GENERALIZATION OF A THEOREM OF DAVENPORT ON THE ADDITION OF RESIDUE CLASSES.

BY S. S. PILLAI.
(From the Annamalai University, Annamalainagar, S. India.)

Received August 23, 1937.
(Communicated by Dr. S. Chowla.)

The object of this note is to prove the following Theorem.

Let \( M \) be a positive integer; let \( a_1, a_2, \ldots, a_m \) be \( m \) different residue classes \((\text{mod. } M)\); let \( \beta_1, \ldots, \beta_n \) be \( n \) different residue classes \((\text{mod. } M)\); let \( \gamma_1, \gamma_2, \ldots, \gamma_l \) be all those different residue classes which are representable as

\[
a_i + \beta_j \quad (1 \leq i \leq m, 1 \leq j \leq n).
\]

Further let \( d = \max (|\beta_r - \beta_s|) \), \( 1 \leq r \leq n, 1 \leq s \leq n, r \neq s \).

Then

\[
l \geq m + n - 1;
\]

provided that \( m + n - 1 \leq \frac{M}{d} \) and otherwise, \( l = \frac{M}{d} \).

When \( M \) is a prime, \( d = 1 \). So Davenport’s theorem is a particular case of this. In an issue of this Proceedings, I. Chowla generalized Davenport’s theorem in a different direction and applied it to \( f(k) \) in Waring’s problem. Following I. Chowla, I apply the theorem of the present paper to Waring’s problem with polynomial summands.

The proof follows very closely Davenport’s. So it is proved by induction on \( n \).

For \( n = 1 \), there is nothing to prove.

Let \( n = 2 \). Consider

\[
(A) \quad \{a_1 + \beta_1, a_2 + \beta_1, \ldots, a_m + \beta_1, a_1 + \beta_2, a_2 + \beta_2, \ldots, a_m + \beta_2, a_1 + \beta_3, a_2 + \beta_3, \ldots, a_m + \beta_3, \ldots\},
\]

\[
1 \quad a_r + \beta \neq a_t + \beta \quad (\text{mod. } M),
\]

otherwise \( a_r = a_t \) \((\ldots)\).

\[
2 \quad a_r + \beta_1 = a_t + \beta_2 \quad \text{and} \quad a_r + \beta_1 = a_t + \beta_2
\]

are impossible; for otherwise, by subtraction

\[
a_r = a_t
\]

which is against our assumption.

* \((a, b)\) stands for the greatest common factor of \( a \) and \( b \).

(3) Hence, if there are only \( m \) residue classes in (A), \( a_r + \beta_1 = a_t + \beta_2 \), where for every \( r \) there is one unique \( t \). Therefore

\[
\sum_{r=1}^{m} (a_r + \beta_1) \equiv \sum_{s=1}^{m} (a_s + \beta_2) \pmod{M}.
\]

So

\[
m \beta_1 \equiv m \beta_2 \pmod{M}.
\]

Consequently,

\[
m \equiv 0 \pmod{\frac{M}{(M, \beta_2 - \beta_1)}}.
\]

Therefore when \( n = 2 \), \( l \geq m + n - 1 \), provided \( m < \frac{M}{(M, \beta_2 - \beta_1)} \).

\[\text{i.e.,} \quad l \leq \frac{M}{(M, \beta_2 - \beta_1)}\]

So we can suppose that \( n > 2 \) and that the theorem is true for all \( n' < n \). We apply the theorem to the two sets of residue classes \( \gamma_1, \gamma_2, \ldots, \gamma_l; \beta_1, \ldots, \beta_n \).

If \( l \geq \frac{M}{(M, \beta_1 - \beta_n)} \), there is nothing to prove.

So we may suppose that \( l < \frac{M}{(M, \beta_1 - \beta_n)} \).

Hence there are \( l + 1 \) residue classes in the set

\[\gamma_i + \beta_1; \gamma_i + \beta_n, i = 1, \ldots, l.\]

Therefore there is a class \( \delta \) such that \( \delta - \beta_1 \) is a \( \gamma \) and \( \delta - \beta_n \) is not. Since we can arrange \( \beta_2, \ldots, \beta_{n-1} \) and also \( \gamma_1, \ldots, \gamma_l \) in any order we please, we may suppose, without loss of generality, that there exists a suffix \( r, 1 \leq r < n \), such that

\[\delta - \beta_s = \gamma_s, \text{ for } 1 \leq s \leq r,\]

and

\[\delta - \beta_t = \epsilon_t, \text{ for } r < t \leq n,\]

\[\epsilon_t \neq \gamma_u, \text{ for } r < t \leq n, \quad 1 \leq u \leq l.\]

We now observe that none of the residue classes \( \gamma_s - \beta_t \) (where \( r < t \leq n \), \( 1 \leq s \leq r \)) is an \( \alpha \). For if so, we should have

\[a + \beta_s = \gamma_s = \delta - \beta_s,\]

\[\text{i.e.,} \quad a + \beta_s = \delta - \beta_t = \epsilon_t.\]

But

\[a + \beta_s \text{ is a } \gamma.\]

Hence \( \epsilon_t \) would be a \( \gamma \), which is not the case. Therefore the \( l' \) residue classes representable in the form \( a_i + \beta_t \) (\( 1 \leq i \leq m, \ r < t \leq n \)) form a subset of \( \gamma' \)'s not containing \( \gamma_1, \gamma_2, \ldots, \gamma_r \). Thus \( l' \leq l - r \). But by our theorem with \( n' = n - r \),

\[l' \geq m + (n - r) - 1,\]

provided \( l' \leq \frac{M}{d'} \).

where \( d' = \max. (M, \beta_i - \beta_j), i, j = r + 1, r + 2, \ldots, n; i \neq j'. \)

In virtue of our hypothesis the last condition is satisfied.

Hence \( l \geq m + n - 1 \).