Heini Halberstam

Sieve methods and applications

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, nº 1 (1967-1968), exp. nº 7, p. 1-8

<http://www.numdam.org/item?id=SDPP_1967-1968__9_1_A7_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des Nombres)
9e année, 1967/68, n° 7

14 décembre 1967

SIEVE METHODS AND APPLICATIONS (*)

by Heini HALBERSTAM

1. - Let M , N be positive integers and $\mathfrak{A}$ a sequence of distinct natural numbers in the interval $[M + 1 , M + N]$. If the cardinality A of $\mathfrak{A}$ is not too small compared with N we may expect that almost all residue classes mod p for almost all primes p that are not too large, contain elements of $\mathfrak{A}$. This "sieve principle" was first put into a quantitative form by LINNIK [7], but we shall follow here the formulation of RÉNYI [10].

For any natural number q , define

$$A(q , h) = \sum_{\substack{n\in\mathfrak{A} \\ n\equiv h \bmod q}} 1$$

so that

$$\sum_{h=1}^{q} A(q , h) = A .$$

If $\mathfrak{A}$ were well-distributed among the residue classes mod p for a particular prime p , we should expect each residue class to contain about A/p elements of $\mathfrak{A}$. Accordingly, the expression

$$D_p = \sum_{h=1}^{p} \{A(p , h) - \frac{A}{p}\}^2$$

is a measure of the way $\mathfrak{A}$ is distributed among the residue classes mod p , and a non-trivial inequality of type

$$\sum_{p\leqslant X} pD_p \leqslant K(N , A , X) , \qquad (X < N)$$

uniform in the sense that K does not depend on the individual arithmetic structure of $\mathfrak{A}$, would constitute a quantitative expression of Linnik's principle. What does "non-trivial" mean ? We have

$$pD_p = p \sum_{h=1}^{p} A^2(p , h) - A^2 \leqslant p \sum_{h=1}^{p} A^2(p , h) \tag{1}$$

(*) The presentation derives to a considerable extent from the forthcoming monograph on sieve methods by HALBERSTAM and RICHERT.

and

$$A(p\ ,\ h) \leqslant \frac{N}{p} + 1 \leqslant \frac{2N}{p}$$

uniformly in $\mathfrak{A}$, for all $p < N$. Hence, by (1)

$$pD_p \leqslant p\,\frac{2N}{p}\sum_{h=1}^{p} A(p\ ,\ h) = 2NA\ ,$$

so that, trivially,

(2) $$\sum_{p\leqslant X} pD_p \leqslant 2NAX\ ;$$

we ask therefore whether one can improve on (2).

2. - We transform the question to one about mean values of trigonometric sums. Define

$$S(x) = \sum_{n\in\mathfrak{A}} e^{2\pi inx}\ .$$

then

$$\sum_{a=1}^{p-1} |S(\tfrac{a}{p})|^2 = \sum_{n\in\mathfrak{A}}\ \sum_{n'\in\mathfrak{A}}\ \sum_{a=1}^{p-1} e^{2\pi i(n-n')a/p}$$

and the inner sum is $p - 1$ if $n \equiv n' \mod p$ and -1 otherwise. Hence the sum is equal to

$$p \sum_{n\in\mathfrak{A}} \sum_{\substack{n'\in\mathfrak{A} \\ n\equiv n' \bmod p}} 1 - A^2 = p \sum_{h=1}^{p} \Big(\sum_{\substack{n\in\mathfrak{A} \\ n\equiv h \bmod p}} 1\Big)^2 - A^2\ ,$$

so that, by (1),

(3) $$pD_p = \sum_{a=1}^{p-1} |S(\tfrac{a}{p})|^2\ .$$

We shall be concerned from now on with non-trivial estimates of the sum

(4) $$\sum_{p\leqslant X} \sum_{a=1}^{p-1} |S(\tfrac{a}{p})|^2\ ,$$

We begin by remarking that the sum (4) does not exceed

(5) $$\sum_{q\leqslant X} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(\tfrac{a}{q})|^2\ .$$

and that the expression (5) is simply a special case of sum of type

(6) $$\sum_{r=1}^{R} |S(x_r)|^2$$

where the real numbers x_r are distinct mod 1 and, if $\|\theta\|$ denotes the distance of θ from the nearest integer, the numbers x_r are "well-separated" in the sense that there exists $\delta > 0$ such that

$$\|x_i - x_j\| \geq \delta \qquad \text{if } i \neq j .$$

If the numbers x_r are taken to be the Farey series a/q $(1 \leqslant a \leqslant q , (a , q) = 1)$ of order X , then X^{-2} is an admissible value of δ and (6) becomes (5).

