Math 571 Chapter 5 The Large Sieve

Robert C. Vaughan

February 20, 2025

- The key extra ingredient which gave rise to the B-VMVT was the large sieve.

- The key extra ingredient which gave rise to the B-VMVT was the large sieve.
- This had been invented by Linnik [1941,1942] in work on the least quadratic non–residue $n_2(p)$ modulo a prime p.

- The key extra ingredient which gave rise to the B-VMVT was the large sieve.
- This had been invented by Linnik [1941,1942] in work on the least quadratic non–residue $n_2(p)$ modulo a prime p.
- For those not familiar with the concept, given an odd prime p we say that $n \not\equiv 0 \pmod p$ is a quadratic residue, QR, modulo p when $x^2 \equiv n \pmod p$ is soluble and a quadratic non-residue, QNR, when it is insoluble. I usually leave the 0 residue class unclassified, although some might call it a QR.

- The key extra ingredient which gave rise to the B-VMVT was the large sieve.
- This had been invented by Linnik [1941,1942] in work on the least quadratic non–residue $n_2(p)$ modulo a prime p.
- For those not familiar with the concept, given an odd prime p we say that $n \not\equiv 0 \pmod{p}$ is a quadratic residue, QR, modulo p when $x^2 \equiv n \pmod{p}$ is soluble and a quadratic non-residue, QNR, when it is insoluble. I usually leave the 0 residue class unclassified, although some might call it a QR.
- It is not hard to show that the number of QR equals the number of QNR equals $\frac{p-1}{2}$.

- The key extra ingredient which gave rise to the B-VMVT was the large sieve.
- This had been invented by Linnik [1941,1942] in work on the least quadratic non–residue $n_2(p)$ modulo a prime p.
- For those not familiar with the concept, given an odd prime p we say that $n \not\equiv 0 \pmod{p}$ is a quadratic residue, QR, modulo p when $x^2 \equiv n \pmod{p}$ is soluble and a quadratic non-residue, QNR, when it is insoluble. I usually leave the 0 residue class unclassified, although some might call it a QR.
- It is not hard to show that the number of QR equals the number of QNR equals $\frac{p-1}{2}$.
- The Legendre symbol is defined by

$$\left(\frac{n}{p}\right)_L = \begin{cases} 1 & n \text{ QR}, \\ -1 & n \text{ QNR}, \\ 0 & n \equiv 0 \pmod{p}. \end{cases}$$

- The key extra ingredient which gave rise to the B-VMVT was the large sieve.
- This had been invented by Linnik [1941,1942] in work on the least quadratic non–residue $n_2(p)$ modulo a prime p.
- For those not familiar with the concept, given an odd prime p we say that $n \not\equiv 0 \pmod{p}$ is a quadratic residue, QR, modulo p when $x^2 \equiv n \pmod{p}$ is soluble and a quadratic non-residue, QNR, when it is insoluble. I usually leave the 0 residue class unclassified, although some might call it a QR.
- It is not hard to show that the number of QR equals the number of QNR equals $\frac{p-1}{2}$.
- The Legendre symbol is defined by

$$\left(\frac{n}{p}\right)_L = \begin{cases} 1 & n \text{ QR}, \\ -1 & n \text{ QNR}, \\ 0 & n \equiv 0 \pmod{p}. \end{cases}$$

- This is a character modulo p.

- Gauss had solved the big unsolved problem of the 18th century by showing that if p and q are odd primes, then

$$\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

- Gauss had solved the big unsolved problem of the 18th century by showing that if p and q are odd primes, then

$$\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

- Let $n_2(p)$ denote the least positive quadratic non-residue modulo p.

- Gauss had solved the big unsolved problem of the 18th century by showing that if p and q are odd primes, then

$$\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

- Let $n_2(p)$ denote the least positive quadratic non-residue modulo p.
- It is very easy to show that

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- Gauss had solved the big unsolved problem of the 18th century by showing that if p and q are odd primes, then

$$\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

- Let $n_2(p)$ denote the least positive quadratic non-residue modulo p.
- It is very easy to show that

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- Note that the Wikipedia article on quadratic residues is less than enlightening on this!

- I. M. Vinogradov, 1918, had conjectured that for any fixed $\varepsilon > 0$ we have

$$n_2(p) \ll_\varepsilon p^\varepsilon$$

and showed that

$$n_2(p) \ll p^{\frac{1}{2\sqrt{e}}} (\log p)^2.$$

- I. M. Vinogradov, 1918, had conjectured that for any fixed $\varepsilon > 0$ we have

$$n_2(p) \ll_\varepsilon p^\varepsilon$$

and showed that

$$n_2(p) \ll p^{\frac{1}{2\sqrt{e}}}(\log p)^2.$$

- I. M. Vinogradov, 1918, had conjectured that for any fixed $\varepsilon > 0$ we have

$$n_2(p) \ll_\varepsilon p^\varepsilon$$

and showed that

$$n_2(p) \ll p^{\frac{1}{2\sqrt{e}}}(\log p)^2.$$

- Burgess 1957 improved this to

$$n_2(p) \ll p^{\frac{1}{4\sqrt{e}}}(\log p)^2.$$

- I. M. Vinogradov, 1918, had conjectured that for any fixed $\varepsilon > 0$ we have

$$n_2(p) \ll_\varepsilon p^\varepsilon$$

and showed that

$$n_2(p) \ll p^{\frac{1}{2\sqrt{e}}}(\log p)^2.$$

- Burgess 1957 improved this to

$$n_2(p) \ll p^{\frac{1}{4\sqrt{e}}}(\log p)^2.$$

- Ankeny 1951 showed that on GRH

$$n_2(p) \ll (\log p)^2.$$

- Linnik was able to prove a number of theorems about the frequency with which $n_2(p)$ gets unusually large.

- Linnik was able to prove a number of theorems about the frequency with which $n_2(p)$ gets unusually large.
- Perhaps the most striking of these results says that given any fixed $\delta > 0$, if $E(X)$ is the number of primes $p \le X$ such that $n_2(p) > p^\delta$, then

$$E(X) \ll_\delta \log\log X.$$

- Linnik was able to prove a number of theorems about the frequency with which $n_2(p)$ gets unusually large.
- Perhaps the most striking of these results says that given any fixed $\delta > 0$, if $E(X)$ is the number of primes $p \le X$ such that $n_2(p) > p^\delta$, then

$$E(X) \ll_\delta \log\log X.$$

- So far in exploring sieves we have applied a sieve in which we remove one (primes in an a.p., or the refined version of the twin prime conjecture), or two residue classes (Goldbach and original twin primes) or k, with k fixed (the prime k-tuple conjecture).

- Linnik was able to prove a number of theorems about the frequency with which $n_2(p)$ gets unusually large.
- Perhaps the most striking of these results says that given any fixed $\delta > 0$, if $E(X)$ is the number of primes $p \le X$ such that $n_2(p) > p^\delta$, then

$$E(X) \ll_\delta \log\log X.$$

- So far in exploring sieves we have applied a sieve in which we remove one (primes in an a.p., or the refined version of the twin prime conjecture), or two residue classes (Goldbach and original twin primes) or k, with k fixed (the prime k-tuple conjecture).
- Now we want to remove a large number of residue classes, $(p-1)/2$, for each prime p!

- Consider a set $\mathcal{A} = \{a_n : M + 1 \le n \le M + N\}$ of complex numbers a_n with the property that for each prime p the support $\mathcal{A}$ of a_n lies in $h(p) = p - \rho(p)$ residue classes modulo p, so that just as in the Selberg sieve we can suppose that $\rho(p)$ residue classes have been removed modulo p.

- Consider a set $\mathcal{A} = \{a_n : M+1 \le n \le M+N\}$ of complex numbers a_n with the property that for each prime p the support $\mathcal{A}$ of a_n lies in $h(p) = p - \rho(p)$ residue classes modulo p, so that just as in the Selberg sieve we can suppose that $\rho(p)$ residue classes have been removed modulo p.
- We may certainly suppose that $h(p) \ge 1$ always, since if there is a prime with $h(p) = p$, then we will have removed everything.

- Consider a set $\mathcal{A} = \{a_n : M+1 \le n \le M+N\}$ of complex numbers a_n with the property that for each prime p the support $\mathcal{A}$ of a_n lies in $h(p) = p - \rho(p)$ residue classes modulo p, so that just as in the Selberg sieve we can suppose that $\rho(p)$ residue classes have been removed modulo p.
- We may certainly suppose that $h(p) \ge 1$ always, since if there is a prime with $h(p) = p$, then we will have removed everything.
- We might think of the a_n as being the characteristic function of a set which has had $\rho(p)$ residue classes removed for each p.

- Consider a set $\mathcal{A} = \{a_n : M+1 \le n \le M+N\}$ of complex numbers a_n with the property that for each prime p the support $\mathcal{A}$ of a_n lies in $h(p) = p - \rho(p)$ residue classes modulo p, so that just as in the Selberg sieve we can suppose that $\rho(p)$ residue classes have been removed modulo p.
- We may certainly suppose that $h(p) \ge 1$ always, since if there is a prime with $h(p) = p$, then we will have removed everything.
- We might think of the a_n as being the characteristic function of a set which has had $\rho(p)$ residue classes removed for each p.
- Let

$$Z(q,h) = \sum_{\substack{n=M+1 \\ n \equiv h \pmod q}}^{M+N} a_n$$

and $Z = Z(0,1)$.

- Let

$$Z(q,h) = \sum_{\substack{m=M+1 \\ m\equiv h \pmod q}}^{M+N} a_n$$

and $Z = Z(0,1)$.

- Let

$$Z(q,h) = \sum_{\substack{m=M+1 \\ m\equiv h \pmod q}}^{M+N} a_n$$

and $Z = Z(0,1)$.

- We might hope that for each prime p the support of a_n is fairly uniformly distributed into the $h(p)$ residue classes.

- Let
$$Z(q,h) = \sum_{\substack{m=M+1 \\ m\equiv h \pmod q}}^{M+N} a_n$$
and $Z = Z(0,1)$.
- We might hope that for each prime p the support of a_n is fairly uniformly distributed into the $h(p)$ residue classes.
- Let $\mathcal{R}(p)$ be the set of $h(p)$ residue classes modulo p which contain the support of the a_n and consider the "variance"
$$V(p) = \sum_{r\in\mathcal{R}(p)} \left| Z(p,r) - \frac{Z}{h(p)} \right|^2 .$$

- Let

$$Z(q,h)=\sum_{\substack{m=M+1\\ m\equiv h \pmod q}}^{M+N} a_n$$

and $Z = Z(0,1)$.

