数理解析研究所講究録
第743巻 1991年 51-58

A brief account of the large sieve

By Y. Motohashi

A definition of a sieve problem :

$\mathcal{A}$: a finite set of integers

$\mathcal{P}$: a set of primes

$\omega(p)$: a set of residue classes (mod p) for each $p \in \mathcal{P}$

Problem

Estimate $S(\mathcal{A}, \mathcal{P}, \omega) = |\{\mathcal{A} \ni a \, ; \, a \pmod p \notin \omega(p) \text{ for } \forall p \in \mathcal{P}\}|$

When $|\omega(p)\}$ are not too large, the problem can be handled with the combinatorial sieve method, an account of which can be found in my Tata lecture note. But, if we allow $|\omega(p)|$ become indefinitely large as p's then the problem becomes quite diffeunt, and is dealt with the large sieve method which was originally invented by Ju. V. Linnik (Dokl. Akad. Nauk SSSR 30(1941)). This method was improved by many prominent people in analytic number thory ; the most notable is due to E. Bombieri (Mathematika 12(1965)). His argument was later refined by

A. Selberg, H.L. Montgomery, R.C. Vaughan, P.X. Gallagher and others.

Here we shall follow Montgomery's account of the method (Bull. A.M.S. 84 (1978)) with our observation on the relation between the large sieve and Selberg's Λ^2-sieve (Chap. 1 of my Tata lecture note.)

A formulation of the (large sieve) problem (Davenport-Halberstam)

$\{a_n\}$: arbitrary complex numbers

$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha) \qquad (e(*) = e^{2\pi i *})$$

$\{\alpha_j\}$ $(j=1, \cdots, R)$: δ-well-spaced points, i.e. for $j \neq j'$

$$|\alpha_j - \alpha_{j'}| \pmod 1 \geq \delta > 0.$$

Then, find the best possible Δ such that

$$\sum_{r=1}^{R} |S(\alpha_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |a_n|^2.$$

Lemma 1 (Selberg's inequality)

H : a unitary space with the scalar product $(\ ,\ )$.

$H \ni \varphi_1, \varphi_2, \cdots, \varphi_R, f$: arbitrary vectors

Then we have

$$\sum_{i=1}^{R} |(f, \varphi_i)|^2 \left\{ \sum_{j=1}^{R} |(\varphi_i, \varphi_j)| \right\}^{-1} \leq \|f\|^2$$

Remark

If $\{\varphi_j\}$ are orthonormal, then this is the Bessel inequality.

A simple specialization in Lemma 1 yields

Theorem 1 (Bombieri)

$$\Delta \leq N + 2\delta^{-1}.$$

This is sufficiently sharp for most applications in number theory. Yet, we may drop the coefficient 2 of $2\delta^{-1}$. For this sake we need

Lemma 2 (Montgomery - Vaughan)

Let $\lambda_1 < \lambda_2 < \cdots < \lambda_R$ be such that $\lambda_{r+1} - \lambda_r \geq \delta$ $(1 \leq r < R)$.

Then for any complex $\{w_r\}$ we have

$$\left| \sum_{r \neq s} \frac{w_r \bar{w}_s}{\lambda_r - \lambda_s} \right| \leq \pi \delta^{-1} \sum_r |w_r|^2$$

Remark

This is a generalization of Hilbert's inequality.

Theorem 2 (Montgomery - Vaughan)

$$\Delta \leq N + \delta^{-1}$$

This is very sharp. In fact, it is known that

Theorem 3 (A. Selberg)

The optimal Δ is equal to $N - 1 + \delta^{-1}$.

Selberg's proof of this fact is not elementary, but P. Cohen showed that

it is a simple consequence of Theorem 2.