Finally, we introduce

$$S_0(x) = \sum_{n=-U}^{U} b_n e^{2\pi inx}$$

where the b_n are <u>any</u> complex numbers. Putting

$$U = \begin{cases} \frac{1}{2}(N - 1) , & 2 \nmid N , \\ \frac{1}{2}N , & 2 | N , \end{cases}$$

and $b_n = a_{n+M+1+U}$ (in the latter case, the case of N even, adding a term with $a_{N+M+1} = 0$) we obtain

$$|S_0(x)| = |\sum_{n=M+1}^{M+N} a_n e^{2\pi inx}| ;$$

in particular, taking a_n to be the characteristic function of $\mathfrak{a}$, we have, in this special case, $|S_0(x)| = |S(x)|$. Then our problem is to obtain a non-trivial estimate of sums of type

(7) $$\sum_{r=1}^{R} |S_0(x_r)|^2 .$$

3. - We follow the particularly simple treatment of GALLAGHER [5]. We have

$$S_0^2(x) - S_0^2(x_r) = 2 \int_{x_r}^{x} S_0(y) S_0'(y) \, dy$$

so that

$$|S_0(x_r)|^2 \leqslant |S_0(x)|^2 + 2|\int_{x_r}^{x} |S_0 S_0'|| .$$

Integrate with respect to x over the interval $(x_r - \frac{1}{2}\delta , x_r + \frac{1}{2}\delta)$, to arrive at

$$\delta |S_0(x_r)|^2 \leqslant \int_{x_r-\frac{1}{2}\delta}^{x_r+\frac{1}{2}\delta} |S_0(x)|^2 \, dx + \delta \int_{x_r-\frac{1}{2}\delta}^{x_r+\frac{1}{2}\delta} |S_0(y) \, S_0'(y)| \, dy ,$$

and sum over r . In view of the definition of δ , the intervals $(x_r - \frac{1}{2}\delta , x_r + \frac{1}{2}\delta)$ $(r = 1 , \dots , R)$ are pairwise disjoint, so that

$$\sum_{r=1}^{R} |S_0(x_r)|^2 \leqslant \delta^{-1} \int_0^1 |S_0|^2 + \int_0^1 |S_0 \, S_0'| ;$$

writing

$$Z_0 = \sum_{-U}^{U} |b_n|^2 = \int_0^1 |S_0|^2 ,$$

we obtain, by Cauchy's inequality, that the expression on the right is at most

$$\delta^{-1} Z_0 + Z_0^{1/2} (\int_0^1 |S_0'|^2)^{1/2} \leqslant \delta^{-1} Z_0 + Z_0^{1/2} (4\pi^2 U^2 Z_0)^{1/2} = (\delta^{-1} + 2\pi U) Z_0 .$$

One can improve on this estimate by more accurate methods, and I summarise the present state of knowledge in the following theorem :

THEOREM 1.

$$\sum_{r=1}^{R} |S_0(x_r)|^2 \leqslant \begin{cases} (\delta^{-1} + 2\pi U) \, Z_0 \\ 2 \max(2U , \delta^{-1}) \, Z_0 \\ ((2U)^{1/2} + \delta^{-1/2})^2 \, Z_0 \end{cases}$$

Of these, the tint is in GALLAGHER [5] ; the second and third one based on the method of DAVENPORT-HALBERSTAM [3] and will appear in BOMBIERI-DAVENPORT [2].

As an immediate corollary, we obtain :

THEOREM 2.

$$\sum_{p \leqslant X} pD_p \leqslant \sum_{q \leqslant X} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(\tfrac{a}{q})|^2 \leqslant \begin{cases} (\pi N + X^2) \, A \\ 2 \max(N , X^2) \, A \\ (N^{1/2} + X)^2 \, A \end{cases}$$

If $X \leqslant N^{1/2}$, the second estimate gives the best result, namely $2NA$; if $X = o(N^{1/2})$, the third gives the best estimate, $(1 + o(1))NA$. It is now clear that the saving on compared with the trivial estimate $2NAX$ (cf. (2)) is very considerable (a whole factor X , in fact).

RÉNYI [11] was the first to obtain such an estimate, valid only for $X \leqslant \frac{1}{2} N^{1/3}$. Decisive progress was made by K. F. ROTH [12], who increased the range of validity up to $X \leqslant (N/\log N)^{1/2}$. Shortly afterwards BOMBIERI [1] improved Roth's range slightly to $X \leqslant N^{1/2}$. All the methods of proof were rather complicated.

