MÉMOIRES DE LA S. M. F.

DIETER WOLKE

Farey fractions with prime denominator and the large sieve

Mémoires de la S. M. F., tome 25 (1971), p. 183-188
<http://www.numdam.org/item?id=MSMF_1971__25__183_0>

Colloque Th. Nombres [1969, Bordeaux]
Bull. Soc. math. France,
Mémoire 25, 1971, p. 183 à 188

FAREY FRACTIONS WITH PRIME DENOMINATOR AND THE LARGE SIEVE

by

Dieter WOLKE

-:-:-:-

An interesting problem which arises in connection with the "large sieve" is the following one.

Let Q and N be positive numbers, let M be a real number let a_n $(M < n \leq M+N)$ be any complex numbers. Write

$$S(\alpha) = \sum_n a_n \, e(n\,\alpha) \qquad (e(\beta) = e^{2\pi i\beta}) ,$$

$$A = \sum_n a_n \quad , \qquad A\,(p,b) = \sum_{n \equiv b \bmod p} a_n \quad (p \text{ prime}) ,$$

$$Z = \sum_n |a_n|^2 .$$

We wish an upper bound for the sum

$$\text{(P)} \qquad \sum_{p \leq Q} \sum_{b=1}^{p-1} |S(\tfrac{b}{p})|^2 = \sum_{p \leq Q} p \sum_{b=1}^{p} |\tfrac{A}{p} - A(p,b)|^2 ,$$

which is a measure for the distribution of the a_n's over the residue classes mod p .

Instead of (P) all authors who worked in this subject estimated the larger sum

$$\text{(R)} \qquad \sum_{r \leq Q} \sum_{\substack{b=1 \\ (b,r)=1}}^{r} |S(\tfrac{b}{r})|^2 ,$$

in which r runs over all positive integers $\leq Q$. The result, which in general, and except the value of the constant, is best possible, is

$$\text{(I)} \qquad \text{(R)} \ll (Q^2 + N)\, Z .$$

(see Bombieri, Davenport-Halberstam, Gallagher).

It is natural to ask whether by passing from (P) to (R) one looses a factor $(\ln Q)^{-1}$. Compared with (I) , this would mean

$$\text{(CL)} \qquad \text{(P)} \ll \frac{Q^2+N}{\ln Q}\, Z$$

A discussion of this conjecture is the object of my talk. Before giving some results I will describe an example which shows how important an inequality of type (CL) may be .

Let $\eta(p)$ be the least positive quadratic non-residue mod p . A famous conjecture of Vinogradov is

$$(CV) \qquad \eta(p) \ll_{\varepsilon} p^{\varepsilon} \qquad \text{for every } \varepsilon > 0 .$$

(The best result known at the present time is $\varepsilon > \frac{1}{4} e^{-\frac{1}{2}}$).

One of the first and still most interesting applications of the large sieve is the following due to Linnik.

Let $$N(x,\varepsilon) = \sum_{\substack{p \le x \\ \eta(p) > x^{\varepsilon}}} 1 .$$

Then

$$(Li) \qquad N(x,\varepsilon) \le c(\varepsilon) \qquad (\ c(\varepsilon) \text{ is a constant which depends on } \varepsilon \text{ only}) .$$

(Li) is proved with the help of the following inequality.

Write $$\eta = x^{\varepsilon^2} , \qquad \Psi = \sum_{\substack{n \le Q^2 \\ p|n \Rightarrow p \le \eta}} 1$$

then
$$N(x,\varepsilon) \le 4\Psi^{-2} \sum_{p \le Q} p \sum_{b=1}^{p} (\Psi(p,b) - \frac{\Psi}{p})^2$$

($\Psi(p,b)$ is defined like $A(p,b)$). Using (I) and a lower estimation for Ψ , one gets (Li).

If (CL) or only

$$(P) = o(Q^2\Psi) \qquad (Q \to \infty) .$$

were true in this special case we would get

$$\sum_{\substack{p \le Q \\ \eta(p) > Q^{\varepsilon}}} 1 < 1 \quad \text{for} \quad Q \ge Q_0(\varepsilon) .$$

This is equivalent to (CL) .

