Canad. Math. Bull. Vol. **53** (4), 2010 pp. 654–660
doi:10.4153/CMB-2010-070-5

Variations on a Paper of Erdős and Heilbronn

In celebration of the one hundredth anniversary of the birth of Hans Arnold Heilbronn

P. D. T. A. Elliott

Abstract. It is shown that an old direct argument of Erdős and Heilbronn may be elaborated to yield a result of the current inverse type.

Let p be a prime, $a_1, \dots, a_k$ distinct non-zero residue classes mod p, and N a residue class mod p. Let

$$F(N) = F(N; p; a_1, \dots, a_k)$$

denote the number of solutions of the congruence

$$e_1 a_1 + \cdots + e_k a_k \equiv N \pmod{p},$$

where the $e_1, \dots, e_k$ are restricted to the values 0 and 1.

In their 1964 paper on the addition of residue classes mod p, Erdős and Heilbronn [2] establish two theorems.

Theorem I $F(N) > 0$ *if* $k \geq 3(6p)^{1/2}$.

Theorem II $F(N) = 2^k p^{-1}(1 + o(1))$ *if* $k^3 p^{-2} \to \infty$ *as* $p \to \infty$.

The proof of Theorem I is elementary, resting in part on a result of Cauchy, rediscovered by Davenport [1], that if A, B are sets of distinct residue classes mod p, of respective cardinalities $|A|, |B|$, then the sums formed by taking an element from each of A and B contain at least $\min(|A| + |B| - 1, p)$ distinct classes.

Featured in their proof is the maximum of a function taken over all the u-element subsets of a (possibly relabelled) subset $a_1, \dots, a_{2u}$ of the a_j, $1 \leq u \leq k/2$.

Erdős and Heilbronn remark that Theorem I is nearly best possible. Their conjecture that the appropriate restriction should be $k > 2p^{1/2}$ was justified by Olson [4].

In this paper I shall concentrate on the second of their theorems, a result that they show to be, in a sense, best possible.

If we set $A = \sum_{n=1}^{k} a_n$, then

$$F(N) = p^{-1} \sum_{r=0}^{p-1} e^{-2\pi i r N} \prod_{n=1}^{k} (1 + e^{2\pi i r a_n / p})$$

$$= p^{-1} 2^k \sum_{r=0}^{p-1} e^{\pi i r (A-2N)/p} \beta_r,$$

Received by the editors November 19, 2007.
Published electronically July 26, 2010.
AMS subject classification: **11L07**, 11P70.

where

$$\beta_r = \prod_{n=1}^{k} \cos(\pi r a_n/p).$$

The aim of Erdős and Heilbronn, achieved in their Lemma II.5, is to establish that, as $p \to \infty$ and $kp^{-2/3} \to \infty$, we have $\sum_{r=1}^{p-1} |\beta_r| \to 0$, from which Theorem II is immediate.

If k is a multiple of 4 and the a_n occur in pairs a_n, $p - a_n$, then

$$F(0) = p^{-1}2^k\Big(1 + \sum_{r=1}^{p-1} \beta_r\Big),$$

every β_r is real and positive, and the property $\beta_1 + \cdots + \beta_{p-1} \to 0$ is necessary.

Erdős and Heilbronn set $\Lambda = \log p$, assume $k < p^{2/3}\Lambda$, and define

$$\sigma(r) = \sigma(r, S_m) = \sum_{n=1}^{m} (\sin(\pi r a_n/p))^2,$$

$$\gamma(r) = \gamma(r, S_m) = \sigma(r, S_m)(m^3 p^{-2})^{-1},$$

where $r \not\equiv 0 \pmod p$ and S_m denotes an m-element subset of the a_j, possibly relabelled.

Supposing there exists an r such that $\sigma(r, S_k) < \Lambda$, they define

$$\mu = \min \gamma(s, S_m)(\Lambda^6 + k - m)$$

taken over all $s \not\equiv 0 \pmod p$ and subsets S_m of S_k with $k/2 \le m \le k$. Since the $\gamma(r)$ are bounded below uniformly in r and S_m, say by $\gamma \ge \gamma_0 > 0$, any m for which μ is attained exceeds $k - \gamma_0^{-1}\Lambda^7$.

They then fix a pair s, S_m for which μ is attained and establish a sequence of five lemmas of which the first two follow.

