VI. The Large Sieve

A problem Estimate $S(\mathcal{A},\mathcal{P})$ when $pg(p)$ is not bounded on average,

e.g. $g(p) \approx \frac{1}{2}$.

1. Exponential sum version

Let $e(z) = e^{2\pi i z}$, note $\overline{e(z)} = e(-z)$. Let $a_{M+1}, \cdots, a_{M+N} \in \mathbb{C}$ and consider the exponential sum

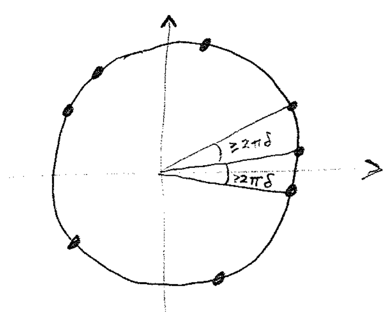
$$(6.1) \qquad S(x) = \sum_{n=M+1}^{M+N} a_n e(nx).$$

It is easy to find the average of $|S(x)|^2$ on the unit interval:

$$\begin{aligned}\int_0^1 |S(x)|^2 dx &= \int_0^1 S(x)\overline{S(x)}\, dx \\ &= \int_0^1 \Big(\sum_n a_n e(nx)\Big)\Big(\sum_{n'} \bar{a}_{n'} e(-n'x)\Big) dx \\ &= \sum_{n,n'} a_n \bar{a}_{n'} \int_0^1 e((n-n')x)\, dx \qquad ; \int_0^1 e(mx)dx = \begin{cases} 1 & m=0 \\ 0 & m\neq 0\end{cases} \\ &= \sum_n |a_n|^2.\end{aligned}$$

(This is Parseval's identity). We derive a kind of discrete analog.

Define $\|x\| = \min\{x-n : n \in \mathbb{Z}\}$, note $0 \le \|x\| \le \frac{1}{2}$ for $x \in \mathbb{R}$. We call a finite set $\{x_1, x_2, \cdots, x_r\}$ δ-spaced if $\|x_i - x_j\| \ge \delta$ when $i \ne j$. Equivalently, the points $e(x_i)$ have arguments differing by $\gtrsim 2\pi\delta$



Theorem 6.1 If $\{x_1, \cdots, x_r\}$ is δ-spaced and $S(x)$ is defined by (6.1), then

$$(6.2) \qquad \sum_{i=1}^{r} |S(x_i)|^2 \le C\left(N + \frac{1}{\delta}\right) \sum_{n=M+1}^{M+N} |a_n|^2.$$

Here C is an absolute constant.

Remarks (i) We prove it with $C = 2\pi$. It has been proven with $C = 1$ due to Montgomery–Vaughan and independently by Selberg.

(ii) Always $\delta \leq \frac{1}{r}$. If $\delta = \frac{1}{r}$, then $x_1, x_2, \cdots x_r$ are equally spaced around the unit circle, and so $\delta \sum_{i=1}^{r} |S(x_i)|^2$ is a Riemann sum for $\int_0^1 |S(x)|^2 dx$.
Thus, as $r \to \infty$, $\delta \sum_{i=1}^{r} |S(x_i)|^2 \to \sum_{n=M+1}^{M+N} |a_n|^2$, i.e. the term $\frac{1}{\delta}$ cannot be removed.

Also, if $r \geq 1$, $a_n = 1 \ \forall n$ and $x_1 = 0$, then
$$|S(x_1)|^2 = N^2 = N \sum_{n=M+1} |a_n|^2,$$ so the term N cannot be removed.

In other words, (6.2) is best possible with $C = 1$.

(iii) Assume $|a_n| = 1$. The theorem says that on average over i,
$$|S(x_i)| \ll \left(\frac{1}{r}\left(N + \frac{1}{\delta}\right) N\right)^{\frac{1}{2}} \ll \frac{N}{\sqrt{r}} \quad \text{if } \delta \gg \frac{1}{N}.$$ In particular, this holds for at least one i. This is a savings of $\frac{1}{\sqrt{r}}$ over the trivial bound $|S(x_i)| \leq N$.

(iv) The parameter M is irrelevant and WLOG may be taken to be zero.
We have
$$|S(x)| = \left|\sum_{n=M+1}^{M+N} a_n e(nx)\right| = |S^*(x)| = \left|\sum_{m=1}^{N} a_{m+M} e(mx)\right|,$$
where $S^*(x) = e(-Mx) S(x)$.

Proof idea

For a continuous function $f : \mathbb{R} \to \mathbb{C}$, $f(x) \approx \frac{1}{2\varepsilon} \int_{x-\varepsilon}^{x+\varepsilon} f(u)\,du$ if ε small.

The error depends on the size of $f'(u)$ for u close to x.

We will approximate $|S(x)|^2$ by $\int_{x-\delta/2}^{x+\delta/2} |S(u)|^2 du$ using the following lemma.