4. - Let $z(p)$, for each $p \leqslant N^{1/2}$, denote the number of residue classes mod p containing no elements of $\mathfrak{A}$. Clearly $z(p) < p$. Then :

THEOREM 3. - $A \sum_{p \leqslant N^{1/2}} \frac{z(p)}{p - z(p)} \leqslant 2N$.

Proof. - The A elements of $\mathfrak{A}$ are distributed among $p - z(p)$ residue classes h mod p. Let $\sum_h'$ denote summation over these non-empty classes. Then, by Cauchy's inequality,

$$\frac{p}{p - z(p)} A^2 = \frac{p}{p - z(p)} \Big(\sum_h{}' A(p , h)\Big)^2 \leqslant p \sum_{h=1}^{p} A^2(p , h) = pD_p + A^2$$

by (1), whence

$$\frac{z(p)}{p - z(p)} A^2 \leqslant pD_p .$$

Hence the result, using the second estimate of theorem 2.

The form of this result is due essentially to GALLAGHER [5].

The following application underlines the relevance of these theorems to the original Linnik principle.

THEOREM 4. - *Let* α *satisfy* $0 < \alpha < 1$. *With the notation of theorem 3, let* Y *denote the number of primes* $p \leqslant N^{1/2}$ *for which* $z(p) > \alpha p$. *Then*

$$Y \leqslant 2 \frac{1 - \alpha}{\alpha} \frac{N}{A} .$$

Proof. - For each p counted by Y, $\frac{z(p)}{p - z(p)} \geqslant \frac{\alpha}{1 - \alpha}$. Now apply theorem 3.

We observe that if A is large, Y is small. In particular, if $A > CN$ $(0 < C < 1)$, the number Y of "exceptional" primes is bounded.

For all but at most Y exceptional primes, $\mathfrak{A}$ contains elements in at least $(1 - \alpha)p$ residue classes mod p, $p \leqslant N^{1/2}$.

We describe another application of theorem 3, discovered by LINNIK [8]. First a preliminary result :

THEOREM 5. - <u>Let</u> $\eta(p)$ <u>denote the least quadratic non-residue</u> mod p . <u>Suppose</u> $x \geq y \geq 1$ <u>and define</u> $\Psi(x , y)$ <u>to be the number of natural numbers less than</u> or <u>equal to</u> x , <u>divisible by no prime greater than</u> y . <u>Then</u>

$$\sum_{\substack{p \leq x \\ \eta(p) > y}} 1 \leq \frac{4x^2}{\Psi(x^2 , y)} .$$

<u>Proof</u>. - It is well-known that $\eta(p)$ is itself prime, so that if $\eta(p) > y$, all primes $\leq y$ are quadratic residues mod p . Hence so are all numbers $\leq x^2$ made up entirely of primes $\leq y$. Take these numbers to be our set $\mathfrak{A}$, so that $A = \Psi(x^2 , y)$. Then the elements of $\mathfrak{A}$ are restricted to at most $\frac{1}{2}(p + 1)$ residue classes mod p for each prime $p \leq x$ with $\eta(p) > y$. Applying theorem 3 with $N = x^2$, we obtain

$$\sum_{\substack{p \leq x \\ \eta(p) > y}} \frac{p - 1}{p + 1} \leq \frac{2x^2}{\Psi(x^2 , y)} ,$$

whence the result.

It is conjectured that $\eta(p) = O(p^{\varepsilon})$, and in support of this conjecture we have the following theorem :

THEOREM 6. - <u>Let</u> ε <u>be any number satisfying</u> $0 < \varepsilon < \frac{1}{2}$. <u>Then the number</u> $R = R(x)$ <u>of primes</u> p , $x^{\varepsilon} \leq p \leq x$, <u>whose least quadratic non-residues</u> $\eta(p)$ <u>satisfy</u> $\eta(p) > p^{\varepsilon}$, <u>is bounded ; provided</u> $x \geq x_0(\varepsilon)$. <u>Indeed</u>,

$$R \leq 4 \exp\{u(\log u + \log\log u + 4)\} , \qquad u = 2\varepsilon^{-2} .$$

<u>Proof</u>. - For each p counted in R we have $\eta(p) > p^{\varepsilon} \geq x^{\varepsilon^2}$. Hence

$$R \leq 4x^2/\Psi(x^2 , x^{\varepsilon^2})$$

by theorem 5, and it can be proved that

$$\Psi(y^u , y) \geq y^u \exp\{- u(\log u + \log\log u + 4)\} \qquad \text{if } u > e^2 , \quad y \geq y_0(u) .$$

In our case take $y^u = x^2$, $y = x^{\varepsilon^2}$ (so that $u = 2\varepsilon^{-2}$) to arrive at the result stated.