Lemma II.1 *If $\sigma(r, S_m) < \Lambda$, $r \not\equiv s \pmod p$, then there exist integers u, v such that $vr \equiv us \pmod p$, $(u, v) = 1$, $1 \le v \le \Lambda$, $1 \le u \le \Lambda^2$.*

Further, assuming the residue classes sa_n, $1 \le n \le m$, are represented by numbers in the interval $[-p/2, p/2]$, these numbers are divisible by v with at most $2\Lambda^3 m^3 p^{-2}$ exceptions.

Lemma II.2 *$v = 1$ under the conditions of Lemma II.1.*

It might be said that the tactic used by Erdős and Heilbronn was to prune the a_n until they reached a subset S_m, with m/k not too small, for which the small $\sigma(r, S_m)$ have a structure adequate to an estimate from below.

In fact, the minimality of μ does not enter into play until the second of these results, and it is worthwhile to relieve their combined argument of its particularities.

I begin again. For an odd prime p and distinct residue class representatives a_j, $j = 1, \ldots, k$, define

$$\sigma(r) = \sigma(r, S_k) = \sum_{j=1}^{k} (\sin \pi r a_j/p)^2.$$

https://doi.org/10.4153/CMB-2010-070-5 Published online by Cambridge University Press

Lemma A *Assume that for distinct non-zero residue classes r and s (mod p), we have* $\sigma(r) \le \Delta$ *and* $\sigma(s) \le \Delta$, *where* $k \ge \max(14, (32p)^{4/7}\Delta^{3/7})$. *Then there are integers* u, v, $1 \le u \le \lambda^2$, $1 \le v \le \lambda$, $(u, v) = 1$, *with* $\lambda = 16pk^{-3/2}\Delta^{1/2}$, *for which* $rv \equiv su \pmod p$.

Proof Without loss of generality $s = 1$ and $|a_j| < p/2$ for all j.

By Dirichlet's box principle, if $\lambda \ge 1$, then there are integers u, v, $(u, v) = 1$, $1 \le v \le \lambda$, $1 \le u \le p\lambda^{-1}$, such that $rv \equiv su \pmod p$. Set $vr = su + qp$.

By hypothesis $(\sin \pi r a_j/p)^2 \ge 4\Delta/k$ cannot hold for more than $k/4$ of the a_j; likewise, $(\sin \pi a_j/p)^2 \ge 4\Delta/k$. Set $\rho = (\Delta/k)^{1/2}$. Then there are at least $[(k+1)/2]$ integers n for which $|a_n| < p\rho$, $|ra_n - \tau_n p| < p\rho$ hold, the τ_n integers. With $h_n = -qa_n + v\tau_n$, we see that

$$|ua_n - h_n p| < vp\rho \le \lambda p\rho.$$

The interval $[-p\rho, p\rho]$ contains at least $[(k+1)/2]$ of the a_n; thus there exists a pair a', a'', such that $0 < a'' - a' \le 2p\rho(k/2 - 1)^{-1} < 8p\rho/k$.

By subtraction, there is an integer h such that $u(a'' - a') - hp| < 2\lambda p\rho$. Since $u(a'' - a') < p\lambda^{-1}8p\rho k^{-1}$, if $2\rho\lambda + \lambda^{-1}8p\rho k^{-1} \le 1$, then $h = 0$. For example, if we set $\lambda = 16p\rho k^{-1}$, then $2\rho\lambda = 32p\rho^2 k^{-1} = 32p\Delta k^{-2} \le 1/3$.

Thus $h = 0$ and $u \le u(a'' - a') < 2\lambda p\rho$.

Consider now how many integers w, whatsoever, can satisfy $|w| < p\rho$ and for some integer t, $|uw - tp| < \lambda p\rho$. For a fixed t, there are $\le 1 + 2\lambda p\rho u^{-1}$ choices for w. Moreover, $|t| < p^{-1}(\lambda p\rho + up\rho)$. Altogether, the number of values for w cannot exceed

$$(1 + 2\lambda p\rho u^{-1})(1 + 2(\lambda + u)\rho) = 1 + 2\lambda\rho + 4\lambda p\rho^2 + 2\lambda p\rho(1 + 2\lambda\rho)u^{-1} + 2u\rho.$$

As arranged earlier, $2\lambda\rho \le 1/3$. Moreover, from the improved bound on u, $2u\rho \le 4\lambda p\rho^2$. Then $8\lambda p\rho^2 = 8.16p^2k^{-1}(\Delta k^{-1})^{3/2} \le k/8$ from our upper bound on Δ.

