Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 37 (1962-1963)

Artikel: Theorems in the Additive Theory of Numbers.
Autor: Bose, R.C. / Chowla, S.
DOI: https://doi.org/10.5169/seals-28613

Theorems in the Additive Theory of Numbers[1])

R. C. Bose and S. Chowla

Summary. This paper extends some earlier results on difference sets and B_2 sequences by Singer, Bose, Erdös and Turan, and Chowla.

1. Singer (6) proved that if $m = p^n$ (where p is a prime), then we can find $m + 1$ integers

$$d_0, d_1, \ldots, d_m$$

such that the $m^2 + m$ differences $d_i - d_j (i \neq j,\ i, j = 0, 1, \ldots, m)$ when reduced $\bmod (m^2 + m + 1)$, are all the different non-zero integers less than $m^2 + m + 1$.

Bose (1) proved that if $m = p^n$ (where p is a prime), then we can find m integers

$$d_1, d_2, \ldots, d_m$$

such that the $m(m - 1)$ differences $d_i - d_j (i \neq j,\ i, j = 1, 2, \ldots, m)$ when reduced $\bmod (m^2 - 1)$, are all the different non-zero integers less than $m^2 - 1$, which are not divisible by $m + 1$.

From the theorems of Singer and Bose the following corollaries are obvious.

Corollary 1. If $m = p^n$ (where p is a prime), then we can find $m + 1$ integers

$$d_0, d_1, \ldots, d_m$$

such that the sums $d_i + d_j$ are all different $\bmod (m^2 + m + 1)$, where $0 \leq i \leq j \leq m$.

Corollary 2. If $m = p^n$ (where p is prime), then we can find m integers

$$d_1, d_2, \ldots, d_m$$

such that the sums $d_i + d_j$ are all different $\bmod (m^2 - 1)$, where

$$0 \leq i \leq j \leq m.$$

We shall prove here the following two theorems generalizing corollaries 1 and 2.

[1]) This research was supported in part by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under Contract No. AF 49 (638)–213. Reproduction in whole or part is permitted for any purpose of the United States Government.

Theorem 1. If $m = p^n$ (where p is prime) we can find m non-zero integers (less than m^r)

$$d_1 = 1,\ d_2, \ldots, d_m \tag{1.0}$$

such that the sums

$$d_{i_1} + d_{i_2} + \ldots + d_{i_r} \tag{1.1}$$

$1 \leq i_1 \leq i_2 \ldots \leq i_r \leq m$ are all different $\bmod (m^r - 1)$.

Proof. Let $\alpha_1 = 0,\ \alpha_2, \ldots,\ \alpha_m$ be all the different elements of the GALOIS field $GF(p^n)$. Let x be a primitive element of the extended field $GF(p^{nr})$. Then x cannot satisfy any equation of degree less than r with coefficients from $GF(p^n)$. Let

$$x^{d_i} = x + \alpha_i,\ i = 1, 2, \ldots,\ m;\ d_i < p^{nr} \tag{1.2}$$

then the required set of integers is

$$d_1 = 1,\ d_2, \ldots,\ d_m .$$

If possible let

$$d_{i_1} + d_{i_2} + \ldots d_{i_r} \equiv d_{j_1} + d_{j_2} + \ldots + d_{j_r} \mod (m^r - 1)$$

where $1 \leq i_1 \leq i_2 \ldots \leq i_r \leq m,\ 1 \leq j_1 \leq j_2 \leq \ldots \leq j_r \leq m,$ and

$$(i_1, i_2, \ldots, i_r) \neq (j_1, j_2, \ldots, j_r) .$$

Then

$$x^{d_{i_1}} x^{d_{i_2}} \ldots x^{d_{i_r}} = x^{d_{j_1}} x^{d_{j_2}} \ldots x^{d_{j_r}} . \tag{1.3}$$

Hence from (1.2)

$$(x + \alpha_{i_1})(x + \alpha_{i_2}) \ldots (x + \alpha_{i_r}) = (x + \alpha_{j_1})(x + \alpha_{j_2}) \ldots (x + \alpha_{j_r}).$$

After cancelling the highest power of x from both sides we are left with an equation of the $(r - 1)$-th degree in x, with coefficients from $GF(p^n)$, which is impossible. Hence the theorem.