Using Rényi's form of theorem 2, ERDÖS [4] proved that

$$\sum_{p \leq x} \eta(p) \sim \frac{x}{\log x} \sum_{n=1}^{\infty} p_n 2^{-n} \qquad (x \to \infty) ,$$

in further support of the conjecture.

5. - It has been shown recently by MONTGOMERY [9] that the correct generalisation of (3) is the identity

$$(8)\qquad q\sum_{h=1}^{q}\Big|\sum_{d|q}\frac{\mu(d)}{d}A\left(\frac{q}{d},h\right)\Big|^2=\sum_{\substack{a=1\\(a,q)=1}}^{q}\Big|S\left(\frac{a}{q}\right)\Big|^2 ,$$

which readily reduces to (3) if q is prime.

Just as (3) and theorem 2 led to theorem 3, so MONTGOMERY showed (although the proof is much more complicated) that (8) combines with theorem 2 to give :

THEOREM 7. - $A\sum_{q\leqslant X}\mu^2(q)\prod_{p|q}\frac{z(p)}{p-z(p)}\leqslant (N^{1/2}+X)^2$.

It is very interesting to note that $\mathfrak{A}$ can be the sequence of integers left in the interval $[M+1 , M+N]$ when we have removed from this interval all those integers lying in one of $z(p)$ residue classes mod p for each $p\leqslant X$. In other words, theorem 7 is an upper bound sieve estimate of the Brun-Selberg type.

For example, if $z(p)=1$ for each $p\leqslant X$, we have

$$A\leqslant\frac{(N^{1/2}+X)^2}{\sum_{q\leqslant X}\frac{\mu^2(q)}{\Phi(q)}} ;$$

and if we take $X=N^{1/2}/\log\log N$ we find, using $\sum_{q\leqslant X}\frac{\mu^2(q)}{\Phi(q)}\geqslant\log X$, that

$$\pi(M+N)-\pi(M)<\frac{2N}{\log N}\left(1+O\left(\frac{\log\log N}{\log N}\right)\right) ,$$

a result known (without the log log N factor) from SELBERG [13].

Lower bound estimates are much harder to find, but for the most recent sharp results see HALBERSTAM, JURKAT and RICHERT [6].

BIBLIOGRAPHY

[1] BOMBIERI (E.). - On the large sieve, Mathematika, London, t. 12, 1965, p. 201-225.

[2] BOMBIERI (E.) and DAVENPORT (H.), in "Landau Memorial Volume" (to appear).

[3] DAVENPORT (H.) and HALBERSTAM (H.). - The values of a trigonometrical polynomial at well spaced points, Mathematika, London, t. 13, 1966, p. 91-96.

[4] ERDÖS (Pál). - Számelméleti megjegyzések I, Matematikai Lapok, t. 12, 1961, p. 10-17.

[5] GALLAGHER (P. X.). - The large sieve, Mathematika, London, t. 14, 1967, p. 14-20.

[6] HALBERSTAM (H.), JURKAT (W.) et RICHERT (H.-E.). - Un nouveau résultat de la méthode du crible, C. R. Acad. Sc. Paris, t. 264, 1967, Série A, p. 920-923.

[7] LINNIK (Ju. V.). - The large sieve [in Russian], Doklady Akad. Nauk SSSR, N. S., t. 30, 1941, p. 292-294.

[8] LINNIK (Ju. V.). - A remark on the least quadratic non-residue [in Russian], Doklady Akad. Nauk SSSR, N. S., t. 36, 1942, p. 119-120.

[9] MONTGOMERY (H. L.), in "Mordell Volume", J. London math. Soc. (to appear).

[10] RÉNYI (Alfred). - Un nouveau théorème concernant les fonctions indépendantes et ses applications à la théorie des nombres, J. Math. pures et appl., Série 9, t. 28, 1949, p. 137-149.

[11] RÉNYI (Alfred). - On the representation of an even number as the sum of a single prime and a single almost-prime number [in Russian], Izvest. Akad. Nauk SSSR, Ser. Mat., t. 12, 1948, p. 57-78.

[12] ROTH (K. F.). - On the large sieves of Linnik and Rényi, Mathematika, London, t. 12, 1965, p. 1-9.

[13] SELBERG (Atle). - On elementary methods in primenumber-theory and their limitations, Den 11te Skandinaviske Matematikerkongress [1949. Trondheim], p. 13-22. - Oslo, Johan Grundt Tanums Forlag, 1952.