- We might hope that for each prime p the support of a_n is fairly uniformly distributed into the $h(p)$ residue classes.
- Let $\mathcal{R}(p)$ be the set of $h(p)$ residue classes modulo p which contain the support of the a_n and consider the "variance"

$$V(p)=\sum_{r\in\mathcal{R}(p)}\left|Z(p,r)-\frac{Z}{h(p)}\right|^2.$$

- Let

$$S(\alpha)=\sum_{n=M+1}^{M+N} a_n e(n\alpha).$$

- Let

$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha).$$

- Let
$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha).$$
- The additive characters $e(an/q)$ modulo q satisfy the orthogonality relationship
$$\sum_{a=1}^{q} e(am/q)e(-an/q) = \begin{cases} q & m \equiv n \pmod q, \\ 0 & m \not\equiv n \pmod q. \end{cases}$$

- Let
$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha).$$
- The additive characters $e(an/q)$ modulo q satisfy the orthogonality relationship
$$\sum_{a=1}^{q} e(am/q)e(-an/q) = \begin{cases} q & m \equiv n \pmod q, \\ 0 & m \not\equiv n \pmod q. \end{cases}$$
- Thus
$$\sum_{a=1}^{q} |S(a/q)|^2 = \sum_{m=M+1}^{M+N} \sum_{\substack{n=M+1 \\ n \equiv m \pmod q}}^{M+N} q a_m \overline{a}_n$$
$$= q \sum_{a=1}^{q} Z(q,a)\overline{Z}(q,a) = q \sum_{a=1}^{q} |Z(q,a)|^2$$

- Let
$$S(\alpha)=\sum_{n=M+1}^{M+N} a_n e(n\alpha).$$
- The additive characters $e(an/q)$ modulo q satisfy the orthogonality relationship
$$\sum_{a=1}^{q} e(am/q)e(-an/q)=\begin{cases} q & m\equiv n \pmod q,\\ 0 & m\not\equiv n \pmod q.\end{cases}$$
- Thus
$$\sum_{a=1}^{q}|S(a/q)|^2=\sum_{m=M+1}^{M+N}\sum_{\substack{n=M+1\\ n\equiv m \pmod q}}^{M+N} qa_m\overline{a}_n$$
$$=q\sum_{a=1}^{q} Z(q,a)\overline{Z}(q,a)=q\sum_{a=1}^{q}|Z(q,a)|^2$$
- For the time being consider the special case $q=p$.

- Since $Z(p,a) = 0$ unless $a \in \mathcal{R}(p)$ we have

$$\sum_{a=1}^{p} |S(a/p)|^2 = p \sum_{a \in \mathcal{R}(p)}^{p} |Z(p,a)|^2.$$

- Since $Z(p,a) = 0$ unless $a \in \mathcal{R}(p)$ we have

$$\sum_{a=1}^{p} |S(a/p)|^2 = p \sum_{a\in\mathcal{R}(p)}^{p} |Z(p,a)|^2.$$

- We defined

$$\begin{aligned}
&V(p)\\
&= \sum_{a\in\mathcal{R}(p)} \left| Z(p,a) - \frac{Z}{h(p)} \right|^2\\
&= \sum_{a\in\mathcal{R}(p)} \left(|Z(p,a)|^2 - 2\Re Z(p,a)\overline{Z}/h(p) + |Z|^2/h(p)^2 \right)\\
&= \sum_{a\in\mathcal{R}(p)} |Z(p,a)|^2 - p|Z|^2/h(p).
\end{aligned}$$

- Since $Z(p,a)=0$ unless $a\in\mathcal{R}(p)$ we have

$$\sum_{a=1}^{p}|S(a/p)|^2 = p\sum_{a\in\mathcal{R}(p)}^{p}|Z(p,a)|^2.$$

- We defined

$$\begin{aligned}
&V(p)\\
&=\sum_{a\in\mathcal{R}(p)}\left|Z(p,a)-\frac{Z}{h(p)}\right|^2\\
&=\sum_{a\in\mathcal{R}(p)}\left(|Z(p,a)|^2-2\Re Z(p,a)\overline{Z}/h(p)+|Z|^2/h(p)^2\right)\\
&=\sum_{a\in\mathcal{R}(p)}|Z(p,a)|^2-p|Z|^2/h(p).
\end{aligned}$$

- Thus $pV(p)+|Z|^2\dfrac{p-h(p)}{h(p)}=\displaystyle\sum_{a=1}^{p-1}|S(a/p)|^2.$

- Thus $pV(p) + |Z|^2 \frac{p - h(p)}{h(p)} = \sum_{a=1}^{p-1} |S(a/p)|^2.$

- Thus $pV(p) + |Z|^2 \dfrac{p - h(p)}{h(p)} = \displaystyle\sum_{a=1}^{p-1} |S(a/p)|^2.$
- We have $V(p) \geq 0$ so

- Thus $pV(p) + |Z|^2 \dfrac{p - h(p)}{h(p)} = \displaystyle\sum_{a=1}^{p-1} |S(a/p)|^2.$
- We have $V(p) \geq 0$ so
- summing the above over a set $\mathcal{P}$ of primes gives

$$|Z|^2 \sum_{p\in\mathcal{P}} \frac{p - h(p)}{h(p)} \leq \sum_{p\in\mathcal{P}} \sum_{a=1}^{p-1} |S(a/p)|^2.$$

- We have

$$|Z|^2 \sum_{p\in\mathcal{P}} \frac{p-h(p)}{h(p)} \le \sum_{p\in\mathcal{P}} \sum_{a=1}^{p-1} |S(a/p)|^2.$$

- We have

$$|Z|^2 \sum_{p\in\mathcal{P}} \frac{p-h(p)}{h(p)} \le \sum_{p\in\mathcal{P}} \sum_{a=1}^{p-1} |S(a/p)|^2.$$

- Suppose we can obtain an non-trivial upper bound for the right hand side, such as

$$\sum_{p\in\mathcal{P}} \sum_{a=1}^{p-1} |S(a/p)|^2 \le Y \sum_{n=M+1}^{M+N} |a_n|^2.$$

- We have
$$|Z|^2 \sum_{p\in\mathcal{P}} \frac{p-h(p)}{h(p)} \le \sum_{p\in\mathcal{P}} \sum_{a=1}^{p-1} |S(a/p)|^2.$$
- Suppose we can obtain an non-trivial upper bound for the right hand side, such as
$$\sum_{p\in\mathcal{P}} \sum_{a=1}^{p-1} |S(a/p)|^2 \le Y \sum_{n=M+1}^{M+N} |a_n|^2.$$
- We know from the Cauchy-Schwarz inequality that such bounds exist and indeed this sum could be written in terms of a Hermitian matrix, so Y could be taken to be its largest eigenvalue.

- We have
$$|Z|^2 \sum_{p\in\mathcal{P}} \frac{p-h(p)}{h(p)} \le \sum_{p\in\mathcal{P}} \sum_{a=1}^{p-1} |S(a/p)|^2.$$
- Suppose we can obtain an non-trivial upper bound for the right hand side, such as
$$\sum_{p\in\mathcal{P}} \sum_{a=1}^{p-1} |S(a/p)|^2 \le Y \sum_{n=M+1}^{M+N} |a_n|^2.$$
- We know from the Cauchy-Schwarz inequality that such bounds exist and indeed this sum could be written in terms of a Hermitian matrix, so Y could be taken to be its largest eigenvalue.
- Suppose further that a_n is the characteristic function of an interesting set. Then $Z = |Z| = \sum_{n=M+1}^{M+N} |a_n|^2$ so we have
$$|Z| \le Y / \sum_{p\in\mathcal{P}} \frac{p-h(p)}{h(p)}.$$

- Note that

$$\frac{p-h(p)}{h(p)} = \frac{\rho(p)}{p-\rho(p)} = \frac{f(p)}{1-f(p)} = g(p)$$

in the notation we used for the Selberg sieve. That looks familiar!

- Note that
$$\frac{p-h(p)}{h(p)} = \frac{\rho(p)}{p-\rho(p)} = \frac{f(p)}{1-f(p)} = g(p)$$
in the notation we used for the Selberg sieve. That looks familiar!
- We just proved that
$$|Z| \le \frac{Y}{\sum_{p\in\mathcal{P}} g(p)}.$$

- Note that

$$\frac{p-h(p)}{h(p)} = \frac{\rho(p)}{p-\rho(p)} = \frac{f(p)}{1-f(p)} = g(p)$$

in the notation we used for the Selberg sieve. That looks familiar!

- We just proved that

$$|Z| \le \frac{Y}{\sum_{p\in\mathcal{P}} g(p)}.$$

- Now there is no restraint on g and no remainder term R_d to worry about.

- Suppose that for each odd prime $p \le Q$ we remove the quadratic non-residues. Then the number of residue classes remaining is $h(p) = p - \frac{p-1}{2} = \frac{p+1}{2}$.

- Suppose that for each odd prime $p \le Q$ we remove the quadratic non-residues. Then the number of residue classes remaining is $h(p) = p - \frac{p-1}{2} = \frac{p+1}{2}$.
- Thus $g(p) = \frac{p-h(p)}{h(p)} = \frac{p-1}{p+1}$ and so by the prime number theorem
$$\sum_{p \le Q} g(p) \sim \frac{Q}{\log Q}.$$

- Suppose that for each odd prime $p \le Q$ we remove the quadratic non-residues. Then the number of residue classes remaining is $h(p) = p - \frac{p-1}{2} = \frac{p+1}{2}$.
- Thus $g(p) = \frac{p-h(p)}{h(p)} = \frac{p-1}{p+1}$ and so by the prime number theorem
$$\sum_{p \le Q} g(p) \sim \frac{Q}{\log Q}.$$
- We shall see that it is possible to take $Y \ll N + Q^2$, and then the optimal choice for Q is about $N^{1/2}$ and so $Z \ll N^{1/2} \log N$.

- Suppose that for each odd prime $p \le Q$ we remove the quadratic non-residues. Then the number of residue classes remaining is $h(p) = p - \frac{p-1}{2} = \frac{p+1}{2}$.
- Thus $g(p) = \frac{p-h(p)}{h(p)} = \frac{p-1}{p+1}$ and so by the prime number theorem
$$\sum_{p \le Q} g(p) \sim \frac{Q}{\log Q}.$$
- We shall see that it is possible to take $Y \ll N + Q^2$, and then the optimal choice for Q is about $N^{1/2}$ and so $Z \ll N^{1/2} \log N$.
- Amazingly this is close to best possible, since the perfect squares cannot be sieved out!