Further, if $u > \lambda^2$, then

$$2\lambda p\rho(1 + 2\lambda\rho)u^{-1} < 3\lambda p\rho u^{-1} < 3p\rho\lambda^{-1} = 3k/16.$$

Our upper bound is thus less than $3/2 + 3k/16 + k/8 < k/2 - 1$. This contradicts the existence of at least $[(k+1)/2]$ of the restricted a_j.

Hence $u \le \lambda^2$, and the lemma is justified. ∎

Under the conditions on k, Δ in Lemma A, there are at most $(16pk^{-3/2}\Delta^{1/2})^3$ values of r for which $\sigma(r) \le \Delta$. This corresponds to only the first part of Lemma II.1, but it is already enough to furnish Theorem II.

For $r \not\equiv 0 \pmod p$, we have

$$|\beta_r| \le \prod_{n=1}^{k} |\cos(\pi r a_n/p)| \le \Big(k^{-1}\sum_{n=1}^{k}\big(\cos(\pi r a_n/p)\big)^2\Big)^{k/2}$$
$$= \big(1 - k^{-1}\sigma(r, S_k)\big)^{k/2} \le \exp\big(-\sigma(r, S_k)/2\big).$$

https://doi.org/10.4153/CMB-2010-070-5 Published online by Cambridge University Press

Considering those r for which $2^j\alpha \le \sigma(r) \le 2^{j+1}\alpha$, $j = 0, 1, \dots$, where α is a minimal value of $\sigma(r)$, we have

$$\sum_{r=1}^{p-1} |\beta_r| \le (16pk^{-3/2}\alpha^{1/2})^3 \sum_{j=0}^{\infty} 2^{3(j+1)/2} \exp(-2^{j-1}\alpha) + p\exp(-k^{7/3}(32p)^{-4/3}).$$

Here,

$$\alpha \ge 2\sum_{m=1}^{[k/2]} 4(m/p)^2 > (8/3)p^{-2}[k/2]^3 > k^3/(5p^2).$$

If $k^3 \ge p^2$, then

$$F(N) = 2^k p^{-1}\Big(1 + O\big(\exp(-k^3/(10p^2)) + \exp(-2^{-7}p^{2/9})\big)\Big)$$

and Theorem II is evident.

Since there has been no application of minimality, we may interchange the rôles of r and s and obtain integers $u_1, v_1, (u_1, v_1) = 1, 1 \le u_1 \le \lambda^2, 1 \le v_1 \le \lambda$ for which $u_1 r \equiv v_1 s \pmod p$.

Eliminating between the pair of congruences involving r and s gives $vv_1 - uu_1 \equiv 0 \pmod p$. Moreover, $|vv_1 - uu_1| \le \max(1, \lambda^4) < p$ provided $\Delta < (16)^{-2}k^{3/2}p^{-3/2}$. From what we have already required of Δ, $k > 4p^{1/4}$ will certainly secure this. Hence $vv_1 = uu_1$, u divides v_1 and satisfies the stronger bound $u \le \lambda$.

I now enjoin the ideas of Lemma II.2 and, as the account of that lemma by Erdős and Heilbronn is abbreviated, elaborate.

Lemma B *If $k \ge 28$, $\Delta \le \min(k^{7/3}(2^7p)^{-4/3}, 2^{11}k^3p^{-3/2})$, then the reduced residue classes $r \pmod p$ for which $\sigma(r, S_k) \le \Delta$ lie in a progression us, $1 \le u \le \lambda_1$ with $\lambda_1 = 2^{11/2}k^{-3/2}\Delta^{1/2}p$.*

Individual $\sigma(us, S_k)$ may still exceed Δ.

Proof For a positive real τ to be chosen later, let m, T give a minimal value δ for $\sigma(r, B)(\tau + k - r)$ taken over all subsets B of S_k with a cardinality $|B| \ge k/2$ and all reduced residue classes $r \pmod p$.

Without loss of generality, there is a t for which $\sigma(t, S_k) \le \Delta$. Hence,

$$\sigma(m, T)(\tau + k - |T|) \le \sigma(t, S_k)\tau \le \Delta\tau.$$

In particular, $\sigma(m, T) \le \Delta$. Moreover, for $k \ge 28$, $\sigma(m, T) \ge k^3(40p^2)^{-1}$, so that $|T| \ge k - 40p^2\Delta\tau k^{-3} + \tau$.

Suppose there is an $r \not\equiv m \pmod p$ for which $\sigma(r, T) \le \Delta$. We apply Lemma A and, under the slightly stronger restriction on Δ obtained by replacing k with $k/2$, obtain integers u, v, $1 \le u \le \lambda_1$ (which is λ with k replaced by $k/2$), $1 \le v \le \lambda_1$, $(u, v) = 1$, for which $rv \equiv um \pmod p$.