We may refine Lemma 2 as follows :

Lemma 3 (Montgomery - Vaughan)

Under the same condition as in Lemma 2 we suppose further that $|\lambda_r - \lambda_s| \geq \delta_r$ $(s \neq r)$. Then

$$\left| \sum_{r \neq s} \frac{w_r \overline{w_s}}{\lambda_r - \lambda_s} \right| \leq \frac{3}{2} \pi \sum_r |w_r|^2 \delta_r^{-1}.$$

This implies

Theorem 4 (Montgomery - Vaughan)

$$\sum_r |S(\alpha_r)|^2 \left(N + \frac{3}{2} \delta_r^{-1}\right)^{-1} \leq \sum_n |a_n|^2 .$$

Namely we may take into account the irregularity of the distribution of the points $\{\alpha_r\}$. Later we shall see that this refinement has an important consequence in the theory of primes.

Next we turn to our original problem, i.e. the sieve problem. By appealing to Theorem 3, or rather its dual, we shall show

Theorem 5 (The large sieve)

If $\mathcal{A} \subseteq (M, M+N]$, then we have

$$S(\mathcal{A},P,\omega) \le (N-1+Q^2)\Big\{\sum_{q\in\mathcal{Q}}\prod_{p\mid q}\frac{|\omega(p)|}{p-|\omega(p)|}\Big\}^{-1}.$$

where

$$\mathcal{Q}=\Big\{q\le Q\,;\, q\mid\prod_{p\in P}p\Big\}$$

Proof We follow our argument (Proc. Japan Acad., 53 (1977), p.122-124.)

We first extend the definition of ω to composite integers. So, let $d\in\mathcal{Q}$ be such that $d=p_1\cdots p_r$. Then $\omega(d)$ be the set of residues (mod d) obtained from $\omega(p_i)$ $1\le i\le r$ by the way of Chinese remainder theorem. $n\in\omega(d)$ means $n\pmod d\in\omega(d)$, so $n\in\omega(1)$ for any n.

By the fundamental idea (the Λ^2-sieve) of A. Selberg we have

$$S(\mathcal{A},P,\omega)\le\sum_{M<n\le M+N}\Big|\sum_{n\in\omega(d)}\lambda_d\Big|^2$$

for any complex numbers λ_d defined on $\mathcal{Q}$ whose values may be arbitrary, except for the condition

$$\lambda_1=1.$$

The characteristic function of the set of integers n such that $n\in\omega(d)$ is given by

$$\frac{1}{d}\sum_{h=1}^{d}\sum_{l\in\omega(d)}\exp\Big(2\pi i\frac{h}{d}(n-l)\Big)=\frac{1}{d}\sum_{q\mid d}\sum_{\substack{r=1\\(q,r)=1}}^{q}\sum_{l\in\omega(d)}\exp\Big(2\pi i\frac{r}{q}(n-l)\Big)$$

$$=\frac{|\omega(d)|}{d}\sum_{q\mid d}\frac{1}{|\omega(q)|}\sum_{\substack{r=1\\(q,r)=1}}^{q}e\Big(\frac{r}{q}n\Big)\sum_{l\in\omega(q)}e\Big(-\frac{r}{q}l\Big).$$

Inserting this into the right side of the last inequality, we have

$$S(\mathcal{A},P,\omega) \le \sum_{M<n\le M+N} \Big| \sum_{q\in\mathcal{Q}} |\omega(q)|^{-1} \sum_{\substack{r=1\\(q,r)=1}}^{q} e\left(\frac{r}{q}n\right)\Big(\sum_{d\equiv 0 \,(\mathrm{mod}\, q)} \frac{\lambda_d}{d}|\omega(d)|\Big) \times \Big(\sum_{\ell\in\omega(d)} e\left(-\frac{r}{q}\ell\right)\Big)\Big|^2.$$

We write this as

$$S(\mathcal{A},P,\omega) \le \sum_{M<n\le M+N} \Big| \sum_{\frac{r}{q}} b\left(\frac{r}{q}\right) e\left(\frac{r}{q}n\right)\Big|^2,$$

where

$$b\left(\frac{r}{q}\right) = |\omega(q)|^{-1}\Big(\sum_{d\equiv 0\,(\mathrm{mod}\, q)} \frac{\lambda_d}{d}|\omega(d)|\Big)\Big(\sum_{\ell\in\omega(d)} e\left(-\frac{r}{q}\ell\right)\Big)$$

for those $q\in\mathcal{Q}$.