- Thus any non-trivial value for $Y(N,Q)$ for which

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2 \le Y(N,Q)\sum_{n=M+1}^{M+N}|a_n|^2$$

holds for any complex numbers a_n, has become known as the "The Large Sieve".

- Thus any non-trivial value for $Y(N,Q)$ for which

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2 \le Y(N,Q)\sum_{n=M+1}^{M+N}|a_n|^2$$

  holds for any complex numbers a_n, has become known as the "The Large Sieve".
- More generally one can ask for values of $Y_0(N,\delta)$ such that whenever $x_1,\ldots,x_R$ are R real numbers with $\|x_r - x_s\| \ge \delta$ whenever $r \ne s$ we have

$$\sum_{r=1}^{R}|S(x_r)|^2 \le Y_0(N,\delta)\sum_{n=M+1}^{M+N}|a_n|^2$$

  for any complex numbers a_n. Such inequalities are called "The Large Sieve" now also.

- Thus any non-trivial value for $Y(N,Q)$ for which

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2 \le Y(N,Q)\sum_{n=M+1}^{M+N}|a_n|^2$$

holds for any complex numbers a_n, has become known as the "The Large Sieve".

- More generally one can ask for values of $Y_0(N,\delta)$ such that whenever $x_1,\ldots,x_R$ are R real numbers with $\|x_r - x_s\| \ge \delta$ whenever $r \ne s$ we have

$$\sum_{r=1}^{R}|S(x_r)|^2 \le Y_0(N,\delta)\sum_{n=M+1}^{M+N}|a_n|^2$$

for any complex numbers a_n. Such inequalities are called "The Large Sieve" now also.

- By the way, $\|\alpha\|$ is the metric on $\mathbb{T}=\mathbb{R}/\mathbb{Z}$, that is

$$\|\alpha\| = \min_{n\in\mathbb{Z}}|\alpha - n|.$$

- The first modern version of the large sieve is Roth [1965],

$$Y(N,Q) \ll N + Q^2 \log Q.$$

- The first modern version of the large sieve is Roth [1965],

$$Y(N,Q) \ll N + Q^2 \log Q.$$

- Bombieri [1965] then obtained $Y(N,Q) = N + CQ^2$.

- The first modern version of the large sieve is Roth [1965],

$$Y(N,Q) \ll N + Q^2 \log Q.$$

- Bombieri [1965] then obtained $Y(N,Q) = N + CQ^2$.
- Gallagher [1967] gave a quite short proof that $Y(N,Q) = \pi N + Q^2$ is permissible.

- The first modern version of the large sieve is Roth [1965],

$$Y(N,Q) \ll N + Q^2 \log Q.$$

- Bombieri [1965] then obtained $Y(N,Q) = N + CQ^2$.
- Gallagher [1967] gave a quite short proof that $Y(N,Q) = \pi N + Q^2$ is permissible.
- Then there was a lot of work improving the constants.

- The first modern version of the large sieve is Roth [1965],

$$Y(N, Q) \ll N + Q^2 \log Q.$$

- Bombieri [1965] then obtained $Y(N, Q) = N + CQ^2$.
- Gallagher [1967] gave a quite short proof that $Y(N, Q) = \pi N + Q^2$ is permissible.
- Then there was a lot of work improving the constants.
- Finally Montgomery and Vaughan [1973,1974], with an added wrinkle by Paul Cohen [1977], and Selberg [1991, but known by him before 1977] gave the bound

$$Y_0(N, \delta) = N - 1 + \delta^{-1}.$$

- The first modern version of the large sieve is Roth [1965],

$$Y(N, Q) \ll N + Q^2 \log Q.$$

- Bombieri [1965] then obtained $Y(N, Q) = N + CQ^2$.
- Gallagher [1967] gave a quite short proof that $Y(N, Q) = \pi N + Q^2$ is permissible.
- Then there was a lot of work improving the constants.
- Finally Montgomery and Vaughan [1973,1974], with an added wrinkle by Paul Cohen [1977], and Selberg [1991, but known by him before 1977] gave the bound

$$Y_0(N, \delta) = N - 1 + \delta^{-1}.$$

- Bombieri and Davenport had shown [1968] that this is best possible even for $Y(N, Q)$.

- The first modern version of the large sieve is Roth [1965],

$$Y(N,Q) \ll N + Q^2 \log Q.$$

- Bombieri [1965] then obtained $Y(N,Q) = N + CQ^2$.
- Gallagher [1967] gave a quite short proof that $Y(N,Q) = \pi N + Q^2$ is permissible.
- Then there was a lot of work improving the constants.
- Finally Montgomery and Vaughan [1973,1974], with an added wrinkle by Paul Cohen [1977], and Selberg [1991, but known by him before 1977] gave the bound

$$Y_0(N,\delta) = N - 1 + \delta^{-1}.$$

- Bombieri and Davenport had shown [1968] that this is best possible even for $Y(N,Q)$.
- For an overall account of this see Montgomery [1978].

- Recall the bound, when $|a_n| = 1$ or 0,

$$|Z| \le \frac{Y(N,Q)}{\sum_{p\le Q} g(p)}$$

which we proved earlier.

- Recall the bound, when $|a_n| = 1$ or 0,

$$|Z| \le \frac{Y(N,Q)}{\sum_{p\le Q} g(p)}$$

which we proved earlier.

- The most general form of this (Montgomery [1968] and Montgomery & RCV [1973]) is

$$|Z| \le \frac{Y(N,Q)}{\sum_{q\le Q} \mu(q)^2 \prod_{p|q} \frac{g(p)}{p-g(p)}}.$$

- Recall the bound, when $|a_n| = 1$ or 0,

$$|Z| \le \frac{Y(N,Q)}{\sum_{p\le Q} g(p)}$$

which we proved earlier.

- The most general form of this (Montgomery [1968] and Montgomery & RCV [1973]) is

$$|Z| \le \frac{Y(N,Q)}{\sum_{q\le Q} \mu(q)^2 \prod_{p|q} \frac{g(p)}{p-g(p)}}.$$

- In some sense this is the dual of the Selberg sieve as applied to an interval.

- Recall the bound, when $|a_n| = 1$ or 0,
$$|Z| \le \frac{Y(N,Q)}{\sum_{p\le Q} g(p)}$$
which we proved earlier.
- The most general form of this (Montgomery [1968] and Montgomery & RCV [1973]) is
$$|Z| \le \frac{Y(N,Q)}{\sum_{q\le Q} \mu(q)^2 \prod_{p|q} \frac{g(p)}{p-g(p)}}.$$
- In some sense this is the dual of the Selberg sieve as applied to an interval.
- At this stage it is useful to observe that if $(a,q) = (b,r) = 1$, $q \le Q$, $r \le Q$ and $a/q \ne b/r$, then $Q^{-2} \le 1/(qr) \le |ar - bq|/(qr) = |a/q - b/r|$ and so one can take
$$Y(N,Q) = Y_0(N,Q^{-2}).$$

- In arithmetical applications it is important to have as precise a bound for $Y(N, Q)$ as possible, and we may return to this later.

- In arithmetical applications it is important to have as precise a bound for $Y(N, Q)$ as possible, and we may return to this later.
- Our immediate objective is to obtain bounds which are useful in “analytic” applications, and then the we don’t mind losing out by something relatively small, such as a power of a logarithm.

- In arithmetical applications it is important to have as precise a bound for $Y(N,Q)$ as possible, and we may return to this later.
- Our immediate objective is to obtain bounds which are useful in “analytic” applications, and then the we don't mind losing out by something relatively small, such as a power of a logarithm.
- One of the most fruitful ideas is that $\sum_{r=1}^{R} |S(x_r)|^2$

$$= \sum_{m=M+1}^{M+N} \sum_{n=M+1}^{M+N} a_m \overline{a}_n \sum_{r=1}^{R} e\big(x_r(m-n)\big) = \mathbf{a}\mathcal{H}\mathbf{a}^*$$

where $\mathcal{H} = \mathcal{M}\mathcal{M}^*$ and $\mathcal{M}$ is the $N \times R$ matrix $\mathcal{M} = \big(e(x_r m)\big)$.

- In arithmetical applications it is important to have as precise a bound for $Y(N,Q)$ as possible, and we may return to this later.
- Our immediate objective is to obtain bounds which are useful in "analytic" applications, and then the we don't mind losing out by something relatively small, such as a power of a logarithm.
- One of the most fruitful ideas is that $\sum_{r=1}^{R} |S(x_r)|^2$

$$= \sum_{m=M+1}^{M+N} \sum_{n=M+1}^{M+N} a_m \overline{a}_n \sum_{r=1}^{R} e\big(x_r(m-n)\big) = \mathbf{a}\mathcal{H}\mathbf{a}^*$$

  where $\mathcal{H} = \mathcal{M}\mathcal{M}^*$ and $\mathcal{M}$ is the $N \times R$ matrix $\mathcal{M} = \big(e(x_r m)\big)$.
- Thus $\mathcal{H}$ is a Hermitian matrix, and we are interested in its largest eigenvalue.

- To start with we state a lemma from linear algebra.

Lemma 1 (Duality Lemma)

Suppose that c_{nr}, $n = 1, \ldots, N, r = 1, \ldots, R$ *are complex numbers and* λ *is a real number such that for all complex numbers* z_r *we have*

$$\sum_{n=1}^{N} \left| \sum_{r=1}^{R} c_{nr} z_r \right|^2 \le \lambda \sum_{r=1}^{R} |z_r|^2.$$

Then

$$\sum_{r=1}^{R} \left| \sum_{n=1}^{N} c_{nr} w_n \right|^2 \le \lambda \sum_{n=1}^{N} |w_n|^2$$

holds for all complex numbers w_n*.*

- The proof uses the second basic principle of ANT!

Proof.

$$LHS = \sum_{m=1}^{N} w_m \sum_{r=1}^{R} c_{mr} \sum_{n=1}^{N} \overline{c}_{nr} \overline{w}_n = \sum_{m=1}^{N} w_m \sum_{r=1}^{R} c_{mr} \overline{z}_r$$

where $z_r = \sum_{n=1}^{N} c_{nr} w_n$. Hence, by Cauchy's inequality,

$$LHS^2 \le \left(\sum_{m=1}^{N} |w_m|^2 \right) \sum_{m=1}^{N} \left| \sum_{r=1}^{R} c_{mr} \overline{z}_r \right|^2 .$$

On hypothesis this is

$$\le \sum_{m=1}^{N} |w_m|^2 \lambda \sum_{r=1}^{R} |z_r|^2 = (LHS) \lambda \sum_{m=1}^{N} |w_m|^2 .$$

□

- By the way I. M. Vinogradov makes repeated use of the Duality Lemma in many special cases in his work on exponential sums, but always obtained directly *via* the Cauchy-Schwarz inequality and without, apparently, being aware that it was a special case of a general theorem!