4-20-11. #34

Lemma 6.1 (Gallagher, 1967)

If $f : \mathbb{R} \to \mathbb{C}$ has continuous derivative on $[x - \delta/2, x + \delta/2]$, then
$$|f(x)| \leq \frac{1}{\delta} \int_{x-\delta/2}^{x+\delta/2} |f(y)|\,dy + \frac{1}{2} \int_{x-\delta/2}^{x+\delta/2} |f'(y)|\,dy.$$

Proof WLOG $x=0$. Using integration by parts,

$$\int_0^{\delta/2}\left(\frac{\delta}{2}-y\right)f'(y)\,dy = -\frac{\delta}{2}f(0) + \int_0^{\delta/2} f(y)\,dy$$

and

$$\int_{-\delta/2}^{0}\left(\frac{\delta}{2}+y\right)f'(y)\,dy = \frac{\delta}{2}f(0) - \int_{-\delta/2}^{0} f(y)\,dy.$$

Subtracting the two equations gives

$$\delta f(0) = \int_{-\delta/2}^{\delta/2} f(y)\,dy + \int_{-\delta/2}^{0}\left(\frac{\delta}{2}+y\right)f'(y) - \int_0^{\delta/2}\left(\frac{\delta}{2}-y\right)f'(y)\,dy.$$

Hence

$$|f(0)| \le \frac{1}{\delta}\int_{-\delta/2}^{\delta/2} f(y)\,dy + \frac{1}{2}\int_{-\delta/2}^{\delta/2}|f'(y)|.$$

#26

Proof of Theorem 6.1

WLOG $M=0$. Apply Lemma 6.1 with $f(x)=S^2(x)$ at each $x=x_i$ to get

$$|S(x_i)|^2 \le \frac{1}{\delta}\int_{I_i}|S(y)|^2dy + \frac{1}{2}\int_{I_i}|2S(y)S'(y)|\,dy, \qquad I_i=\left[x_i-\frac{\delta}{2}, x_i+\frac{\delta}{2}\right].$$

Since the x_i are δ-spaced, the I_i are non-overlapping modulo 1 and their union, modulo 1, is contained in $[0,1]$ ($S(x)$ is periodic with period 1).

Therefore,

$$\sum_{i=1}^{r}|S(x_i)|^2 \le \frac{1}{\delta}\int_0^1|S(y)|^2dy + \int_0^1|S(y)S'(y)|\,dy.$$

By Parseval's identity,

$$\int_0^1|S(y)|^2dy = \sum_{n=1}^{N}|a_n|^2.$$

Also, noting $S'(y)=\sum_{n=1}^{N}2\pi i n\, a_n\, e(nx)$ and using Cauchy-Schwarz inequality,

$$\begin{aligned}\int_0^1|S(y)S'(y)|\,dy &\le \left(\int_0^1|S(y)|^2\right)^{1/2}\left(\int_0^1|S'(y)|^2\right)^{1/2}\\ &= \left(\sum_{n=1}^{N}|a_n|^2\right)^{1/2}\left(\sum_{n=1}^{N}(2\pi n|a_n|)^2\right)^{1/2}\\ &\le 2\pi N\sum_{n=1}^{N}|a_n|^2.\end{aligned}$$

Therefore,

$$\sum_{i=1}^{r} |S(x_i)|^2 \le \left(\frac{1}{\delta} + 2\pi N\right) \sum_{n=1}^{N} |a_n|^2 .$$

#33(2007)

2. Arithmetic version

Let $a_{M+1}, \dots, a_{M+N} \in \mathbb{C}$ and put $S(q,a) = \sum_{\substack{M<n\le M+N \\ n\equiv a \pmod q}} a_n$.

e.g. if A is a finite set of integers $\subseteq \{M+1, \dots, M+N\}$, $a_n = \begin{cases} 1 & n\in A \\ 0 & n\notin A \end{cases}$,

then $S(q,a)$ is the number of elements of A in the residue class $a \bmod q$.

Theorem 6.2 For any $Q\ge 1$,

$$(6.3)\quad \sum_{q\le Q} q \sum_{a=1}^{q} \left| \sum_{d\mid q} \frac{\mu(d)}{d} S(q/d, a)\right|^2 \le C(N+Q^2) \sum_{M<n\le M+N} |a_n|^2,$$

where C is the constant from Theorem 6.1.

Proof. For the points x_i, we take the Farey fractions

$$\left\{ \frac{a}{q} : 1\le q\le Q,\ 1\le a\le q,\ (a,q)=1 \right\} = \left\{ \frac{1}{Q}, \frac{1}{Q-1}, \dots, \frac{Q-1}{Q}, 1 \right\}.$$

Since $\left\| \frac{a}{q} - \frac{a'}{q'} \right\| \ge \frac{1}{qq'} \ge \frac{1}{Q^2}$ for any $\frac{a}{q} \ne \frac{a'}{q'}$, these points are δ-spaced with $\delta = \frac{1}{Q^2}$. By Theorem 6.1,

$$(6.4)\quad \sum_{q\le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left|S\left(\frac{a}{q}\right)\right|^2 \le C(N+Q^2) \sum_{n=M+1}^{M+N} |a_n|^2.$$

We must massage the left side of (6.4). For brevity, write $\sum_a^*$ for $\sum_{\substack{a=1 \\ (a,q)=1}}^{q}$.

