < \varphi(t) \) then
\[
\delta(d, p) \leq n(A(t) + 1)^n \varphi(t)p^{1/n}.
\]

**Proof.** Consider the \((\lceil p^{1/n} \rceil + 1)^n\) numbers
\[
a_1 + a_2 E + \cdots + a_n E^{n-1}, \quad 0 \leq a_i \leq \lfloor p^{1/n} \rfloor, \quad i = 1, \ldots, n.
\]
As there are more than \( p \) of them at least two must be congruent \( \pmod{p} \) and we can solve
\[
a_1 + a_2 E + \cdots + a_n E^{n-1} = 0 \pmod{p} \quad \text{with} \quad |a_i| < p^{1/n}, \quad i = 1, \ldots, n.
\]
If we write \( c = (c_1, \ldots, c_n, 0, \ldots, 0) \) then \( c \in A \) and \( \|c\| < np^{1/n} \). We now define
\[
b_i = f^{-1}(q^{i-1}f(c)), \quad i = 1, \ldots, r.
\]
Clearly the \( b_i \) are linearly independent and by Lemma 4 they are contained in \( A \). For \( 1 \leq i \leq r-n \), \( b_i \) is just \( c \) shifted \( i-1 \) places to the right, i.e.
\[
b_i = (c_1, \ldots, c_n, 0, \ldots, 0),
b_{i+n} = (0, c_1, \ldots, c_{n-1}, c_n, \ldots, 0),
b_{r-n} = (0, \ldots, 0, c_1, \ldots, c_n)
\]
and we have
\[
\|b_1\| + \cdots + \|b_{r-n}\| = (r-n)\|c\| < (r-n)np^{1/n}.
\]
We now write
\[
\mathcal{B}(x) = a_0 + a_1 x + \cdots + a_r x^{r-1} + x^r
\]
and define \( a = (a_0, \ldots, a_r) \). If \( x = (x_1, \ldots, x_r) \) is any element of \( Z' \) we use the standard definition
\[
\|x\| = \sup_{1 \leq i \leq r} |x_i|.
\]
It is easily verified that
\[
f^{-1}(qf(x)) = (0, x_2, \ldots, x_{r-1}) - x_r a
\]
and so
\[
\|f^{-1}(qf(x))\| \leq \|x\| + |a| \leq (A(t) + 1)\|x\|.
\]
Applying this to \( b_{r-n+i} \) for \( i = 1, \ldots, n \) we get
\[
\|b_{r-n+i}\| \leq (A(t) + 1)^i\|b_{r-n}\| \leq (A(t) + 1)^i p^{1/n}, \quad i = 1, \ldots, n
\]
and so
\[
\sum_{i=1}^{n} \|b_{r-n+i}\| \leq np^{1/n} \sum_{i=1}^{n} (A(t) + 1)^i \leq rnp^{1/n} (A(t) + 1)^n,
\]
as \( A(t) \geq 1 \). Adding this estimate to (3) we get
\[
\sum_{i=1}^{r} \|b_i\| \leq 2rn (A(t) + 1)^n p^{1/n},
\]
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 divisor of \( t \). If we write \( d' = (p-1)/t' \) then, as every \( d' \)th power is also a \( d \)th power, we have
\[
\delta(d, p) \leq \delta(d', p).
\]
When \( t > t_0 \) putting \( n = 3q \) in Lemma 4 gives
\[
\delta(d, p) \leq \delta(d', p) < q^{22q} \varphi(t') p^{1/32q}
\]
which with Lemma 2 gives
\[
\gamma(d, p) \leq q^{8q} \varphi(t) \log p q^{1/32q}.
\]
Combining this with (1) gives the first inequality.

If we put \( n = \varphi(t) \) in Lemma 5 we get
\[
\delta(d, p) \leq 2q^2 \varphi(t) (A(t) + 1)^{\varphi(t)} \varphi(t)^{1/\varphi(t)}.
\]
Since \( -1 = R + R^2 + \cdots + R^{t-1} \pmod{p} \), it follows that \( \gamma(d, p) < (t-1) \times \delta(d, p) \). The second inequality of the theorem will therefore hold if we choose \( \epsilon(q) \) to satisfy
\[
o(q) \geq \max_{t \in \mathbb{Q}} \left| (t-1) \varphi(t)^2 (A(t) + 1)^{\varphi(t)} \varphi(t)^{1/\varphi(t)} \right|.
\]
Finally we prove the estimate (2). First we assume that \( t < d^{1/4} \).
Let \( q > \varepsilon^{-1} \) be a fixed positive integer. The condition \( t > 2 \) implies \( \varphi(t) \geq 2 \) and so if \( t \leq t_4(q) \) the theorem gives

\[
\gamma(d, p) \leq d^{1/2} \leq d^{0.2}.
\]

If \( t > t_4 \) then \( \gamma(d, p) \leq \varphi(t) d^{1/2} \leq d^{1/2} + + \) as required.

Tietävänäinen [8] has shown that if \( 2 \) distinct residue classes can be represented as the sum of \( w \) \( d \) th powers, then

\[
\gamma(d, p) \leq w \log d.
\]

It follows easily from the Cauchy–Davenport Theorem ([2] or [8]) that we can represent \( \leq 2 \) residue classes as the sum of \( 2d/3 \) \( d \) th powers, and thus

\[
\gamma(d, p) \leq d^{1-1/3} \log d.
\]

This proves the result at once for \( t \geq d^{1/2} \).

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

References


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