- Below is a theorem which has a very simple proof.

Theorem 2 (Large Sieve Inequality 0)

Suppose that $0 < \delta \le \frac{1}{2}$ *and the* x_r, $r = 1\ldots, R$ *satisfy* $\|x_r - x_s\| \ge \delta$ *whenever* $r \ne s$. *Then*

$$\sum_{r=1}^{R} |S(x_r)|^2 \le Y_0(N,\delta) \sum_{n=M+1}^{M+N} |a_n|^2$$

holds with $Y_0(N,\delta) = N + \dfrac{1}{\delta}\log\dfrac{3}{\delta}$.

- Below is a theorem which has a very simple proof.

Theorem 2 (Large Sieve Inequality 0)

Suppose that $0 < \delta \le \frac{1}{2}$ *and the* x_r, $r = 1\ldots, R$ *satisfy* $\|x_r - x_s\| \ge \delta$ *whenever* $r \ne s$. *Then*

$$\sum_{r=1}^{R} |S(x_r)|^2 \le Y_0(N,\delta) \sum_{n=M+1}^{M+N} |a_n|^2$$

holds with $Y_0(N,\delta) = N + \frac{1}{\delta}\log\frac{3}{\delta}$.

- By the Duality Lemma it suffices to bound

$$\sum_{n=M+1}^{M+N} \left| \sum_{r=1}^{R} b_r e(nx_r) \right|^2 =$$

$$\sum_{r=1}^{R}\sum_{s=1}^{R} b_r \overline{b}_s \sum_{n=M+1}^{M+N} e\big(n(x_r - x_s)\big).$$

- We have $\displaystyle\sum_{r=1}^{R}\sum_{s=1}^{R} b_r\overline{b}_s \sum_{n=M+1}^{M+N} e\big(n(x_r - x_s)\big).$

- We have $\sum_{r=1}^{R}\sum_{s=1}^{R} b_r\overline{b}_s \sum_{n=M+1}^{M+N} e\big(n(x_r - x_s)\big)$.
- The diagonal terms $r = s$ contribute $N\sum_{r=1}^{R}|b_r|^2$ and when $r \neq s$ the sum over n gives

$$\frac{e\big((M+N+1)(x_r - x_s)\big) - e\big((M+1)(x_r - x_s)\big)}{e(x_r - x_s) - 1}$$
$$= e\big((M + 1/2 + N/2)(x_r - x_s)\big)\frac{\sin\left(\pi N(x_r - x_s)\right)}{\sin \pi(x_r - x_s)}$$

- We have $\sum_{r=1}^{R}\sum_{s=1}^{R} b_r\overline{b}_s \sum_{n=M+1}^{M+N} e\big(n(x_r - x_s)\big)$.
- The diagonal terms $r = s$ contribute $N\sum_{r=1}^{R}|b_r|^2$ and when $r \neq s$ the sum over n gives

$$\frac{e\big((M+N+1)(x_r-x_s)\big) - e\big((M+1)(x_r-x_s)\big)}{e(x_r-x_s)-1}$$

$$= e\big((M+1/2+N/2)(x_r-x_s)\big)\frac{\sin\left(\pi N(x_r-x_s)\right)}{\sin\pi(x_r-x_s)}$$

- Thus we obtain the upper bound.

$$N\sum_{r=1}^{R}|b_r|^2 + \sum_{r=1}^{R}\sum_{\substack{s=1\\ s\neq r}}^{R}\frac{|b_r b_s|}{|\sin\pi(x_r-x_s)|}.$$

- $$N\sum_{r=1}^{R}|b_r|^2+\sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R}\frac{|b_rb_s|}{|\sin\pi(x_r-x_s)|}.$$

- $$N\sum_{r=1}^R |b_r|^2 + \sum_{r=1}^R \sum_{\substack{s=1\\ s\neq r}}^R \frac{|b_r b_s|}{|\sin\pi(x_r-x_s)|}.$$
- Now $|b_r b_s| \le (|b_r|^2+|b_s|^2)/2$, and $|\sin \pi x| \ge 2\|x\|$.

- $$N\sum_{r=1}^{R}|b_r|^2+\sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R}\frac{|b_rb_s|}{|\sin\pi(x_r-x_s)|}.$$
- Now $|b_rb_s|\le(|b_r|^2+|b_s|^2)/2$, and $|\sin\pi x|\ge 2\|x\|$.
- Thus, by symmetry, we get the upper bound

$$\sum_{r=1}^{R}|b_r|^2\left(N+\sum_{\substack{s=1\\s\neq r}}^{R}\frac{1}{2\|x_r-x_s\|}\right).$$

- $$N\sum_{r=1}^{R}|b_r|^2+\sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R}\frac{|b_rb_s|}{|\sin\pi(x_r-x_s)|}.$$
- Now $|b_rb_s|\le(|b_r|^2+|b_s|^2)/2$, and $|\sin\pi x|\ge 2\|x\|$.
- Thus, by symmetry, we get the upper bound
$$\sum_{r=1}^{R}|b_r|^2\left(N+\sum_{\substack{s=1\\s\neq r}}^{R}\frac{1}{2\|x_r-x_s\|}\right).$$
- Note also that since we can suppose, by adding integers to each x_r, that
$$\min_r x_r+(R-1)\delta\le\max_r x_r \text{ and } \max_r x_r+\delta\le 1+\min_r x_r$$
and so
$$R\delta\le 1.$$

- We have the upper bound

$$\sum_{r=1}^{R} |b_r|^2 \left(N + \sum_{\substack{s=1 \\ s \neq r}}^{R} \frac{1}{2\|x_r - x_s\|} \right).$$

- We have the upper bound

$$\sum_{r=1}^{R} |b_r|^2 \left(N + \sum_{\substack{s=1 \\ s \neq r}}^{R} \frac{1}{2\|x_r - x_s\|} \right).$$

- Consider, given r, the sum over s. The function $\|x\|$ has period 1, so we can add integers to the x_s so that $x_r - \frac{1}{2} \le x_s \le x_r + \frac{1}{2}$. Since the x_r are δ apart, the two closest to x_r are no closer that δ, the next two closest are no closer than 2δ and so on. Thus

$$\sum_{\substack{s=1 \\ s \neq r}}^{R} \frac{1}{2\|x_r - x_s\|} \le 2 \sum_{k=1}^{R-1} \frac{1}{2k\delta}.$$

- We have the upper bound

$$\sum_{r=1}^{R}|b_r|^2\left(N+\sum_{\substack{s=1\\s\neq r}}^{R}\frac{1}{2\|x_r-x_s\|}\right).$$

- Consider, given r, the sum over s. The function $\|x\|$ has period 1, so we can add integers to the x_s so that $x_r-\frac{1}{2}\le x_s\le x_r+\frac{1}{2}$. Since the x_r are δ apart, the two closest to x_r are no closer that δ, the next two closest are no closer than 2δ and so on. Thus

$$\sum_{\substack{s=1\\s\neq r}}^{R}\frac{1}{2\|x_r-x_s\|}\le 2\sum_{k=1}^{R-1}\frac{1}{2k\delta}.$$

- We could use Euler's estimate, but crudely we have

$$\sum_{k=1}^{R-1}\frac{1}{k}\le 1+\int_1^R\frac{dx}{x}=1+\log R\le\log 3/\delta$$

This establishes the theorem.

- Let me give an overview of the various improvements.

- Let me give an overview of the various improvements.
- Go back to the start of the above proof. The non-diagonal terms in the formula we obtained can be rewritten as

$$\sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R} b_r\overline{b}_s \frac{e\big((M+N+1/2)(x_r-x_s)\big)}{2i\sin\big(\pi(x_r-x_s)\big)}$$

$$-\sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R} b_r\overline{b}_s \frac{e\big((M+1/2)(x_r-x_s)\big)}{2i\sin\big(\pi(x_r-x_s)\big)}.$$

- Let me give an overview of the various improvements.
- Go back to the start of the above proof. The non-diagonal terms in the formula we obtained can be rewritten as

$$\sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R} b_r\overline{b}_s \frac{e\big((M+N+1/2)(x_r-x_s)\big)}{2i\sin\left(\pi(x_r-x_s)\right)} - \sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R} b_r\overline{b}_s \frac{e\big((M+1/2)(x_r-x_s)\big)}{2i\sin\left(\pi(x_r-x_s)\right)}.$$

- If we write

$$c_r = e\big((M+N+1/2)x_r\big), \quad d_r = e\big((M+1/2)x_r\big),$$

then this can be written more succinctly as

$$\sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R} \frac{c_r\overline{c}_s}{2i\sin\left(\pi(x_r-x_s)\right)} - \sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R} \frac{d_r\overline{d}_s}{2i\sin\left(\pi(x_r-x_s)\right)}$$

- The sum
$$\sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R}\frac{c_r\overline{c}_s}{2i\sin\left(\pi(x_r-x_s)\right)}$$
looks like a generalization of that occurring in Hilbert's inequality
$$\left|\sum_{r=1}^{R}\sum_{\substack{s=1\\s\neq r}}^{R}\frac{a_r\overline{a}_s}{r-s}\right|<\pi\sum_{r=1}^{R}|a_r|^2.$$

- The sum
$$\sum_{r=1}^{R}\sum_{\substack{s=1\\ s\neq r}}^{R}\frac{c_r\overline{c}_s}{2i\sin\left(\pi(x_r-x_s)\right)}$$
looks like a generalization of that occurring in Hilbert's inequality
$$\left|\sum_{r=1}^{R}\sum_{\substack{s=1\\ s\neq r}}^{R}\frac{a_r\overline{a}_s}{r-s}\right|<\pi\sum_{r=1}^{R}|a_r|^2.$$
- There is a very slick proof of this using
$$\int_0^1\left(x-\frac{1}{2}\right)e(xh)dx=\begin{cases}\frac{1}{2\pi ih} & (h\in\mathbb{Z}\setminus\{0\})\\ 0 & (h=0).\end{cases}$$

- The sum
$$\sum_{r=1}^{R}\sum_{\substack{s=1\\ s\neq r}}^{R}\frac{c_r\overline{c}_s}{2i\sin\left(\pi(x_r-x_s)\right)}$$
looks like a generalization of that occurring in Hilbert's inequality
$$\left|\sum_{r=1}^{R}\sum_{\substack{s=1\\ s\neq r}}^{R}\frac{a_r\overline{a}_s}{r-s}\right| < \pi\sum_{r=1}^{R}|a_r|^2.$$
- There is a very slick proof of this using
$$\int_0^1\left(x-\frac{1}{2}\right)e(xh)dx=\begin{cases}\frac{1}{2\pi ih} & (h\in\mathbb{Z}\setminus\{0\})\\ 0 & (h=0).\end{cases}$$
- Then use $|x-1/2|<1/2$ and apply Parseval to
$$\sum_{r=1}^{R}\sum_{\substack{s=1\\ s\neq r}}^{R}\frac{a_r\overline{a}_s}{2\pi i(r-s)}=\int_0^1\left|\sum_{r=1}^{R}a_re(rx)\right|^2\left(x-\frac{1}{2}\right)dx.$$

- That proof does not generalise easily, but there is another proof due to Schur which does generalise with a little bit of work.