Of the a_j in T, at most $\lambda_1^2\Delta$ satisfy $(\sin \pi r a_j/p)^2 \ge \lambda_1^{-2}$, and a similar number $(\sin \pi m a_j/p)^2 \ge \lambda_1^{-2}$. The members of the remaining set, which we call Y, satisfy $||ra_j/p|| < (2\lambda_1)^{-1}$, $||ma_j/p|| < (2\lambda_1)^{-1}$.

https://doi.org/10.4153/CMB-2010-070-5 Published online by Cambridge University Press

Again we may assume $m = 1$ and $|a_j| < p/2$. Then $|a_j| < p(2\lambda_1)^{-1}$ and, in the notation of Lemma A, $|ra_j - \tau_j p| < p(2\lambda_1)^{-1}$. Therefore,

$$|ua_j - h_j p| < vp(2\lambda_1)^{-1} \le p/2 \quad \text{and} \quad |ua_j| < \lambda_1(p2\lambda_1)^{-1} = p/2.$$

Hence, $h_j = 0$, *i.e.*, $v\tau_j = qa_j$. Since $rv = mu + qp = u + qp$ and $(u, v) = 1$, we have $(v, q) = 1$ and $v \mid a_j$. This is the second part of Lemma II.1.

Consider now

$$\sigma(\bar{v}, Y) = \sum_{a_j \in Y} (\sin \pi v^{-1} a_j p^{-1})^2,$$

where $v\bar{v} \equiv 1 \pmod{p}$, and we apply that for integers a_j in Y, $p^{-1}(v\bar{v} - 1)v^{-1}a_j$ is an integer. Typically,

$$|\sin(\pi v^{-1} a_j p^{-1})| \le \pi v^{-1} |a_j p^{-1}| \le \pi (2v)^{-1} |\sin(\pi a_j p^{-1})|.$$

As a consequence,

$$\sigma(\bar{v}, Y) \le (\pi/(2v))^2 \sigma(1, Y) \le (\pi/(2v))^2 \sigma(1, T),$$

and

$$\sigma(\bar{v}, Y)(\tau + k - |Y|) \le (\pi(2v)^{-1})^2 (1 + \tau^{-1}(|T| - |Y|))\sigma(1, T)(\tau + k - |T|).$$

Since $|T| - |Y| \le 2\lambda_1^2 \Delta$, if $v > 1$ and we choose $\tau = 6\lambda_1^2 \Delta$, then

$$(\pi/(2v))^2 (1 + \tau^{-1}(|T| - |Y|)) < \tfrac{11}{12}.$$

This will contradict the minimality of δ unless $|Y| < k/2$ and, in particular, $k/2 < 40p^2\tau k^{-3}$. However, with our choice of τ, the first bound on Δ ensures that this last expression does not exceed $2^{-9}k$.

Thus $v = 1$. Moreover, if $r \not\equiv us \pmod{p}$, $1 \le u \le \lambda_1$, then $\sigma(r, S_k) \ge \sigma(r, T) > \Delta$.

Lemma B is established. ∎

As a corollary, if $k \ge 2^6 p^{4/7} (\log p)^{3/7}$, then $F(N) \ll 2^k k^{-3/2}$. To this end we need only that

$$\sum_{j=0}^{\infty} (2^j \alpha)^{1/2} \exp(-2^j \alpha)$$

is bounded uniformly in $\alpha > 0$. For $\alpha \ge 1$, this is straightforward. If $\alpha < 1$ and we define the integer w by $2\alpha^w \le 1 < 2^{w+1}\alpha$, then the terms with $j \ge w$ may also be readily treated. The remaining terms contribute

$$\le \alpha^{1/2} \sum_{j=0}^{w-1} (\sqrt{2})^j = \alpha^{1/2}((\sqrt{2})^w - 1)(\sqrt{2} - 1)^{-1} \le 3(2^w \alpha)^{1/2} \le 3.$$

In a subsequent treatment of concentration functions using Fourier analysis, Halász [3], yields the concentration estimate implicit in Lemma B subject to the weaker

https://doi.org/10.4153/CMB-2010-070-5 Published online by Cambridge University Press

condition (say) $\Delta \le k/4$ from which the bound $F(N) \ll 2^k k^{-3/2}$ follows unconditionally. The method, which is flexible and short, again employs results of Cauchy–Davenport type, but does not characterize those r for which $\sigma(r, S_k)$ is small. For a related combinatorial treatment of such concentration estimates, see Sárközy and Szemerédi [5].