Example 1. Let $p^n = 5,\ r = 3$. The roots of the equation $x^3 = 2x + 3$ are primitive elements of $GF(5^3)$. [See CARMICHAEL (2), p. 262]. If x is any root then we can express the powers of x in the form $ax + b$ where a and b belong to the field $GF(5)$. We get

$$x^1 = x + 0,\ x^{103} = x + 1,\ x^{119} = x + 2,\ x^{14} = x + 3,\ x^{34} = x + 4 .$$

Hence the set of integers

$$d_1 = 1,\ d_2 = 14,\ d_3 = 34,\ d_4 = 103,\ d_5 = 119$$

is such that the sum of any three (repetitions allowed) is not equal to the sum of any other three mod (124). This can be directly verified by calculating the 35 sums $d_{i_1} + d_{i_2} + d_{i_3},\ 1 \leq i_1 \leq i_2 \leq i_3 \leq 5$.

Theorem 2. If $m = p^n$ (where p is a prime) and

$$q = (m^{r+1} - 1)/(m - 1) \tag{1.4}$$

we can find $m + 1$ integers (less than q)

$$d_0 = 0,\ d_1 = 1,\ d_2, \ldots, d_m \tag{1.5}$$

such that the sums

$$d_{i_1} + d_{i_2} + \ldots + d_{i_r} \tag{1.6}$$

$0 \leq i_1 \leq i_2 \leq \ldots \leq i_r \leq m$, are all different mod (q).

Proof. Let $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3, \ldots \alpha_m$ be all the elements of $GF(p^n)$, and let x be a primitive element of the extended field $GF(p^{nr+n})$. Then x^q and its various powers belong to $GF(p^n)$, and x cannot satisfy any equation of degree less than $r + 1$, with coefficients from $GF(p^n)$. Let

$$(\lambda_0, \mu_0),\ (\lambda_1, \mu_1), \ldots,\ (\lambda_m, \mu_m)$$

be pairs of elements from $GF(p^n)$, such that the ratios $\lambda_0/\mu_0, \lambda_1/\mu_1, \ldots, \lambda_m/\mu_m$ are all different, where infinity is regarded as one of the ratios. Thus we may take for example

$$(\lambda_0, \mu_0) = (1, 0), (\lambda_i, \mu_i) = (\alpha_i, 1), \quad i = 1, 2, \ldots, m.$$

We can find $d_i < q$ $(i = 0, 1, 2, \ldots, m)$, such that

$$\varrho_i\, x^{d_i} = \lambda_i + \mu_i x \tag{1.7}$$

ϱ_i being a suitably chosen non-zero element of $GF(p^n)$. Then the required set of integers is

$$d_0 = 0,\ d_1 = 1,\ d_2, \ldots, d_m\,.$$

If possible let

$$d_{i_1} + d_{i_2} + \ldots + d_{i_r} \equiv d_{j_1} + d_{j_2} + \ldots + d_{j_r} \pmod q \tag{1.8}$$

where

$$0 \leq i_1 \leq i_2 \leq \ldots \leq i_r \leq m,\ 0 \leq j_1 \leq j_2 \leq \ldots \leq j_r \leq m\,,$$

$(i_1, i_2, \ldots, i_r) \neq (j_i, j_2, \ldots j_r)$. Then

$$x^{d_{i_1}} x^{d_{i_2}} \ldots x^{d_{i_r}} = \alpha\, x^{d_{j_1}} x^{d_{j_2}} \ldots x^{d_{j_r}}$$

where α is an element of $GF(p^n)$. Substituting from (1.7) we have an equation of degree r in x, with coefficients from $GF(p^n)$. This is impossible. Hence the theorem.

Example 2. Let $p^n = 3$, $r = 3$. The roots of the equation $x^4 = 2x^3 + 2x^2 + x + 1$ are primitive elements of $GF(3^4)$ [See Carmichael (2),

p. 262]. If x is any root then we can express the powers of x in the form $ax+b$ where a and b belong to the field $GF(3)$. We get

$$x^0 = 1\,,\ x^1 = x\,,\ 2x^{26} = 1 + x\,,\ 2x^{32} = 2 + x\,.$$

Hence the set of integers

$$d_0 = 0\,,\ d_1 = 1\,,\ d_2 = 26\,,\ d_3 = 32$$

is such that the sum of any three (repetitions allowed) is not equal to the sum of any other three mod (40). This can be directly verified by calculating the 20 sums $d_{i_1} + d_{i_2} + d_{i_3}$, $0 \leq d_{i_1} \leq d_{i_2} \leq d_{i_3} \leq 3$.