- That proof does not generalise easily, but there is another proof due to Schur which does generalise with a little bit of work.
- However there is an alternative method which has far reaching generalisations.

- That proof does not generalise easily, but there is another proof due to Schur which does generalise with a little bit of work.
- However there is an alternative method which has far reaching generalisations.
- The reason for the log in the previous result is because the characteristic function of $[M+1, M+N]$ has jump discontinuities.

- That proof does not generalise easily, but there is another proof due to Schur which does generalise with a little bit of work.
- However there is an alternative method which has far reaching generalisations.
- The reason for the log in the previous result is because the characteristic function of $[M+1, M+N]$ has jump discontinuities.
- The solution is to majorise it by a smooth upper bound.

- That proof does not generalise easily, but there is another proof due to Schur which does generalise with a little bit of work.
- However there is an alternative method which has far reaching generalisations.
- The reason for the log in the previous result is because the characteristic function of $[M+1, M+N]$ has jump discontinuities.
- The solution is to majorise it by a smooth upper bound.
- Thus we replace our dual form by

$$\sum_n f(n)\left|\sum_{r=1}^R b_r e(nx_r)\right|^2.$$

- That proof does not generalise easily, but there is another proof due to Schur which does generalise with a little bit of work.
- However there is an alternative method which has far reaching generalisations.
- The reason for the log in the previous result is because the characteristic function of $[M+1, M+N]$ has jump discontinuities.
- The solution is to majorise it by a smooth upper bound.
- Thus we replace our dual form by

$$\sum_n f(n) \left| \sum_{r=1}^{R} b_r e(nx_r) \right|^2 .$$

- Selberg found a very sophisticated way of doing this.

- A quite simple way to do this is to consider

$$f(x) = \max\left(0, 2\frac{N - |x - N_0 - M|}{N}\right),$$

where $N_0 = \lceil N/2 \rceil$.

- A quite simple way to do this is to consider
$$f(x) = \max\left(0, 2\frac{N - |x - N_0 - M|}{N}\right),$$
where $N_0 = \lceil N/2 \rceil$.
- When $x \in [M+1, M+N]$ we have $-N/2 \le 1 - N_0 \le |x - N_0 - M| \le N/2$. Multiplying out the sum over n becomes a Fejér kernel
$$\sum_n f(n) e\big(n(x_r - x_s)\big)$$
$$= \frac{2}{N} e\big((N_0 - M)(x_r - x_s)\big) \sum_{h=-N}^{N} (N - |h|) e\big(h(x_r - x_s)\big)$$
$$= \frac{2}{N} e\big((N_0 - M)(x_r - x_s)\big)\Big) \left| \sum_{j=0}^{N-1} e\big(j(x_r - x_s)\big) \right|^2$$
$$= 2e\big((N_0 - M)(x_r - x_s)\big)\Big) \frac{\sin^2 \pi N(x_r - x_s)}{N \sin^2 \pi(x_r - x_s)}.$$

- To amplify,

$$\left|\sum_{j=0}^{N-1} e(j\alpha)\right|^2 = \sum_k \sum_{\substack{j_1,j_2 \\ j_2-j_1=k}} e(k\alpha)$$

and given k the number of solutions of $j_2 - j_1 = k$ with $0 \le j_1, j_2 \le N-1$ is the number of j with $0 \le j \le N-1$ and $0 \le j+k \le N-1$, and one can check that this number is $\max(0, N-|k|)$.

- We have established that

$$\sum_n f(n)e\big(n(x_r - x_s)\big)$$

$$= 2e\big((N_0 - M)(x_r - x_s)\big)\frac{\sin^2 \pi N(x_r - x_s)}{N \sin^2 \pi(x_r - x_s)}.$$

- We have established that

$$\sum_n f(n)e\big(n(x_r - x_s)\big)$$

$$= 2e\big((N_0 - M)(x_r - x_s)\big)\frac{\sin^2 \pi N(x_r - x_s)}{N\sin^2 \pi(x_r - x_s)}.$$

- and this satisfies

$$\ll \min\left(N, \frac{1}{N\|x_r - x_s\|^2}\right)$$

- We have established that

$$\sum_n f(n)e\big(n(x_r - x_s)\big)$$

$$= 2e\big((N_0 - M)(x_r - x_s)\big)\frac{\sin^2 \pi N(x_r - x_s)}{N \sin^2 \pi(x_r - x_s)}.$$

- and this satisfies

$$\ll \min\left(N, \frac{1}{N\|x_r - x_s\|^2}\right)$$

- Thus we find that

$$\sum_{n=M+1}^{M+N}\left|\sum_{r=1}^{R} b_r e(nx_r)\right|^2$$

$$\ll \sum_{r=1}^{R}|b_r|^2\sum_{s=1}^{R}\min\left(N, \frac{1}{N\|x_r - x_s\|^2}\right).$$

- We have the bound $\displaystyle\sum_{r=1}^{R} |b_r|^2 \sum_{s=1}^{R} \min\left(N, \frac{1}{N\|x_r - x_s\|^2}\right)$.

- We have the bound $\sum_{r=1}^{R} |b_r|^2 \sum_{s=1}^{R} \min\left(N, \frac{1}{N\|x_r - x_s\|^2}\right)$.
- By the spacing hypothesis for the x_r it follows that this is

$$\ll \sum_{r=1}^{R} |b_r|^2 \left(N + \sum_{k=1}^{\infty} \min\left(N, \frac{1}{N(k\delta)^2}\right)\right).$$

- We have the bound $\displaystyle\sum_{r=1}^{R}|b_r|^2\sum_{s=1}^{R}\min\left(N,\frac{1}{N\|x_r-x_s\|^2}\right)$.
- By the spacing hypothesis for the x_r it follows that this is

$$\ll \sum_{r=1}^{R}|b_r|^2\left(N+\sum_{k=1}^{\infty}\min\left(N,\frac{1}{N(k\delta)^2}\right)\right).$$

- If $N\delta>1$, then the inner sum is $\ll N(1+N^{-2}\delta^{-2})\ll N$, and if $N\delta\le 1$, then it is

$$\ll \sum_{k\le N^{-1}\delta^{-1}} N+\sum_{k>N^{-1}\delta^{-1}}\frac{1}{N(k\delta)^2}\ll (N+\delta^{-1}).$$

- We have the bound $\sum_{r=1}^{R}|b_r|^2\sum_{s=1}^{R}\min\left(N,\frac{1}{N\|x_r-x_s\|^2}\right)$.
- By the spacing hypothesis for the x_r it follows that this is

$$\ll\sum_{r=1}^{R}|b_r|^2\left(N+\sum_{k=1}^{\infty}\min\left(N,\frac{1}{N(k\delta)^2}\right)\right).$$

- If $N\delta>1$, then the inner sum is $\ll N(1+N^{-2}\delta^{-2})\ll N$, and if $N\delta\le 1$, then it is

$$\ll\sum_{k\le N^{-1}\delta^{-1}}N+\sum_{k>N^{-1}\delta^{-1}}\frac{1}{N(k\delta)^2}\ll(N+\delta^{-1}).$$

- Thus in every case we have the bound $\ll N+\frac{1}{\delta}$.

- We have the bound $\sum_{r=1}^{R} |b_r|^2 \sum_{s=1}^{R} \min\left(N, \frac{1}{N\|x_r - x_s\|^2}\right)$.
- By the spacing hypothesis for the x_r it follows that this is

$$\ll \sum_{r=1}^{R} |b_r|^2 \left(N + \sum_{k=1}^{\infty} \min\left(N, \frac{1}{N(k\delta)^2}\right)\right).$$

- If $N\delta > 1$, then the inner sum is $\ll N(1 + N^{-2}\delta^{-2}) \ll N$, and if $N\delta \le 1$, then it is

$$\ll \sum_{k \le N^{-1}\delta^{-1}} N + \sum_{k > N^{-1}\delta^{-1}} \frac{1}{N(k\delta)^2} \ll (N + \delta^{-1}).$$

- Thus in every case we have the bound $\ll N + \frac{1}{\delta}$.
- Note: Describe Bombieri and Selberg proofs.

- We have established

Theorem 3 (A Large Sieve Inequality 1)

The inequality

$$\sum_{r=1}^{R} |S(x_r)|^2 \le Y_0(N,\delta) \sum_{n=M+1}^{M+N} |a_n|^2$$

holds with

$$Y_0(N,\delta) \ll N + \frac{1}{\delta}$$

and

$$\sum_{q\le Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right)\right|^2 \le Y(N,Q) \sum_{n=M+1}^{M+N} |a_n|^2$$

holds with

$$Y(N,Q) \ll N + Q^2.$$

- The expression

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2$$

tells us something about polynomials formed from additive characters $e(a*/q)$.

- The expression

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2$$

  tells us something about polynomials formed from additive characters $e(a*/q)$.
- It would be very interesting to have a similar result for Dirichlet characters, i.e. multiplicative characters.

- We have

Theorem 4 (A Large Sieve for Characters)

Suppose that

$$S(\chi) = \sum_{n=M+1}^{M+N} a_n \chi(n).$$

Then

$$\sum_{q \le Q} \frac{q}{\phi(q)} \sum_{\chi \bmod q}^{*} |S(\chi)|^2 \le Y(N,Q) \sum_{n=M+1}^{M+N} |a_n|^2$$

holds with

$$Y(N,Q) \ll N + Q^2.$$

- We have

Theorem 4 (A Large Sieve for Characters)

Suppose that

$$S(\chi) = \sum_{n=M+1}^{M+N} a_n \chi(n).$$

Then

$$\sum_{q\le Q} \frac{q}{\phi(q)} \sum_{\chi \text{ mod } q}{}^{*} |S(\chi)|^2 \le Y(N,Q) \sum_{n=M+1}^{M+N} |a_n|^2$$

holds with

$$Y(N,Q) \ll N + Q^2.$$

- Here $\sum^*_{\chi \pmod q}$ indicates a sum over the primitive characters modulo q.