We interpret $\sum_a^* |S(\frac{a}{q})|^2$ in terms of a discrete Parseval identity.

Let $T(q,h) = \sum_a^* S(\frac{a}{q}) e(\frac{-ha}{q})$. Then

$$\sum_{h=1}^{q} |T(q,h)|^2 = \sum_{h=1}^{q} \sum_a^* \sum_{a'}^* S(\tfrac{a}{q}) \overline{S(\tfrac{a'}{q})}\, e(-\tfrac{ha}{q}) e(\tfrac{ha'}{q})$$

$$= \sum_a^* \sum_{a'}^* S(\tfrac{a}{q}) S(\tfrac{-a'}{q}) \sum_{h=1}^{q} e\left(\frac{h(a'-a)}{q}\right) \qquad \text{inner sum} = \begin{cases} q & a=a' \\ 0 & a\neq a' \end{cases}$$

$$= q \sum_a^* |S(\tfrac{a}{q})|^2.$$

Using the identity for Ramanujan sums

$$c_q(n) = \sum_a^* e(\tfrac{an}{q}) = \sum_{d|(q,n)} d\mu(\tfrac{q}{d}),$$

we have

$$T(q,h) = \sum_a^* S(\tfrac{a}{q}) e(\tfrac{-ha}{q})$$

$$= \sum_n a_n \sum_a^* e\left(\frac{(n-h)a}{q}\right)$$

$$= \sum_n a_n c_q(n-h)$$

$$= \sum_n a_n \sum_{d|(q,n-h)} d\mu(\tfrac{q}{d}) \qquad f = q/d$$

$$= \sum_n a_n \sum_{\substack{f|q \\ \frac{q}{f}|(n-h)}} \frac{q}{f}\mu(f)$$

$$= q \sum_{f|q} \frac{\mu(f)}{f} \sum_{n\equiv h \,(\mathrm{mod}\, q/f)} a_n$$

$$= q \sum_{f|q} \frac{\mu(f)}{f} S(q/f, h).$$

Therefore, the left side of (6.4) is

$$\sum_{q\le Q} \frac{1}{q} \sum_{h=1}^{q} |T(q,h)|^2 = \sum_{q\le Q} q \left| \sum_{f|q} \frac{\mu(f)}{f} S(q/f,h)\right|^2,$$

as desired.

Corollary 6.3

We have

$$(6.5)\quad \sum_{p\le\sqrt{N}} \frac{1}{p} \sum_{a=1}^{p} \left| \frac{p}{N} \sum_{\substack{n\equiv a \pmod p\\ M<n\le N+M}} a_n - \frac{1}{N} \sum_{M<n\le N+M} a_n \right|^2 \le \frac{2C}{N} \sum_n |a_n|^2 .$$

Proof. Take $Q=\sqrt{N}$ and restrict the sum over q in (6.3) to prime q only. Then divide through by N^2.

#27 Remarks Writing $D(p,a) = \frac{p}{N} \sum_{\substack{M<n\le N+M\\ n\equiv a \pmod p}} a_n - \frac{1}{N}\sum_{M<n\le M+N} a_n$, the left side of (6.5) becomes

$$\sum_{p\le\sqrt{N}} \frac{1}{p} \sum_{a=1}^{p} |D(p,a)|^2 .$$

$D(p,a)$ is roughly the difference between the average of a_n over $n\equiv a \pmod p$ and the average over all a_n. Corollary 6.3 then says that $D(p,a)$ is small for "most" a and p.

4-22-11. #35 An important case is when a_n is the characteristic function of a set $\mathcal{N} \subseteq \{M+1,\dots,M+N\}$. Write

$$Z = |\mathcal{N}|,\quad Z(q,a) = |\{n\in\mathcal{N} : n\equiv a \pmod q\}| .$$

Corollary 6.4 For any $Q\ge 1$,

$$\sum_{q\le Q} q \sum_{a=1}^{q} \left| \sum_{d|q} \frac{\mu(d)}{d} Z\left(\frac{q}{d}, a\right) \right|^2 \le C\,(N+Q^2) Z .$$

Also

$$(6.6)\quad \sum_{p\le Q} \frac{1}{p} \sum_{a=1}^{p} |p Z(p,a) - Z|^2 \le C(N+Q^2) Z .$$

If $Q=\sqrt{N}$, (6.6) says roughly that on average over p and a,

$$|pZ(p,a)-Z| \ll \sqrt{Z N^{1/2}\log N} \ll N^{3/4}\sqrt{\log N},$$

i.e., for most a and p, $Z(p,a) \approx \frac{Z}{p}$, so $\mathcal{N}$ contains the expected number of elements in the residue class $a \bmod p$. If $|pZ(p,a)-Z|$ is large for many a and p, (6.6) implies that Z must be small.