3. A B_2-sequence is a sequence of integers

$$d_1, d_2, d_3, \ldots, d_k$$

in ascending order of magnitude, such that the sums $d_i + d_j (i \leq j)$ are all different. Let $F_2(x)$ denote the maximum number of members which a B_2-sequence can have, when no member of the sequence exceeds x. Clearly $F_2(x)$ is a non-decreasing function of x. ERDÖS and TURAN (4) proved that

$$F_2(m)/\sqrt{m} < 1 + \epsilon \tag{3.0}$$

for all positive ϵ and $m > m(\epsilon)$, and conjectured that

$$\underset{n \to \infty}{Lt}\ F_2(m)/\sqrt{m} = 1\,. \tag{3.1}$$

CHOWLA (3) deduced from corollaries 1 and 2, of section 1, that if m is a prime power

$$\text{(i)}\ F_2(m^2) \geq m + 1\,,\quad \text{(ii)}\ F_2(m^2 + m + 2) \geq m + 2\,, \tag{3.2}$$

and proved the conjecture of ERDÖS and TURAN.

We shall here generalize the notion of a B_2-sequence and prove some theorems about these generalized sequences.

A B_r-sequence $(r \geq 2)$ may be defined as a sequence

$$d_1, d_2, d_3, \ldots, d_k$$

of integers in ascending order of magnitude such that the sums

$$d_{i_1} + d_{i_2} + \ldots + d_{i_r} \quad (i_1 \leq i_2 \leq \ldots \leq i_r)$$

are all different. Let $F_r(x)$ denote the maximum number of members a B_r-sequence can have when no member of the sequence exceeds x. Clearly $F_r(x)$ is a non-decreasing function of x. We can then state the following theorem.

Theorem 3. If $m = p^n$, where p is prime, and $r \geq 2$

$$\text{(i) } F_r(m^r) \geq m + 1, \qquad \text{(ii) } F_r\left(1 + \frac{m^{r+1} - 1}{m - 1}\right) \geq m + 2. \tag{3.3}$$

Proof of part (i). Let $m = p^n$, and let $d_1 = 1, d_2, \ldots, d_m$ be integers satisfying the conditions of Theorem 1. Then the sequence

$$d_1 = 1, \ d_2, \ldots, d_m, d_{m+1} = m^r \tag{3.4}$$

is a B_r-sequence. For if possible let

$$d_{i_1} + d_{i_2} + \ldots + d_{i_r} = d_{j_1} + d_{j_2} + \ldots + d_{j_r} \tag{3.5}$$

$1 \leq i_1 \leq i_2 \leq \ldots \leq i_r \leq m + 1$, $1 \leq j_1 \leq j_2 \leq \ldots \leq j_r$, $(i_1, i_2, \ldots, i_r) \neq$ $\neq (j_1, j_2, \ldots j_r)$.

Let d_i occur n_i times on the left hand side of (3.5) and n_i' times on the right hand side of (3.5), $(i = 1, 2, \ldots, m + 1)$. Then

$$n_1 + n_2 + \ldots + n_m + n_{m+1} = n_1' + n_2' + \ldots + n_m' + n_{m+1}' = r \tag{3.6}$$

where

$$(n_1, n_2, \ldots, n_m, n_{m+1}) \neq (n_1', n_2', \ldots, n_m', n_{m+1}'). \tag{3.7}$$

If we replace each d_m in (3.5) by d_1, the relation will remain true mod $(m^r - 1)$ and will contradict Theorem 1, unless

$$(n_1 + n_{m+1}, n_2, \ldots, n_m) = (n_1' + n_{m+1}', n_2, \ldots, n_m). \tag{3.8}$$

In this case it follows from (3.6) and (3.7) that

$$n_1 = n_1' - \theta, \ n_2 = n_2', \ \ldots, \ n_m = n_m', \ n_{m+1} = n_{m+1}' + \theta$$

where θ is a non-zero integer positive or negative.

Hence

$$d_{i_1} + d_{i_2} + \ldots + d_{i_r} = d_{j_1} + d_{j_2} + \ldots + d_{j_r} + \theta(m^r - 1)$$

which contradicts (3.5). Hence (3.4) is a B_r-sequence with $m + 1$ members, where no member exceeds m^r. This shows that $F_r(m^r) \geq m + 1$.

Proof of part (ii). Let $m = p^n$, and let $d_0 = 0$, $d_1 = 1$, $d_2, \ldots, d_m$ satisfy conditions of Theorem 2. Then the sequence

$$d_1 = 1, \ d_2, \ldots, d_m, \ d_{m+1} = q, \ d_{m+2} = q + 1 \tag{3.9}$$

where $q = (m^{r+1} - 1)/(m - 1)$ is a B_r-sequence. For if possible let

$$d_{i_1} + d_{i_2} + \ldots + d_{i_r} = d_{j_1} + d_{j_2} + \ldots + d_{j_r} \tag{3.10}$$

where $1 \leq i_1 \leq i_2 \ldots \leq i_r \leq m + 2$, $1 \leq j_1 \leq j_2 \leq \ldots \leq j_r \leq m + 2$, $(i_1, i_2, \ldots, i_r) \neq (j_1, j_2, \ldots, j_r)$.