- We transfer the problem from multiplicative characters to additive ones, and for this we use the Gauss sum.

- We transfer the problem from multiplicative characters to additive ones, and for this we use the Gauss sum.
- Recall Theorem 2.8. If χ is a primitive, then

$$\chi(n)\tau(\overline{\chi}) = \sum_{a=1}^{q} \overline{\chi}(a)e(an/q).$$

and $|\tau(\chi)| = \sqrt{q}$.

- We transfer the problem from multiplicative characters to additive ones, and for this we use the Gauss sum.
- Recall Theorem 2.8. If χ is a primitive, then

$$\chi(n)\tau(\overline{\chi}) = \sum_{a=1}^{q} \overline{\chi}(a)e(an/q).$$

and $|\tau(\chi)| = \sqrt{q}$.
- Thus

$$\sum_{n=M+1}^{M+N} a_n\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q}\overline{\chi}(a)\sum_{n=M+1}^{M+N} a_n e(an/q).$$

- We transfer the problem from multiplicative characters to additive ones, and for this we use the Gauss sum.
- Recall Theorem 2.8. If χ is a primitive, then

$$\chi(n)\tau(\overline{\chi}) = \sum_{a=1}^{q} \overline{\chi}(a)e(an/q).$$

and $|\tau(\chi)| = \sqrt{q}$.

- Thus

$$\sum_{n=M+1}^{M+N} a_n\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi}(a) \sum_{n=M+1}^{M+N} a_n e(an/q).$$

- Hence

$$\begin{aligned}\sideset{}{^*}\sum_{\chi \bmod q} |S(\chi)|^2 &= \frac{1}{q} \sideset{}{^*}\sum_{\chi \bmod q} \left| \sum_{a=1}^{q} \overline{\chi}(a)S(a/q) \right|^2 \\ &\le \frac{1}{q} \sum_{\chi \bmod q} \left| \sum_{a=1}^{q} \overline{\chi}(a)S(a/q) \right|^2\end{aligned}$$

- We have

$$\sum_{\chi \bmod q}^{*} |S(\chi)|^2 \le \frac{1}{q} \sum_{\chi \bmod q} \left| \sum_{a=1}^{q} \overline{\chi}(a) S(a/q) \right|^2$$

- We have

$$\sum_{\chi \bmod q}^{*} |S(\chi)|^2 \le \frac{1}{q} \sum_{\chi \bmod q} \left| \sum_{a=1}^{q} \overline{\chi}(a) S(a/q) \right|^2$$

- and by Parseval's identity this is

$$\frac{\phi(q)}{q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(a/q)|^2.$$

- We have

$$\sum_{\chi \bmod q}{}^{*} |S(\chi)|^2 \le \frac{1}{q} \sum_{\chi \bmod q} \left| \sum_{a=1}^{q} \overline{\chi}(a) S(a/q) \right|^2$$

- and by Parseval's identity this is

$$\frac{\phi(q)}{q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(a/q)|^2.$$

- Thus

$$\frac{q}{\phi(q)} \sum_{\chi \bmod q}{}^{*} |S(\chi)|^2 \le \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(a/q)|^2$$

and the theorem follows from the previous one.

- Two variants of the large sieve that are useful in applications.

- Two variants of the large sieve that are useful in applications.
- In practice one does not have the square of a Dirichlet polynomial $|S(\chi)|^2$ arising naturally in a problem.

- Two variants of the large sieve that are useful in applications.
- In practice one does not have the square of a Dirichlet polynomial $|S(\chi)|^2$ arising naturally in a problem.
- However one can arrange to have a product of two different such polynomials.

Lemma 5

Suppose that $a_1, \ldots, a_M$, $b_1, \ldots, b_N$ are complex numbers. Then

$$\sum_{q\le Q} \frac{q}{\phi(q)} \sum_{\chi}{}^{*} \left| \sum_{m=1}^{M} \sum_{n=1}^{N} a_m b_n \chi(mn) \right| \ll \sqrt{(M+Q^2)(N+Q^2) \sum_{m=1}^{M} |a_m|^2 \sum_{n=1}^{N} |b_n|^2}.$$

- Two variants of the large sieve that are useful in applications.
- In practice one does not have the square of a Dirichlet polynomial $|S(\chi)|^2$ arising naturally in a problem.
- However one can arrange to have a product of two different such polynomials.

Lemma 5

Suppose that $a_1, \ldots, a_M$, $b_1, \ldots, b_N$ are complex numbers. Then

$$\sum_{q\le Q} \frac{q}{\phi(q)} \sum_{\chi}{}^{*} \left| \sum_{m=1}^{M} \sum_{n=1}^{N} a_m b_n \chi(mn) \right| \ll \sqrt{(M+Q^2)(N+Q^2) \sum_{m=1}^{M} |a_m|^2 \sum_{n=1}^{N} |b_n|^2}.$$

- Proof: Cauchy-Schwarz.

- To illustrate what can happen with a simple special case, recall the Dirichlet divisor problem

$$\sum_{n\le X} d(n).$$

- To illustrate what can happen with a simple special case, recall the Dirichlet divisor problem

$$\sum_{n\le X} d(n).$$

- There we wrote $d(n)$ as the number of ordered pairs l, m with $lm = n$, so that the sum is the number of such ordered pairs with $lm \le X$.

- To illustrate what can happen with a simple special case, recall the Dirichlet divisor problem

$$\sum_{n\le X} d(n).$$

- There we wrote $d(n)$ as the number of ordered pairs l, m with $lm = n$, so that the sum is the number of such ordered pairs with $lm \le X$.
- That is, given an l we are counting the m with $m \le X/l$, so we could rearrange the sum as

$$\sum_{l\le X} \sum_{m\le X/l} 1.$$

- To illustrate what can happen with a simple special case, recall the Dirichlet divisor problem

$$\sum_{n \leq X} d(n).$$

- There we wrote $d(n)$ as the number of ordered pairs l, m with $lm = n$, so that the sum is the number of such ordered pairs with $lm \leq X$.
- That is, given an l we are counting the m with $m \leq X/l$, so we could rearrange the sum as

$$\sum_{l \leq X} \sum_{m \leq X/l} 1.$$

- So there is an interaction in our sums - the end point in the inner sum depends on l.

- To illustrate what can happen with a simple special case, recall the Dirichlet divisor problem

$$\sum_{n\le X} d(n).$$

- There we wrote $d(n)$ as the number of ordered pairs l, m with $lm = n$, so that the sum is the number of such ordered pairs with $lm \le X$.
- That is, given an l we are counting the m with $m \le X/l$, so we could rearrange the sum as

$$\sum_{l\le X}\sum_{m\le X/l} 1.$$

- So there is an interaction in our sums - the end point in the inner sum depends on l.
- Dirichlet minimised the effect by a trick, but the dependence remains.

- Another example is a formula for the von Mangoldt function.

- Another example is a formula for the von Mangoldt function.
- Recall $\log = \mathbf{1} * \Lambda$, and $\Lambda = \mu * \log$.

- Another example is a formula for the von Mangoldt function.
- Recall $\log = \mathbf{1} * \Lambda$, and $\Lambda = \mu * \log$.
- Thus we are interested in expressions of the kind

$$\sum_{n \le x} \Lambda(n)\chi(n) = \sum_{l \le x} \sum_{m \le x/l} \mathbf{1}(l)\chi(l) \log(m)\big(\chi(m)\big).$$

The interdependence of l and m is a nuisance.

- Another example is a formula for the von Mangoldt function.
- Recall $\log = \mathbf{1} * \Lambda$, and $\Lambda = \mu * \log$.
- Thus we are interested in expressions of the kind

$$\sum_{n\le x} \Lambda(n)\chi(n) = \sum_{l\le x}\sum_{m\le x/l} \mathbf{1}(l)\chi(l)\log(m)\big(\chi(m)\big).$$

The interdependence of l and m is a nuisance.

- Classically this is solved by two observations. Firstly $\zeta(s) = \displaystyle\sum_{k=1}^{\infty} k^{-s}$,

$$\zeta(s)^{-1} = \sum_{l=1}^{\infty} \mu(l) l^{-s}, \sum_{m=1}^{\infty} (\log m) m^{-s} = -\zeta'(s)$$

so that formally

$$\sum_{n=1}^{\infty} \Lambda(n) n^{-s} = -\zeta(s)^{-1}\zeta'(s).$$

- Firstly
$$\sum_{n=1}^{\infty} \Lambda(n) n^{-s} = -\zeta(s)^{-1}\zeta'(s).$$

- Firstly

$$\sum_{n=1}^{\infty} \Lambda(n) n^{-s} = -\zeta(s)^{-1}\zeta'(s).$$

- Secondly

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s} ds = \begin{cases} 0 & (0 < y < 1), \\ \frac{1}{2} & (y = 1), \\ 1 & (1 < y). \end{cases}$$

- Firstly
$$\sum_{n=1}^{\infty}\Lambda(n)n^{-s} = -\zeta(s)^{-1}\zeta'(s).$$
- Secondly
$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{y^s}{s}ds = \begin{cases} 0 & (0<y<1), \\ \frac12 & (y=1), \\ 1 & (1<y). \end{cases}$$
- Thus
$$\begin{aligned}\sum_{n\le x}{}' \Lambda(n) &= \sum_{lm\le x}\mu(l)(\log m) \\ &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(-\frac{\zeta'}{\zeta}(s)\right)\frac{x^s}{s}ds.\end{aligned}$$

- Firstly

$$\sum_{n=1}^{\infty} \Lambda(n) n^{-s} = -\zeta(s)^{-1}\zeta'(s).$$

- Secondly

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s} ds = \begin{cases} 0 & (0 < y < 1), \\ \frac{1}{2} & (y = 1), \\ 1 & (1 < y). \end{cases}$$

- Thus

$$\sum_{n\le x}{}' \Lambda(n) = \sum_{lm\le x} \mu(l)(\log m)$$
$$= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds.$$

- Notice how the condition $lm \le x$ has been separated out.