#34(2007)

Theorem 6.5 (Large Sieve – Sieve version)
Let $\mathcal{N} \in \{M+1, \dots, M+N\}$ and define $Z, Z(q,a)$ as above. Suppose, for each prime p, there are $\rho(p)$ residue classes $a \bmod p$ with $Z(p,a)=0$. Assume $\rho(p)<p$ for all p and for square free q, write

$$h(q) = \prod_{p \mid q} \frac{\rho(p)}{p-\rho(p)}.$$

Then

$$Z \le \frac{c(N+Q^2)}{J} \quad ; \; J = \sum_{q \le Q} \mu^2(q) h(q) \qquad \left(= G(Q) \text{ from Selberg sieve}\right)$$

Remarks if $\rho(p)=p$ for some p, then $Z=0$.
Theorem 6.5 is very similar to Selberg's sieve (Theorem 15), and both give roughly the same strength results when $\rho(p)$ is bounded on average. When $\rho(p)$ is quite large, the error term in Selberg's sieve is diffucult to manage, while the error in Theorem 6.5 (the Q^2 term) is quite easy.

Proof. We shall prove that for any $a_{M+1}, \dots, a_{M+N} \in \mathbb{C}$, s.t. $S(p,a)=0$ for $\rho(p)$ a-values

$$(6.7) \qquad \sum_a{}^{*} \left|S\left(\tfrac{a}{q}\right)\right|^2 \ge S(0)^2 h(q). \qquad (\mu^2(q)=1).$$

Then, by (6.4),

$$c(N+Q^2) Z \ge \sum_{\substack{q \le Q \\ \mu^2(q)=1}} Z^2 h(q),$$

as desired. First we show (6.7) when $q=p$, p a prime. From the proof of Theorem 6.2,

$$\sum_a{}^{*} \left|S\left(\tfrac{a}{p}\right)\right|^2 = \frac{1}{p} \sum_{h=1}^{p} |T(p,h)|^2,$$

where $T(p,h) = p\left(S(p,h) - \frac{1}{p}S\right)$, $S = S(1,1) = \sum_n a_n$. Then

$$\sum_a{}^{*} \left|S\left(\tfrac{a}{p}\right)\right|^2 = p \sum_{h=1}^{p} \left|S(p,h) - \frac{S}{p}\right|^2 = p \sum_{h=1}^{p} |S(p,h)|^2 - 2\,\mathrm{Re}\left[S \sum_{h=1}^{p} S(p,h)\right] + |S|^2$$

$$\ge p \sum_{h=1}^{p} |S(p,h)|^2 - |S|^2.$$

By Cauchy–Schwarz,

$$|S|^2 = \left|\sum_{h=1}^{p} S(p,h)\right|^2 = \left|\sum_{\substack{1\le h\le p\\ S(p,h)\neq 0}} S(p,h)\right|^2$$

$$\le \Big(\sum_{\substack{1\le h\le p\\ S(p,h)\neq 0}} 1\Big)\Big(\sum_{1\le h\le p} |S(p,h)|^2\Big) \le (p-\rho(p)) \sum_{h=1}^{p} |S(p,h)|^2.$$

Thus $$\sum_a{}^{*} |S(\tfrac{a}{p})|^2 \geq \frac{p}{p-\rho(p)}|S|^2 - |S|^2 = h(p)|S|^2 = h(p)|S(0)|^2.$$

#28

Next, suppose (6.7) holds for $q=r$ and $q=s$, where $(r,s)=1$.
Every c, $1\le c\le rs$, $(c,rs)=1$ may be written uniquely as $c\equiv er+fs \pmod{rs}$
with $1\le e\le s$, $1\le f\le r$, $(e,s)=1$, $(f,r)=1$. Then

$$\sum_{\substack{1\le c\le rs\\ (c,rs)=1}} |S(\tfrac{c}{rs})|^2 = \sum_{\substack{1\le e\le s\\ (e,s)=1}} \sum_{\substack{1\le f\le r\\ (f,r)=1}} |S(\tfrac{e}{s}+\tfrac{f}{r})|^2.$$