Here $\left\{\frac{r}{q}\right\}$ are Q^{-2}-well-distributed. Hence by the <u>dualized</u> form of Theorem 3 we get immediately

$$S(\mathcal{A},P,\omega) \le (N-1+Q^2)\sum_{\frac{r}{q}} |b\left(\frac{r}{q}\right)|^2$$

$$= (N-1+Q^2)\sum_{q\in\mathcal{Q}}\prod_{p\mid q}\left(p|\omega(p)|^{-1}-1\right)\Big|\sum_{d\equiv 0\,(\mathrm{mod}\, q)}\frac{\lambda_d}{d}|\omega(d)|\Big|^2.$$

Then we put $y_q = \sum_{d\equiv 0\,(\mathrm{mod}\, q)} \frac{\lambda_d}{d}|\omega(d)|$. We have

$$\sum_{q\in\mathcal{Q}} \mu(q) y_q = \lambda_1 = 1,$$

where μ is the Möbius function. And by Schwarz's inequality we get, for certain optimal y_q,

$$\Big\{ \sum_{q \in \mathcal{Q}} |y_q|^2 \prod_{p \mid q} (p |\omega(p)|^{-1} - 1) \Big\} \Big\{ \sum_{q \in \mathcal{Q}} \prod_{p \mid q} \frac{|\omega(p)|}{p - |\omega(p)|} \Big\} = 1 .$$

From this the theorem follows immediately.

Remark

It seems that our proof of Theorem #5 is the simplest among several known proofs. Moreover, our proof can be extended to include into discussion the larger sieves of P.X. Gallagher and A. Selberg (see our Tata notes).

A consequence of Theorem #5 is the Brun-Titchmarsh theorem: Denoting by $\pi(x; k, \ell)$ the number of primes less than x which are $\equiv \ell \pmod k$ we have

$$\pi(x; k, \ell) \leq \frac{2x}{\varphi(k) \log \frac{x}{k}} \left(1 + O\left(\frac{\log\log \frac{x}{k}}{\log \frac{x}{k}}\right)\right)$$

as x/k tends to infinity, where φ is the Euler function. However, Montgomery and Vaughan showed that their Theorem 4 yields

$$\pi(x; k, \ell) \leq \frac{2x}{\varphi(k) \log \frac{x}{k}} .$$

Hence it is important, in number theoretical applications, to take into account the irregularity of the distribution of the points $\{\alpha_r\}$. Further we should note that if the constant 2 in the last inequality is ever replaced by a smaller one then an extremely deep consequence on the zeros of Dirichlet L-functions would follow (see our paper: Proc.

Japan Acad., 55(1979), 190-192.)

Another important application of Theorem 5, in a quite different context, can be found in a recent book of J.P. Serre on Mordell conjecture.

However, the most important application of the large sieve method is to the problem of estimating in mean the error-term in the prime number theorem for arithmetic progressions. Thus, denoting by $E(x;k,l)$ the quantity $\pi(x;k,l) - \frac{1}{\varphi(k)} \mathrm{li}\, x$, Bombieri (1965) proved, as a culmination of a series of deep researches due to many people (started by A. Rényi (1947)),

$$\sum_{k \leq x^{\frac{1}{2}} \log^{-B} x} \max_{l \,(\mathrm{mod}\, k)} |E(x;k,l)| \ll x \log^{-A} x ,$$

where $B = B(A)$, and A is arbitrary. It is now known that this mean prime number theorem of Bombieri is a rather simple consequence of Theorem 1.

Remark

The last result is a consequence of the so-called extended Riemann hypothesis; namely the large sieve method allows us to avoid the Riemann hypothesis in a certain extent. Also, we should note that A.I. Vinogradov proved the last result independently from Bombieri; his argument is an extension of Rényi's and dependent on another deep method of Linnik (the dispersion method).