Unfortunately, (CL) is not true in general. Elliott showed that for $Q = N^2$ - which indeed is the most interesting part of the Q-N region - one can find complex numbers a_n so that

$$(P) \asymp (R) \asymp Q^2 Z$$

($f \asymp g$ means, as usual,

$$c_1 g \leq f \leq c_2 g\ ) .$$

The numbers a_n are rather artificial. So one can hope that for simple a_n's , for example $a_n = 0$ or 1 , a bit of (CL) can be saved. Indeed, Erdős, and Renyi showed by probabilistic arguments that (CL) is true for "almost all" sequences a_n with $a_n = 0$ or 1 if we assume

$$Q \leq N^{\frac{1}{2}} .$$

(I will not give the exact formulation of their theorem. All questions mentioned in this talk will be discussed in detail in a forthcoming monograph of Halberstam and Richert on sieve methods).

As I am going to show now (CL) is almost fulfilled in the complementary part of the Q-N region.

THEOREM. Let $Q \geq 10$, $0 < \delta < 1$, $N \leq Q^{1+\delta}$.

Then we have, with an absolute constant C ,

$$\sum_{p \leq Q} \sum_{b=1}^{p-1} |S(\tfrac{b}{p})|^2 \leq \frac{C}{1-\delta} \; Q^2 \frac{\ln \ln Q}{\ln Q} \; Z .$$

It is easy to see that this is better than (I) if

$$Q \geq N^{\frac{1}{2}} (\ln\ N)^{C_1}$$

is assumed. It is perhaps possible to modify my method as to come near to the point $Q = N^{\frac{1}{2}}$, but I am sure one cannot reach it in this way. Nevertheless there are some applications to the theorem which make it worth while talking about it.

I will now give a short idea of the proof.

In all proofs to (I) one uses the simple fact that the distance between two different Farey fractions of order Q is bigger than $1/Q^2$. I use an upper estimation for the number of Farey fractions of order Q and prime denominator which lie in a small interval.

LEMMA. Let $Q \geq 10$, $0 < \delta \leq 1 - \dfrac{4 \ln \ln Q}{\ln Q}$,

$$\Delta = Q^{-1-\delta} \ , \ \alpha \text{ real} \ , \ I(\alpha) = [\ \alpha - \Delta,\ \alpha + \Delta],$$

$$P(\alpha) = \sum_{\substack{p \leq Q,\ (b,p)=1 \\ \frac{b}{p} \in I(\alpha)}} 1 \qquad .$$

Then we have

$$P(\alpha) \leq \frac{C}{1-\delta} \frac{Q^2 \ln \ln Q}{\ln Q} \Delta .$$

The theorem easily follows from the Lemma and a general large sieve inequality due to Davenport and Halberstam.

1. In the case

$$1 - \frac{4 \ln \ln Q}{\ln Q} < \delta < 1$$

the Theorem is not better than (I) , so there is nothing to prove.

2. For δ as supposed in the Lemma we use the following theorem.

Let $\| x \|$ denote the distance betwen x and the nearest integer, i.e.

$$\|x\| = \min (x-[x] , [x]+ 1 - x) .$$

Let $x_1, \ldots, x_R$ be any real numbers for which

$$\|x_r - x_s\| \geq \eta \quad (\text{if } r \neq s , \quad 0 < \eta \leq \tfrac{1}{2})$$

holds. Then we have

$$\text{(DH)} \qquad \sum_{r=1}^{R} |S(x_r)|^2 > 2 \max(N, \eta^{-1}) Z .$$

(In the original paper (DH) is proved with 2.2 instead of 2 , in the monograph mentioned above it will appear in this form).

Because of our Lemma the set $\{ \frac{b}{p} ; P \leq Q ; b = 1 , \ldots, p-1 \}$ can be split up into at most

$$\frac{C}{1-\delta} \frac{Q^2 \ln \ln Q}{\ln Q} \Delta$$

classes K_i , so that for every i

$$\left\| \frac{b_1}{p_1} - \frac{b_2}{p_2} \right\| \geq \Delta \quad \text{if} \quad \frac{b_1}{p_1} \neq \frac{b_2}{p_2} \text{ and } \frac{b_1}{p_1} , \frac{b_2}{p_2} \in K_i$$

holds.

For fixed i , (DH) gives

$$\sum_{\frac{b}{p} \in K_i} |S(\tfrac{b}{p})|^2 \leq 2 \Delta^{-1} Z .$$

Summation over i implies the Theorem.