Since (6.7) holds with $q=s$ and all sets $a_{M+1},\dots,a_{M+N}$ of complex numbers, it holds with a_n replaced by $a_n e^{2\pi i n f/r}$, i.e.,

$$\sum_{\substack{1\le e\le s\\ (e,s)=1}} |S(\tfrac{e}{s}+\tfrac{f}{r})|^2 = \sum_{\substack{1\le e\le s\\ (e,s)=1}} |S^*(e/s)|^2 \quad ; \quad S^*(x) = \sum_n \left(a_n e(\tfrac{nf}{r})\right) e(nx)$$

$$\geq h(s)\,|S^*(0)|^2 = h(s)\,|S(f/r)|^2.$$

Thus $$\sum_{\substack{1\le c\le rs\\ (c,rs)=1}} |S(\tfrac{c}{rs})|^2 \geq h(s) \sum_{\substack{1\le f\le r\\ (f,r)=1}} |S(\tfrac{f}{r})|^2 \geq h(s) g(r)\,|S(0)|^2,$$

i.e. (6.7) holds with $q=rs$. By induction on the number of prime factors of q, (6.7) holds for all square free q ∎

4-25-11. #36

App. primes in $(x-y, x]$, Brun–Titchmarsh thm

Applications

A. "pseudo-squares". Suppose $\mathcal{N} \subseteq \{M+1, \dots, M+N\}$, and for $3 \le p \le \sqrt{N}$, $\mathcal{N}$ avoids $\frac{p-1}{2}$ residue classes modulo p, and let $Z = |\mathcal{N}|$. In the notation of Theorem 6.5, for odd squarefree q,

$$h(q) = \prod_{p \mid q} \frac{\frac{p-1}{2}}{\frac{p+1}{2}} = \frac{\phi(q)}{\sigma(q)}$$

Take $Q = \sqrt{N}$. By Theorem 6.5,

$$Z \le \frac{2CN}{L}, \quad L \ge \sum_{\substack{q \le Q \\ q \text{ odd}}} \frac{\mu^2(q)\phi(q)}{\sigma(q)} \gg Q = \sqrt{N}.$$

Hence

(6.8) $$Z \ll \sqrt{N}.$$

An example of such a set $\mathcal{N}$ is the set of squares $\le N$. The $\frac{p-1}{2}$ residue classes which $\mathcal{N}$ avoids are those corresponding to quadratic nonresidues mod p. So (6.8) gives the correct order of Z. The power of (6.8) is that it remains true no matter which residue classes are avoided.

[redacted]

#35 (2007)

#29

(omit 2011)

B. (Heilbronn, 1958). Average of $\left(\frac{p}{p'}\right)$ over primes p, p'.

<u>Theorem</u> Suppose $Q \ge 3$. Then

$$\left| \sum_{3 \le p \le Q} \sum_{3 \le p' \le Q} \left(\frac{p'}{p}\right) \right| \ll Q^{7/4} (\log Q)^{-5/4}.$$

{First, "try" to separate p' into res classes mod p}

<u>Remark</u>. The trivial bound is $\pi(Q)^2 \ll Q^2 (\log Q)^{-2}$.

<u>Proof</u>. Denote by H the double sum on the left side. By Cauchy–Schwarz,

$$H^2 \le \left(\sum_{3 \le p \le Q} 1 \right) \left(\sum_{3 \le p \le Q} \left| \sum_{3 \le p' \le Q} \left(\frac{p'}{p}\right) \right|^2 \right)$$

$$\le \pi(Q) \sum_{3 \le p \le Q} \sum_{\substack{3 \le p' \le Q \\ 3 \le p'' \le Q}} \left(\frac{p'}{p}\right)\left(\frac{p''}{p}\right)$$

$$\le \pi(Q) \sum_{3 \le p \le Q} \left\{ \pi(Q) + 2 \sum_{3 \le p' < p'' \le Q} \left(\frac{p' p''}{p}\right) \right\}.$$

Let $\mathcal{N} = \{p'p'' : 3 \le p' < p'' \le Q\} \subseteq [1, Q^2]$, so $Z = |\mathcal{N}| = \frac{1}{2}\pi(Q)(\pi(Q)-1)$. Then

$$H^2 \le \pi(Q)^3 + 2\pi(Q) \sum_{3 \le p \le Q} \left| \sum_{n \in \mathcal{N}} \left(\frac{n}{p}\right) \right|.$$

By Cauchy–Schwarz again,

$$\sum_{3 \le p \le Q} \left| \sum_{n \in \mathcal{N}} \left(\frac{n}{p}\right) \right| \le \pi(Q)^{\frac{1}{2}} \left\{ \sum_{3 \le p \le Q} \left(\sum_{n \in \mathcal{N}} \left(\frac{n}{p}\right) \right)^2 \right\}^{1/2}.$$

Using $\sum_{h=1}^{p} \left(\frac{h}{p}\right) = 0$, we have

$$\sum_{n \in \mathcal{N}} \left(\frac{n}{p}\right) = \sum_{h=1}^{p} \sum_{\substack{n \in \mathcal{N} \\ n \equiv h \ (\mathrm{mod}\ p)}} \left(\frac{n}{p}\right) = \sum_{h=1}^{p} \left(\frac{h}{p}\right) Z(p,h)$$

$$= \sum_{h=1}^{p} \left(\frac{h}{p}\right) \left(Z(p,h) - \frac{Z}{p} \right).$$