Adapting the further argument of Erdős and Heilbronn to the circumstances of Lemma B and without loss of generality assuming $s = 1$, at most $k/2$ of the a_j in S_k satisfy $(\sin(\pi a_j/p))^2 \ge 2k^{-1}\Delta$. For the remaining sequence, W say,

$$\sum_{a_j \in W} (\sin(\pi a_j/p))^4 < 2k^{-1}\Delta^2.$$

Since

$$(\sin(t\alpha))^2 - (t\sin\alpha)^2 \ll (t^2 + t^4)(\sin\alpha)^4$$

holds for all real t and α, $|\alpha| \le \pi/2$ (the solo upper bound factor t^4 in Erdős and Heilbronn is untenable for small t), there is a lower bound estimate

$$\sigma(u, S_k) \ge u^2(\sigma(1, W) - c_0 u^2 k^{-1}\Delta^2) \ge c_1 u^2(k^3 p^{-2} - c_2 u^2 k^{-1}\Delta^2)$$

for all integers u, $1 \le u \le \lambda_1$; and a bound $\sigma(r, S_k) > \Delta$ for the remaining $r \not\equiv 0 \pmod p$.

This is the essential content of Lemma II.4 of Erdős and Heilbronn and is again adequate to deliver Theorem II.

Having symmetrized the argument of Erdős and Heilbronn, we may arrange for the a_n to act upon the r.

Lemma C *If there are m reduced classes $r \pmod p$ for which $\sigma(r, S_k) \le \Delta$, then after removing at most*

$$28 + \max((2^7 p)^{4/3} m^{-4/3}, 2^{11} p^{3/2} m^{-2})\Delta$$

members of S_k, the remaining a_n are contained in an arithmetic progression $us \pmod p$, $1 \le u \le \min(2m^{-1/3}p^{1/3}, p^{1/4})$.

Proof There are r_t, $1 \le t \le m$, such that

$$\sum_{t=1}^{m} \sum_{n=1}^{k} (\sin(\pi r_t a_n/p))^2 \le m\Delta.$$

Let $M > 0$ and denote the set of classes $r_t \pmod p$ by R. Interchanging the order of summation, we obtain at least $k - m\Delta/M$ of the a_j for which $\sigma(a_j, R) \le M$.

We apply Lemma B to this dual system. If $k - m\Delta/M \ge 28$ and

$$M \le \min(m^{7/3}(2^7 p)^{-4/3}, 2^{-11} m^3 p^{-3/2}),$$

then our remaining a_j lie in an arithmetic progression

$$us \pmod p, 1 \le u \le 2^{11/2} m^{-3/2} p M^{1/2}.$$

Choosing M to effect equality with its upper bound, we may rapidly complete the argument. ∎

https://doi.org/10.4153/CMB-2010-070-5 Published online by Cambridge University Press

No attempt has been made to sharpen this result, which becomes non-trivial if k is below approximately $p^{1/4}$.

Underlying Lemma C is the notion that the dual of the operator

$$(z_j) \in \mathbb{C}^k \to \Big(\sum_{r=0}^{k} z_j (\sin(\pi r_t a_j/p))^2 \Big) \in \mathbb{C}^m$$

with L^∞ norms is the operator

$$(y_t) \in \mathbb{C}^m \to \Big(\sum_{t=1}^{m} y_t (\sin(\pi r_t a_j/p))^2 \Big) \in \mathbb{C}^k$$

with L^1 norms.

We have reached a result that is (in current parlance) of inverse type.

"Read the masters!" said Davenport. What excellent advice.

References

[1] H. Davenport. *On the addition of residue classes.* Journ. London Math. Soc. **10**(1935), 30–32.
[2] P. Erdős and H. Heilbronn, *On the addition of residue classes mod p.* Acta Arith. **9**(1964), 149–159.
[3] G. Halász, *Estimates for the concentration function of combinatorial number theory and probability.* Period. Math. Hungar. **8**(1977), 3–4, 197–211. doi:10.1007/BF02018403
[4] J. E. Olson, *An addition theorem modulo p.* J. Comb. Th. **5**(1968), 45–52. doi:10.1016/S0021-9800(68)80027-4
[5] A. Sárközy and E. Szemerédi, *Über ein Problem von Erdős and Moser.* Acta Arith. **11**(1965), 205–208.

Boulder, Colorado
e-mail: pdtae@euclid.colorado.edu