Because of the short time I will only give a rough idea of the proof to the Lemma, which is the most important part of the Theorem.

One first shows that

$$\frac{b}{p} \in I(\alpha) \quad , \quad p \in J$$

(J is a certain not too long interval) implies $p \equiv k \mod n$ where k and n are certain numbers which depend on the Farey arc on which α lies. Now the Brun-Titchmarsh Theorem and some calculation lead to the Lemma.

I will now give some applications to the Theorem which are - roughly spoken - average value theorems like Erdös's Theorem about the least positive quadratic non-residue or Burgess-Elliott's Theorem on the average of the least primitive root mod p .

Let us consider a sequence $\mathcal{A}$ of different positive integers with the following properties.

(i) $$C_1 \frac{N}{(\ln N)^{\gamma}} \le A(N) = \sum_{\substack{n \le N \\ n \in \mathcal{A}}} 1 \le C_2 \frac{N}{(\ln N)^{\gamma}}$$

(γ_1, C_1 , C_2 , ... are constants which depend on $\mathcal{A}$ only).

Let

$$m(p,b) = \min_{\substack{n \in \mathcal{A} \\ n \equiv b \mod p}} n \qquad (b = 1,\dots,p-1)$$

and assume

(ii) $$m(p,b) \le C_{3p}\, C_4 \, .$$

Then, with a modified form of the Theorem, one can prove

(M) $$\sum_{p \le Q} \sum_{b=1}^{p-1} m^{\alpha}(p,b) \le C_5(\alpha, \mathcal{A})\, \pi(Q)\, Q(Q(\ln Q)^{\gamma} \ln_3 Q)^{\alpha}$$

$$\text{if } 0 < \alpha < \min\left(1 , \frac{1}{C_{4-1}}\right) .$$

Except the factor $\ln_3^{\alpha} Q$ this is what one would expect.

In some special cases it is possible to show a bit more.

I. - Let $S(p,b)$ be the least squarefree number $\equiv b \mod p$,

$$S(p,b) = \min_{\substack{n \equiv b \mod p \\ \mu^2(n) = 1}} n \quad .$$

Prachar showed

$$S(p,b) << p^{\frac{3}{2}+\varepsilon} \qquad \text{for every} \quad \varepsilon > 0 \quad ,$$

which implies (M) in this special case. Using some special properties of the squarefree numbers, one can show, for $0 < \alpha < 1$

$$(S) \qquad \sum_{p \le Q} \sum_{b=1}^{p-1} S^{\alpha}(p,b) = (C(\alpha) + o(1))\, \pi(Q)\, Q^{1+\alpha} .$$

II. - Let $q(p,b) = \min\limits_{p \equiv b \bmod q} p$.

Linnik's famous theorem says $q(p,b) \ll p^{L}$ for some fixed $L > 2$. Again one can show a bit more than (M) , namely

$$\sum_{p \le Q} \sum_{b=1}^{p-1} q^{\alpha}(p,b) \asymp \pi(Q)\, Q (Q \ln Q)^{\alpha} .$$

I hope I can prove an asymptotic formula such as (S) in this case too, but I am not sure whether I will succeed.

Questions at the end.

1. Estimate the corresponding sum

$$\sum_{n \le Q} \sum_{\substack{b=1 \\ (b,n)=1}}^{n} m^{\alpha}(n,b)$$

(Difficulties which arise).

2. The distribution function $(c > 0)$

$$F(Q,c) = \frac{1}{\pi(Q)\, Q} \sum_{\substack{p \le Q \;;\; b=1,\dots,q-1 \\ \frac{q(p,b)}{Q \ln Q} < c}} 1$$

Does this tend to a limit for $Q \to \infty$ and every c ? (The limit exists for $S(p,b)$).

3. The main problem is the region near $Q^2 = N$. Can you find conditions on the a_n's , so that

(CL) holds in a certain form ? Surely one must find a new type of proof for the large sieve because in all known methods no special properties of the a_n's are used.

Mathematisches Institut der Universität Marburg
Universitätsstraße 24 - Fernruf 693727
355 Marburg-Lahn (Allemagne)

Joseph FLOCH, Maître-Imprimeur à Mayenne - 8-9-1971 - nº 4178