By another application of Cauchy-Schwarz,

$$\left(\sum_{n \in \mathcal{N}} \left(\frac{n}{p}\right) \right)^2 \le \left(\sum_{h=1}^{p} \left(\frac{h}{p}\right)^2 \right) \left(\sum_{h=1}^{p} |Z(p,h) - Z/p|^2 \right)$$

$$\le p \sum_{h=1}^{p} |Z(p,h) - Z/p|^2.$$

Hence

$$H^2 \le \pi(Q)^3 + 2\pi(Q)^{3/2} \left\{ \sum_{3 \le p \le Q} p \sum_{h=1}^{p} |Z(p,h) - Z/p|^2 \right\}^{1/2}.$$

By Corollary 6.4, (6.6), the expression in braces is $\le 2CQ^2 Z \le CQ^2 \pi(Q)^2$.

Hence $$H^2 \ll \left(\frac{Q}{\log Q}\right)^3 + \left(\frac{Q}{\log Q}\right)^{3/2} \left(Q^4 / \log^2 Q \right)^{1/2} \ll \frac{Q^{7/2}}{(\log Q)^{5/2}} \blacksquare$$

C. Least quadratic non-residue modulo a prime

$$n(p) = \min \left\{ n \ge 1 : \left(\frac{n}{p}\right) = -1 \right\}$$

estimates:

$n(p) \ll \sqrt{p} \log p$ (from Polya – Vinogradov Thm)

$n(p) \ll_\varepsilon p^{\frac{1}{4\sqrt{e}} + \varepsilon}$ (best known: Burgess est. + "Vinogradov trick")

$n(p) \ll (\log p)^2$ (Ankeny; assumes ERH for Dirichlet L-funct.)

Theorem 6.6 (Linnik)

Fix $\varepsilon>0$. There is a constant $c(\varepsilon)$ so that for all $N\geq 3$,

$$\left|\{3\leq p\leq N : n(p)>N^{\varepsilon}\}\right|\leq c(\varepsilon).$$

Corollary For any fixed $\varepsilon>0$,

$$\left|\{3\leq p\leq N : n(p)>p^{\varepsilon}\}\right| \ll_{\varepsilon} \log\log N.$$

Pf of Corollary

Define J by $N^{2^{-J}}\leq e < N^{2^{-J+1}}$, so that $J=\left\lfloor \frac{\log\log N}{\log 2}\right\rfloor+1$. Then

$$\begin{aligned}\left|\{3\leq p\leq N : n(p)>p^{\varepsilon}\}\right| &= \sum_{j=1}^{J}\left|\{N^{2^{-j}}<p\leq N^{2^{-j+1}} : n(p)>p^{\varepsilon}\}\right| \\ &\leq \sum_{j=1}^{J}\left|\{p\leq N^{2^{-j+1}} : n(p)>(N^{2^{-j+1}})^{\varepsilon/2}\}\right| \\ &\leq c(\tfrac{\varepsilon}{2})J \ll_{\varepsilon} \log\log N.\end{aligned}$$

Proof of Theorem 6.6

Apply Theorem 6.5 with the set $\mathcal{N}=\{1\leq n\leq N^2 : P^+(n)\leq N^{\varepsilon}\}$.
If $p\geq 3$ and $n(p)>N^{\varepsilon}$, then $\left(\frac{q}{p}\right)=1$ for primes $q\leq N^{\varepsilon}$. Hence, $\left(\frac{n}{p}\right)=1$ for all $n\in\mathcal{N}$. Hence $\mathcal{N}$ avoids $\frac{p-1}{2}=\rho(p)$ residue classes mod p, for every such prime p. Take $Q=N$. Also

$$L=\sum_{q\leq Q}\prod_{p\mid q}\frac{\rho(p)}{p-\rho(p)} \geq \sum_{\substack{3\leq p\leq N\\ n(p)>N^{\varepsilon}}}\frac{p-1}{p+1}\geq \frac{1}{2}\#\{3\leq p\leq N : n(p)>N^{\varepsilon}\}.$$

Theorem 6.5 gives

$$|\mathcal{N}|\leq \frac{c(N^2+Q^2)}{L}\leq \frac{4N^2}{\#\{3\leq p\leq N : n(p)>N^{\varepsilon}\}}.$$

On the other hand, $|\mathcal{N}|=\Psi(N^2,N^{\varepsilon})\gg_{\varepsilon} N^2$ by Theorem Ψ.
and the theorem follows.

3. Character sum version of large sieve, Bombieri-Vinogradov Theorem

Recall that a Dirichlet character χ mod q is <u>primitive</u> if there is no character ψ mod q_1, $q_1 | q$, $q_1 < q$, so that $\chi = \psi \chi_0$, where χ_0 is the principal character mod q. Equivalently, for all $q_1 | q$, $q_1 < q$, there is an l so that $\chi(lq_1 + 1) \notin \{0, 1\}$.