- We can use this idea to deal with more general series

- We can use this idea to deal with more general series
- Then one can write formally

$$\sum_{l} a_l \sum_{m\le x/l} b_m = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \sum_{l} \frac{a_l}{l^s} \sum_{m} \frac{b_m}{m^s} \frac{x^s}{s} ds.$$

- We can use this idea to deal with more general series
- Then one can write formally

$$\sum_l a_l \sum_{m \le x/l} b_m = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \sum_l \frac{a_l}{l^s} \sum_m \frac{b_m}{m^s} \frac{x^s}{s} ds.$$

- Note that this "factoring out" of the x would enable one to choose different x for each character χ, which is useful.

- We can use this idea to deal with more general series
- Then one can write formally

$$\sum_l a_l \sum_{m\le x/l} b_m = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \sum_l \frac{a_l}{l^s} \sum_m \frac{b_m}{m^s}\frac{x^s}{s}ds.$$

- Note that this "factoring out" of the x would enable one to choose different x for each character χ, which is useful.
- Rather than develop this, I am going to use a real variable variant. By the way there are other alternatives, for example by Rademacher-Menchov functions, or Walsh functions.

- Here is the ultimate form of the large sieve for characters

Theorem 6

Suppose that $X \ge 2$, and the a_m and b_n are complex numbers. Then

$$\sum_{q\le Q}\frac{q}{\phi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\sup_{Y\le X}\left|\sum_{m=1}^{M}\sum_{\substack{n=1\\ mn\le Y}}^{N} a_m b_n \chi(mn)\right|$$

$$\ll (\log XMN)\sqrt{(M+Q^2)(N+Q^2)\sum_{m=1}^{M}|a_m|^2\sum_{n=1}^{N}|b_n|^2}.$$

- The first step in the proof is the observation that for some positive constant C,

$$\int_{-\infty}^{\infty} e^{i\beta\alpha} \frac{\sin(\gamma\alpha)}{C\alpha} d\alpha = \begin{cases} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{cases} \tag{1}$$

- The first step in the proof is the observation that for some positive constant C,

$$\int_{-\infty}^{\infty} e^{i\beta\alpha}\frac{\sin(\gamma\alpha)}{C\alpha}d\alpha = \begin{cases} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{cases} \tag{1}$$

- It turns out that we can take $C = \displaystyle\int_{-\infty}^{\infty} \frac{\sin \alpha}{\alpha} d\alpha$.

- The first step in the proof is the observation that for some positive constant C,

$$\int_{-\infty}^{\infty} e^{i\beta\alpha}\frac{\sin(\gamma\alpha)}{C\alpha}d\alpha = \begin{cases} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{cases} \tag{1}$$

- It turns out that we can take $C = \displaystyle\int_{-\infty}^{\infty} \frac{\sin \alpha}{\alpha} d\alpha.$
- That C exists and $C > 0$ is trivial from

$$\int_{-\infty}^{\infty} \frac{\sin \alpha}{\alpha} d\alpha = 2\sum_{n=1}^{\infty}(-1)^{n-1}\int_0^{\pi} \frac{\sin \alpha}{\pi(n-1)+\alpha}.d\alpha$$

The terms oscillate in sign and the integrals form a decreasing sequence tending to 0, so Leibnitz' test applies.

- The first step in the proof is the observation that for some positive constant C,

$$\int_{-\infty}^{\infty} e^{i\beta\alpha}\frac{\sin(\gamma\alpha)}{C\alpha}d\alpha = \begin{cases} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{cases} \tag{1}$$

- It turns out that we can take $C = \displaystyle\int_{-\infty}^{\infty} \frac{\sin\alpha}{\alpha}d\alpha.$
- That C exists and $C > 0$ is trivial from

$$\int_{-\infty}^{\infty} \frac{\sin\alpha}{\alpha}d\alpha = 2\sum_{n=1}^{\infty}(-1)^{n-1}\int_0^{\pi} \frac{\sin\alpha}{\pi(n-1)+\alpha}.d\alpha$$

The terms oscillate in sign and the integrals form a decreasing sequence tending to 0, so Leibnitz' test applies.

- Pairing α and $-\alpha$ in (1) shows that the integral is real.

- The first step in the proof is the observation that for some positive constant C,

$$\int_{-\infty}^{\infty} e^{i\beta\alpha}\frac{\sin(\gamma\alpha)}{C\alpha}d\alpha = \begin{cases} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{cases} \tag{1}$$

- It turns out that we can take $C = \int_{-\infty}^{\infty} \frac{\sin\alpha}{\alpha}d\alpha.$
- That C exists and $C > 0$ is trivial from

$$\int_{-\infty}^{\infty} \frac{\sin\alpha}{\alpha}d\alpha = 2\sum_{n=1}^{\infty}(-1)^{n-1}\int_0^{\pi} \frac{\sin\alpha}{\pi(n-1)+\alpha}.d\alpha$$

The terms oscillate in sign and the integrals form a decreasing sequence tending to 0, so Leibnitz' test applies.

- Pairing α and $-\alpha$ in (1) shows that the integral is real.
- Also $\cos\beta\alpha\sin\gamma\alpha = \frac{1}{2}(\sin((\gamma+\beta)\alpha) + \sin((\gamma-\beta)\alpha))$ and changing variables gives 1 when $0 \le \beta < \gamma$ and 0 when $\beta > \gamma$.

- We have

$$\int_{-\infty}^{\infty} e^{i\beta\alpha}\frac{\sin(\gamma\alpha)}{C\alpha}d\alpha = \begin{cases} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{cases}$$

- We have

$$\int_{-\infty}^{\infty} e^{i\beta\alpha}\frac{\sin(\gamma\alpha)}{C\alpha}d\alpha = \begin{cases} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{cases}$$

- By integration by parts, provided that $Z > 0$ and $A > 0$, one has

$$\int_{A}^{\infty} \frac{\sin Z\alpha}{\alpha}d\alpha \ll \frac{1}{ZA}.$$

- We have
$$\int_{-\infty}^{\infty} e^{i\beta\alpha}\frac{\sin(\gamma\alpha)}{C\alpha}d\alpha = \begin{cases} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{cases}$$
- By integration by parts, provided that $Z > 0$ and $A > 0$, one has
$$\int_{A}^{\infty} \frac{\sin Z\alpha}{\alpha}d\alpha \ll \frac{1}{ZA}.$$
- Thus, on taking $Z = |\gamma \pm \beta|$ and using $\cos\beta\alpha\sin\gamma\alpha = \frac{1}{2}(\sin((\gamma+\beta)\alpha) + \sin((\gamma-\beta)\alpha))$ we have
$$\left\{\begin{matrix} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{matrix}\right\} = \int_{-A}^{A} e^{i\beta\alpha}\frac{\sin\gamma\alpha}{C\alpha}d\alpha + O\left(\frac{1}{A|\gamma-\beta|}\right).$$

- We have

$$\begin{Bmatrix} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{Bmatrix} = \int_{-A}^{A} e^{i\beta\alpha} \frac{\sin \gamma\alpha}{C\alpha} d\alpha + O\left(\frac{1}{A|\gamma - \beta|} \right).$$

- We have

$$\begin{Bmatrix} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{Bmatrix} = \int_{-A}^{A} e^{i\beta\alpha} \frac{\sin \gamma\alpha}{C\alpha} d\alpha + O\left(\frac{1}{A|\gamma - \beta|} \right).$$

- Now we specialise $\gamma = \log\left(\lfloor Y \rfloor + \frac{1}{2}\right)$, $\beta = \log mn$ so that

$$\begin{Bmatrix} 1 & mn \le Y, \\ 0 & mn > Y \end{Bmatrix} = \int_{-A}^{A} (mn)^{i\alpha} \frac{\sin \gamma\alpha}{C\alpha} d\alpha$$

$$+ O\left(\frac{1}{A\left|\log\left(\lfloor Y \rfloor + \frac{1}{2}\right) - \log mn\right|} \right).$$

- We have

$$\begin{Bmatrix} 1 & 0 \le \beta < \gamma, \\ 0 & 0 \le \gamma < \beta. \end{Bmatrix} = \int_{-A}^{A} e^{i\beta\alpha} \frac{\sin \gamma\alpha}{C\alpha} d\alpha + O\left(\frac{1}{A|\gamma - \beta|}\right).$$

- Now we specialise $\gamma = \log\left(\lfloor Y \rfloor + \frac{1}{2}\right)$, $\beta = \log mn$ so that

$$\begin{Bmatrix} 1 & mn \le Y, \\ 0 & mn > Y \end{Bmatrix} = \int_{-A}^{A} (mn)^{i\alpha} \frac{\sin \gamma\alpha}{C\alpha} d\alpha$$

$$+ O\left(\frac{1}{A\left|\log\left(\lfloor Y \rfloor + \frac{1}{2}\right) - \log mn\right|}\right).$$

- Moreover $\min\limits_{m,n} \left|\log\left(\lfloor Y \rfloor + \frac{1}{2}\right) - \log mn\right| =$

$$\min\left(\log \frac{\lfloor Y \rfloor + \frac{1}{2}}{\lfloor Y \rfloor}, \log \frac{\lfloor Y \rfloor + 1}{\lfloor Y \rfloor + \frac{1}{2}}\right) \gg \frac{1}{Y}.$$

- Thus, with $\gamma = \log(\lfloor Y \rfloor + \frac{1}{2})$, and $Y \le X$,

$$\begin{Bmatrix} 1 & mn \le Y, \\ 0 & mn > Y \end{Bmatrix} = \int_{-A}^{A} (mn)^{i\alpha} \frac{\sin \gamma\alpha}{C\alpha} d\alpha + O\left(\frac{X}{A}\right).$$

- Thus, with $\gamma = \log(\lfloor Y \rfloor + \frac{1}{2})$, and $Y \le X$,

$$\begin{Bmatrix} 1 & mn \le Y, \\ 0 & mn > Y \end{Bmatrix} = \int_{-A}^{A} (mn)^{i\alpha} \frac{\sin \gamma\alpha}{C\alpha} d\alpha + O\left(\frac{X}{A}\right).$$