Let d_i occur n_i times on the left hand side of (3.10) and n'_i times on the right hand side of (3.10). Then

$$n_1 + n_2 + \dots + n_{m+1} + n_{m+2} = n'_1 + n'_2 + \dots + n'_{m+1} + n'_{m+2} = r \quad (3.11)$$

where

$$(n_1, n_2, \dots, n_{m+1}, n_{m+2}) \neq (n'_1, n'_2, \dots, n'_{m+1}, n'_{m+2}) . \quad (3.12)$$

If we replace each d_{m+1} in (3.11) with d_0 and each d_{m+2} by d_1, the relation remains true $\mod(q)$ and will contradict Theorem 2, unless

$$(n_{m+1}, n_1 + n_{m+2}, n_2, \dots, n_m) = (n'_{m+1}, n'_1 + n'_{m+2}, n_2, \dots, n_m) . \quad (3.13)$$

In this case it follows from (3.11) and (3.12) that

$$n_1 = n'_1 - \theta,\ n_2 = n'_2, \dots, n_{m+1} = n'_{m+1}, n_{m+2} = n'_{m+2} + \theta$$

where θ is a non-zero integer positive or negative. Hence

$$d_{i_1} + d_{i_2} + \dots + d_{i_r} = d_{j_1} + d_{j_2} + \dots + d_{j_r} + \theta q$$

which contradicts (3.10). Hence (3.9) is a B_r-sequence with $m+2$ members, no member of which exceeds $q+1$. This shows that

$$F_r\left(1 + \frac{m^{r+1}-1}{m+1}\right) \geq m + 2 .$$

Example 3. It follows from Examples 1 and 2, that

(i) 1, 14, 34, 103, 119, 125
(ii) 1, 26, 32, 40, 41

are B_3-sequences.

4. Taking $n = 1$ in Theorem 3 (i), we have

$$F_r(p^r) \geq p + 1 \quad (4.0)$$

where p is any prime. Let

$$p \leq y^{1/r} \leq p' \quad (4.1)$$

where p and p' are consecutive primes. It follows from a theorem of INGHAM (5), that

$$p' - p = O(p^{2/3}). \quad (4.2)$$

It follows from the monotonicity of F_r, that

$$F_r(y) \geq F_r(p^r) \geq p + 1 . \quad (4.3)$$

From (4.1) and (4.2)

$$y^{1/r} = p + O(p^{2/3}). \quad (4.4)$$

Since $y^{1/r} \geq p \geq \frac{1}{2}y^{1/r}$, $p = O(y^{1/r})$. Hence from (4.4)

$$p = y^{1/r} - O(y^{2/3r}) . \tag{4.5}$$

From (4.3) and (4.5)

$$F_r(y) \geq y^{1/r} - O(y^{2/3r}) . \tag{4.6}$$

Hence we have

Theorem 4.

$$\varliminf \frac{F_r(y)}{y^{1/r}} \geq 1, \quad y \to \infty .$$

Erdös and Turan (4), proved that for $r = 2$

$$\varlimsup \frac{F_r(y)}{y^{1/r}} \leq 1 \quad \text{as } y \to \infty . \tag{4.7}$$

We may conjecture that (4.7) remains true for $r \geqq 3$, though we gather from conversations with Professor Erdös that this is still unproved. If the conjecture is correct it will follow that

$$\lim_{y \to \infty} \frac{F_r(y)}{y^{1/r}} = 1 \tag{4.8}$$

for $r \geqq 2$. At present we only know this to be true for $r = 2$.

University of North Carolina and University of Geneva
University of Colorado

REFERENCES

[1] R.C.Bose, *An affine analogue of Singer's theorem*, J.Ind.Math.Soc. (new series) *6* (1942), 1–15.

[2] R.D.Carmichael, *Introduction to the theory of groups of finite order*, Dover publications Inc.

[3] S.Chowla, *Solution of a problem of* Erdös *and* Turan *in additive number theory*, Proc.Nat. Acad.Sci.India *14* (1944), 1–2.

[4] Erdös and Turan, *On a problem of Sidon in additive number theory and some related problems*, J.Lond.Math.Soc. (1941), 212–215.

[5] A.E.Ingham, *On the difference between consecutive primes*, Quarterly J.Math., Oxford series, *8* (1937), 255–266.

[6] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans.Amer.Math.Soc. *43* (1938), 377–385.

(Received March 28, 1962)