<u>Lemma 6.2</u> If χ is a primitive character mod $q > 1$, then for any n,

$$\chi(n) \tau(\bar{\chi}) = \sum_{h=1}^{q} \bar{\chi}(h) e(nh/q),$$

where

$$\tau(\bar{\chi}) = \sum_{m=1}^{q} \bar{\chi}(m) e(m/q) = \sum_{\substack{m=1 \\ (m,q)=1}}^{q} \bar{\chi}(m) e(m/q)$$

is the Gauss sum for $\bar{\chi}$.

<u>Proof</u> If $(n,q)=1$, then

$$\chi(n) \tau(\bar{\chi}) = \sum_{m=1}^{q} \bar{\chi}(m) \chi(n) e(m/q) \qquad m \equiv nh \pmod{q}$$
$$= \sum_{h=1}^{q} \bar{\chi}(h) e\left(\frac{nh}{q}\right).$$

If $q | n$, both sides are zero since $\sum_{h=1}^{q} \bar{\chi}(h) = 0$. Suppose $(n,q) = d > 1$ and $q \nmid n$. Then $n = n_1 d$, $q = q_1 d$ and

$$\sum_{h=1}^{q} \bar{\chi}(h) e\left(\frac{nh}{q}\right) = \sum_{c=0}^{q_1 - 1} e\left(\frac{cn_1}{q_1}\right) \underbrace{\sum_{l=0}^{d-1} \bar{\chi}(q_1 l + c)}_{S(c)}.$$

Note $S(c + q_1) = S(c)$ (replace l with $l-1$). Thus, if $(v,q)=1$ and $v \equiv 1 \pmod{q_1}$ then

$$\bar{\chi}(v) S(c) = \sum_{l=0}^{d-1} \bar{\chi}(vq_1 l + vc) = \sum_{l'=0}^{d-1} \bar{\chi}(l' q_1 + vc) = S(vc) = S(c).$$

If $S(c) \neq 0$, then $\bar{\chi}(v) \in \{0,1\}$ for all such $v \Rightarrow \bar{\chi}$ is imprimitive. Hence $S(c) = 0$ for every c, hence

$$\sum_{h=1}^{q} \bar{\chi}(h) e\left(\frac{nh}{q}\right) = 0 = \chi(n) \tau(\bar{\chi}).$$

#36(2007)

Lemma 6.3 If χ is a primitive character mod q, then
$$|\tau(\chi)| = \sqrt{q}.$$

Proof By Lemma 6.2,
$$|\chi(n)|^2 |\tau(\bar\chi)|^2 = \sum_{h_1=1}^{q} \sum_{h_2=1}^{q} \bar\chi(h_1)\chi(h_2) e\left(\frac{n(h_1-h_2)}{q}\right).$$
Summing over $1 \le n \le q$ gives
$$\phi(q)|\tau(\bar\chi)|^2 = \sum_{h_1=1}^{q} \sum_{h_2=1}^{q} \bar\chi(h_1)\chi(h_2) \sum_{n=1}^{q} e\left(\frac{n(h_1-h_2)}{q}\right).$$
The sum on n is zero unless $h_1 = h_2$, in which case the sum is q. Hence
$$\phi(q)|\tau(\bar\chi)|^2 = q\sum_{h=1}^{q} |\bar\chi(h)|^2 = q\,\phi(q),$$
hence $|\tau(\bar\chi)| = \sqrt{q}$.

Theorem 6.7 (Polya; Vinogradov 1918)
For any nonprincipal Dirichlet character χ mod q, and any $A, B \in \mathbb{R}$,
$$\left|\sum_{A \le n \le B} \chi(n)\right| \ll \sqrt{q}\log q.$$

Proof (For primitive characters)
By Lemma 6.2,
$$\sum_{A \le n \le B} \chi(n) = \frac{1}{\tau(\bar\chi)} \sum_{h=1}^{q-1} \bar\chi(h) \sum_{A \le n \le B} e\left(\frac{nh}{q}\right).$$
Next,
$$\left|\sum_{A\le n\le B} e\left(\frac{nh}{q}\right)\right| = \left|\frac{e\left(\frac{h}{q}(\lfloor B\rfloor - \lceil A\rceil + 1)\right) - 1}{e(h/q) - 1}\right| \le \frac{2}{|e(h/q) - 1|} \le \frac{1}{2\|h/q\|},$$
where $\|x\|$ = distance from x to the nearest integer. Therefore,
$$\left|\sum_{A\le n\le B} \chi(n)\right| \le \frac{1}{|\tau(\bar\chi)|} \sum_{h=1}^{q-1} \frac{1}{2\|h/q\|}$$
$$= \frac{1}{2\sqrt{q}}\left(\sum_{1\le h\le q/2} \frac{q}{h} + \sum_{q/2 < h \le q-1} \frac{q}{q-h}\right)$$
$$\le \frac{q}{2\sqrt{q}}\left(\log\frac{q}{2} + 1 + \log\frac{q}{2} + 1\right) \ll \sqrt{q}\log q.$$

Corollary
(i) $n(p) \ll \sqrt{p}\log p$ (show details)
(ii) $n(p) \ll_\varepsilon p^{\frac{1}{2\sqrt{e}}+\varepsilon}$ for all $\varepsilon > 0$ (exercise)

Let $C(q)$ = set of Dirichlet characters modulo q

$C^*(q)$ = set of primitive characters $\in C(q)$.

