DIETER WOLKE

Farey fractions with prime denominator and the large sieve


<http://www.numdam.org/item?id=MSMF_1971__25__183_0>
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 $a_n$ $(M<n^M+N)$ be any complex numbers. Write

$$S(a) = \sum_n a_n e(n a) \quad (e(\theta) = e^{2\pi i \theta})$$

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

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

We wish an upper bound for the sum

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

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

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

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

$$(I) \quad (R) \ll (Q^2 + N) Z$$

(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

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

\[
(CV) \quad \eta(p) \ll p^\varepsilon \quad \text{for every } \varepsilon > 0.
\]

(The best result known at the present time is \( \varepsilon > \frac{1}{14} e^{-\frac{1}{2}} \).)

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

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

Then

\[
(Li) \quad N(x, \varepsilon) \leq c(\varepsilon) \quad (c(\varepsilon) \text{ is a constant which depends on } \varepsilon \text{ only}).
\]

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

Write \( \eta = x^\varepsilon \), \( \psi = \sum_{\eta \leq Q^2} \frac{1}{n} \sum_{\nu | n = p \leq \eta} \)

then

\[
N(x, \varepsilon) \leq \psi^{1-2} \sum_{p \leq Q} \frac{1}{p} \sum_{b=1}^{P} (\psi(p,b) - \frac{1}{p})^2
\]

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

If (CL) or only

\[
(P) = o(Q^2 \psi) \quad (Q \to \infty).
\]

were true in this special case we would get

\[
\sum_{p \leq Q} 1 < 1 \quad \text{for } Q \geq Q(\varepsilon).
\]

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

\[
(P) \not\approx (R) \not\approx Q^2 \not\approx Z
\]
(f < c^g) means, as usual,
\[ c^g \leq f \leq c^g. \]

The numbers \( a^\alpha \) are rather artificial. So one can hope that for simple \( a^\alpha \)'s, for example \( a^\alpha = 0 \) or \( 1 \), a bit of (CL) can be saved. Indeed, Erdős, and Rényi showed by probabilistic arguments that (CL) is true for "almost all" sequences \( a^\alpha \) with \( a^\alpha = 0 \) or \( 1 \) if we assume
\[ Q \leq N^\frac{1}{5}. \]

(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 \( C \),
\[ \sum_{p \leq Q} \sum_{b=1}^{p-1} |S(b,p)|^2 \leq C \frac{Q^2 \ln \ln Q}{1-\delta} Z. \]

It is easy to see that this is better than (I) if
\[ Q \geq N^\frac{1}{3} (\ln N)^{C_1} \]

is assumed. It is perhaps possible to modify my method as to come near to the point \( Q = N^\frac{1}{3} \), 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 \( Q \geq 10, 0 < \delta \leq 1 - \frac{1}{2} \ln \ln Q \ln Q \),
\[ \Delta = Q^{-1-\delta}, \alpha \text{ real}, I(\alpha) = [\alpha-\Delta, \alpha+\Delta], \]
\[ P(\alpha) = \sum_{\substack{p \leq Q, (b,p)=1 \\ \ b \in I(\alpha)}} 1. \]
Then we have
\[ p(a) \leq \frac{C}{1-\delta} \frac{Q^2 \ln \ln Q}{\ln Q} \Delta. \]

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

1. In the case
\[ 1 - \frac{\ln \ln Q}{\ln Q} < \delta < 1 \]
the Theorem is not better than (I), so there is nothing to prove.

2. For \( \delta \) as supposed in the Lemma we use the following theorem.

Let \( \| x \| \) denote the distance between \( x \) and the nearest integer, i.e.
\[ \| x \| = \min (x-[x], [x]+1-x). \]

Let \( x_1, \ldots, x_p \) be any real numbers for which
\[ \| x_r - x_s \| \geq n \quad (\text{if } r \neq s, \ 0 < n \leq \frac{1}{2}) \]
holds. Then we have
\[ \sum_{r=1}^{p} \| S(x_r) \|^2 \geq 2 \max (N, n^{-1}) Z. \]

(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 \( i \)
\[ \left\| \frac{b_1}{p_1} - \frac{b_2}{p_2} \right\| \geq \Delta \quad \text{if } \frac{b_1}{p_1} \neq \frac{b_2}{p_2} \quad \text{and} \quad \frac{b_1}{p_1}, \frac{b_2}{p_2} \in K_i \]
holds.

For fixed \( i \), (DH) gives
\[ \sum_{\frac{b}{p} \in K_i} |S(\frac{b}{p})|^2 \leq 2 \Delta^{-1} Z. \]

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
\[ \frac{b}{p} \in I(a) \ , \ p \in J \]
(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 \( a \) 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 Erdős'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 \( G \) of different positive integers with the following properties.

(i) \[ C_1 \frac{N}{(\ln N)^\gamma} \leq A(N) = \frac{1}{n^N} \sum_{n \leq N, n \in G} 1 \leq C_2 \frac{N}{(\ln N)^\gamma} \]

(\( \gamma_1, C_1, C_2, \ldots \) are constants which depend on \( G \) only).

Let
\[ m(p, b) = \min_{n \equiv b \mod p} n \quad (b = 1, \ldots, p-1) \]
and assume

(ii) \[ m(p, b) \leq C_3 p C_4. \]

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

(M) \[ \sum_{p \leq Q} \sum_{b=1}^{p-1} m^a(p, b) \leq C_5(a, G) \pi(Q) Q(\ln Q)^\gamma \ln_3 Q)^a \]

if \( 0 < a < \min (1, \frac{1}{C_4+1}) \).

Except the factor \( \ln_3 Q \) 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 \( \equiv b \mod p \),
\[ S(p, b) = \min_{n \equiv b \mod p} n \quad \mu^2(n) = 1 \]
Prachar showed
\[ S(p, b) << \frac{3}{p^2} + \epsilon \]
for every \( \epsilon > 0 \),
which implies (M) in this special case. Using some special properties of the squarefree numbers, one can show, for $0 < a < 1$

\[(S) \sum_{p \leq Q} \sum_{b=1}^{p-1} S^a(p,b) = (C(a) + O(1)) \pi(Q) Q^{1+a} \cdot\]

II. - Let $q(p,b) = \min_{p \equiv b \mod q} p$.

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

\[\sum_{p \leq Q} \sum_{b=1}^{p-1} q^a(p,b) \ll \pi(Q) Q(q \ln Q)^a.\]

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
\[\sum_{n \leq Q} \sum_{b=1}^{n} m^a(n,b)\]
\((b,n)=1\)

(Difficulties which arise).

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

\[F(Q,c) = \frac{1}{\pi(Q)} \sum_{p \leq Q, b=1, \ldots, q-1} \frac{1}{Q \ln Q} < c\]

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.