- Hence

$$\sum_{m=1}^{M} \sum_{\substack{n=1 \\ mn \le Y}}^{N} a_m b_n \chi(mn) =$$

$$\int_{-A}^{A} \sum_{m=1}^{M} \sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha} \chi(mn) \frac{\sin \gamma\alpha}{C\alpha} d\alpha$$

$$+ O\left(\frac{X}{A} \sum_{m=1}^{M} \sum_{n=1}^{N} |a_m b_n|\right).$$

- We have $\sum_{m=1}^{M} \sum_{\substack{n=1 \\ mn \le Y}}^{N} a_m b_n \chi(mn) =$

$$\int_{-A}^{A} \sum_{m=1}^{M} \sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha} \chi(mn) \frac{\sin \gamma\alpha}{C\alpha} d\alpha$$

$$+ O\left(\frac{X}{A} \sum_{m=1}^{M} \sum_{n=1}^{N} |a_m b_n| \right).$$

- We have $\displaystyle\sum_{m=1}^{M}\sum_{\substack{n=1\\mn\le Y}}^{N} a_m b_n \chi(mn) =$

$$\int_{-A}^{A}\sum_{m=1}^{M}\sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha}\chi(mn)\frac{\sin\gamma\alpha}{C\alpha}d\alpha + O\left(\frac{X}{A}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n|\right).$$

- Thus $\displaystyle\sup_{Y\le X}\left|\sum_{m=1}^{M}\sum_{\substack{n=1\\mn\le Y}}^{N} a_m b_n\chi(mn)\right| \ll$

$$\int_{-A}^{A}\left|\sum_{m=1}^{M}\sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha}\chi(mn)\right|\min\left(\log X,\frac{1}{|\alpha|}\right)d\alpha + \frac{X}{A}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n|.$$

- Thus $\sup_{Y\le X}\left|\sum_{m=1}^{M}\sum_{\substack{n=1\\mn\le Y}}^{N} a_m b_n \chi(mn)\right| \ll \frac{X}{A}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n|$

$$+\int_{-A}^{A}\left|\sum_{m=1}^{M}\sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha}\chi(mn)\right| \min\left(\log X, \frac{1}{|\alpha|}\right) d\alpha.$$

- Thus $\sup_{Y\le X}\left|\sum_{m=1}^{M}\sum_{\substack{n=1\\ mn\le Y}}^{N} a_m b_n \chi(mn)\right| \ll \frac{X}{A}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n|$

$$+\int_{-A}^{A}\left|\sum_{m=1}^{M}\sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha}\chi(mn)\right| \min\left(\log X, \frac{1}{|\alpha|}\right) d\alpha.$$

- We choose $A = XMN$. Then, by Cauchy-Schwarz

$$\frac{X}{A}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n| \ll \frac{1}{MN}(MN)^{\frac12}\left(\sum_{m=1}^{M}|a_m|^2\sum_{n=1}^{N}|b_n|^2\right)^{\frac12}.$$

- Thus $\sup_{Y\le X}\left|\sum_{m=1}^{M}\sum_{\substack{n=1\\mn\le Y}}^{N} a_m b_n \chi(mn)\right| \ll \frac{X}{A}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n|$

$$+\int_{-A}^{A}\left|\sum_{m=1}^{M}\sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha}\chi(mn)\right| \min\left(\log X, \frac{1}{|\alpha|}\right) d\alpha.$$

- We choose $A = XMN$. Then, by Cauchy-Schwarz

$$\frac{X}{A}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n| \ll \frac{1}{MN}(MN)^{\frac12}\left(\sum_{m=1}^{M}|a_m|^2\sum_{n=1}^{N}|b_n|^2\right)^{\frac12}.$$

- Summing over $\sum_{q\le Q}\frac{q}{\phi(q)}\sum_{\chi^*}{}^{*}1 \ll \sum_{q\le Q} q$ gives

$$\ll \frac{1}{(MN)^{1/2}}\left((M+Q^2)(N+Q^2)\sum_{m=1}^{M}|a_m|^2\sum_{n=1}^{N}|b_n|^2\right)^{\frac12}.$$

- Thus we can concentrate on the integral in

$$\sup_{Y\le X}\left|\sum_{m=1}^{M}\sum_{\substack{n=1\\mn\le Y}}^{N} a_m b_n \chi(mn)\right| \ll$$

$$\int_{-A}^{A}\left|\sum_{m=1}^{M}\sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha}\chi(mn)\right| \min\left(\log X, \frac{1}{|\alpha|}\right) d\alpha$$

$$+\frac{X}{A}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n|.$$

- Thus we can concentrate on the integral in

$$\sup_{Y\le X}\left|\sum_{m=1}^{M}\sum_{\substack{n=1\\ mn\le Y}}^{N} a_m b_n \chi(mn)\right| \ll$$

$$\int_{-A}^{A}\left|\sum_{m=1}^{M}\sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha}\chi(mn)\right| \min\left(\log X, \frac{1}{|\alpha|}\right) d\alpha$$

$$+\frac{X}{A}\sum_{m=1}^{M}\sum_{n=1}^{N}|a_m b_n|.$$

- Summing the integral over $\sum_{q\le Q}\frac{q}{\phi(q)}\sum_{\chi^*}^{*}$ gives

$$\int_{-A}^{A} T(\alpha)\min\left(\log X, \frac{1}{|\alpha|}\right) d\alpha$$

where

$$T(\alpha)=\sum_{q\le Q}\frac{q}{\phi(q)}\sum_{\chi^*}^{*}\left|\sum_{m=1}^{M}\sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha}\chi(mn)\right|.$$

- Now, by Lemma 5, we have

$$T(\alpha) = \sum_{q\le Q} \frac{q}{\phi(q)} \sum_{\chi^*}{}^{*} \left| \sum_{m=1}^{M} \sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha} \chi(mn) \right|$$

$$\ll \sqrt{(M+Q^2)(N+Q^2) \sum_{m=1}^{M} |a_m|^2 \sum_{n=1}^{N} |b_n|^2}.$$

- Now, by Lemma 5, we have

$$T(\alpha) = \sum_{q \le Q} \frac{q}{\phi(q)} \sum_{\chi^*}{}^{*} \left| \sum_{m=1}^{M} \sum_{n=1}^{N} a_m m^{i\alpha} b_n n^{i\alpha} \chi(mn) \right|$$

$$\ll \sqrt{(M+Q^2)(N+Q^2) \sum_{m=1}^{M} |a_m|^2 \sum_{n=1}^{N} |b_n|^2}.$$

- Also

$$\int_{-A}^{A} \min\left(\log X, \frac{1}{|\alpha|}\right) d\alpha \ll \log XMN.$$

- To summarize, we have just proved that if $X \geq 2$, and the a_m and b_n are complex numbers, then

$$\sum_{q\le Q}\frac{q}{\phi(q)}\sum_{\chi \bmod q}^{*}\sup_{Y\le X}\left|\sum_{m=1}^{M}\sum_{\substack{n=1\\ mn\le Y}}^{N}a_mb_n\chi(mn)\right|$$

$$\ll (\log XMN)\sqrt{(M+Q^2)(N+Q^2)\sum_{m=1}^{M}|a_m|^2\sum_{n=1}^{N}|b_n|^2}.$$

E. Bombieri, On the large sieve, Mathematika 12(1965),201–225

E. Bombieri and H. Davenport, On the large sieve method, Abh. Zahlentheorie Anal. 1968, 9–22

H. Davenport, Multiplicative number theory, Markham, Chicago 1967.

H. Davenport, Multiplicative Number Theory, third edition Springer-Verlag, Berlin 2000.

T. Estermann, Introduction to modern prime number theory, Cambridge University Press, Cambridge, Tract No. 41, 1952

P. X. Gallagher, The large sieve, Mathematika 14(1967), 14–20

P. X. Gallagher, Bombieri's mean value theorem, Mathematika 15(1968), 1–6

- Yu. V. Linnik, The large sieve, C. R. (Dokl.) Acad. Sci. URSS, n. Ser. 30(1941), 292–294
- Yu. V. Linnik, A remark on the least quadratic non-residue, C. R. (Dokl.) Acad. Sci. URSS, n. Ser. 36(1942), 119–120
- H. L. Montgomery, A note on the large sieve, J. Lond. Math. Soc. 43(1968), 93–98
- H. L. Montgomery, The analytic principle of the large sieve, Bull. Am. Math. Soc. 84(1978), 547–567
- H. L. Montgomery, Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis (CBMS Regional Conference Series in Mathematics), Volume 84, 1994, 220 pp.
- H. L. Montgomery and R. C. Vaughan, The large sieve, Mathematika 20(1973), 119–134
- H. L. Montgomery and R. C. Vaughan, Hilbert's inequality, J. Lond. Math. Soc. (2) 8(1974), 73–82

- H. L. Montgomery and R. C. Vaughan, Multiplicative Number Theory. I. Classical Theory, Cambridge University Press, Cambridge 2006
- G. Pólya, Über die Verteilung der quadratischen Reste und Nichtreste, Nachr. Akad. Wiss. Göttingen 1918, 21–29
- K. F. Roth, On the large sieves of Linnik and Renyi, Mathematika 12(1965), 1–9
- I. Schur, Bemerkungen zur Theorie der beschränkten Bilinearformen mit unendlich vielen Veränderlichen, J. Reine Angew. Math., 140(1911), 1—28
- I. Schur, Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Pólya: Über die Verteilung der quadratischen Reste und Nichtreste, Nachr. Akad. Wiss. Göttingen 1918, 30–36
- A. Selberg, Collected papers. Volume II, Springer-Verlag, Berlin 1991

C. L. Siegel,Über die Klassenzahl quadratischer Zahlkörper, Acta Arith. 1(1935), 83–86

E. C. Titchmarsh, A divisor problem, Rend. Circ. Mat. Palermo 54(1930), 414–429

R. C. Vaughan, Sommes trigonométriques sur les nombres premiers, C. R. Acad. Sci. Paris, Série A 285(1977), 981-983

R. C. Vaughan, An elementary method in prime number theory, Acta Arith. 37(1980), 111–115

A. I. Vinogradov, On the density hypothesis for Dirichlet L–series, Izv. Akad. Nauk SSSR, Ser. Mat. 29(1965), 903–934

A. I. Vinogradov, Corrections to the work of A.I. Vinogradov 'On the density hypothesis for Dirichlet L–series', Izv. Akad. Nauk SSSR, Ser. Mat. 30(1966), 719–729

- I. M. Vinogradov, Sur la distribution des résidus et des nonrésidus des puissances, J. Soc. Phys. Math. Univ. Permi 1918, 18–28
- I. M. Vinogradov, Über die Verteilung der quadratischen Reste und Nichtreste, J. Soc. Phys. Math. Univ. Permi 1919, 1–14
- I. M. Vinogradov, Some theorems concerning the theory of primes, Recueil Math. (2) 44(1937), 179–195
- A. Walfisz, Zur additiven Zahlentheorie. II, Math. Z. 40(1936), 592–607