Theorem 6.8 Let $a_{M+1}, \ldots, a_{M+N} \in \mathbb{C}$ and put

$$\mathcal{U}(\chi) = \sum_{M+1 \le n \le M+N} a_n \chi(n).$$

For any $Q \ge 1$, we have

$$\sum_{q \le Q} \frac{q}{\phi(q)} \sum_{\chi \in C^*(q)} |\mathcal{U}(\chi)|^2 \le C(N+Q^2) \sum_{M+1 \le n \le M+N} |a_n|^2.$$

Proof. Apply Lemma 6.2 and sum over n:

$$\tau(\bar{\chi})\mathcal{U}(\chi) = \sum_{h=1}^{q} \bar{\chi}(h) \sum_{M+1 \le n \le M+N} a_n e\left(\frac{nh}{q}\right) = \sum_{h=1}^{q} \bar{\chi}(h) S(h/q),$$

where $$S(x) = \sum_{M+1 \le n \le M+N} a_n e(nx).$$

Therefore,

$$\sum_{\chi \in C^*(q)} |\tau(\bar{\chi})\mathcal{U}(\chi)|^2 = \sum_{\chi \in C^*(q)} \left| \sum_{h=1}^{q} \bar{\chi}(h) S(h/q) \right|^2$$

$$\le \sum_{\chi \in C(q)} \left| \sum_{h=1}^{q} \bar{\chi}(h) S(h/q) \right|^2$$

$$= \sum_{\substack{h_1, h_2 = 1 \\ (h_i, q) = 1}}^{q} S\left(\frac{h_1}{q}\right) \overline{S\left(\frac{h_2}{q}\right)} \sum_{\chi \in C(q)} \bar{\chi}(h_1) \chi(h_2).$$

By orthogonality, the inner sum is 0 unless $h_1 = h_2$, in which case the sum is $\phi(q)$. Applying Lemma 6.3,

$$q \sum_{\chi \in C^*(q)} |\mathcal{U}(\chi)|^2 \le \phi(q) \sum_{\substack{h=1 \\ (h,q)=1}}^{q} |S(h/q)|^2.$$

By Theorem 6.1,

$$\sum_{q \le Q} \frac{q}{\phi(q)} \sum_{\chi \in C^*(q)} |\mathcal{U}(\chi)|^2 \le \sum_{q \le Q} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} |S(h/q)|^2 \le C(N+Q^2) \sum_{M+1 \le n \le M+N} |a_n|^2.$$

#37(2007)

Theorem 6.9 (Large sieve; character version with bilinear forms)

For any complex numbers $a_1, \ldots, a_M, b_1, \ldots, b_N$ and any $Q \geq 1$, we have

$$\sum_{q \leq Q} \frac{q}{\phi(q)} \sum_{\chi \in C^*(q)} \max_u \Big| \sum_{\substack{m=1 \\ mn \leq u}}^{M} \sum_{n=1}^{N} a_m b_n \chi(mn) \Big| \tag{6.9}$$
$$\ll (M^{\frac{1}{2}} + Q)(N^{\frac{1}{2}} + Q) \Big(\sum_{m=1}^{M} |a_m|^2 \Big)^{\frac{1}{2}} \Big(\sum_{n=1}^{N} |b_n|^2 \Big)^{\frac{1}{2}} \log(2MN).$$

Remark. double sum on m,n is $\sum_{c \leq u} f * g(c)$, $f(m) = a_m \chi(m)$, $g(n) = b_n \chi(n)$.

Proof. To handle the condition $mn \leq u$, recall an identity used in a truncated version of Perron's formula:

$$\frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{y^s}{s} ds = \delta(y) + O\Big(\frac{y^c}{T |\log y|} \Big) \qquad (c > 0, y > 0, y \neq 1, T \geq 1)$$

where $\delta(y) = \begin{cases} 1 & 0 < y < 1 \\ 0 & y > 1 \end{cases}$. WLOG $u = u_0 + \frac{1}{2}$, $u_0 \in \mathbb{Z}$, $0 \leq u_0 \leq MN$.

Then
$$\sum_{\substack{m=1 \\ mn \leq u}}^{M} \sum_{n=1}^{N} a_m b_n \chi(mn) = \sum_{m=1}^{M} \sum_{n=1}^{N} a_m b_n \chi(mn) \delta\Big(\frac{u}{mn}\Big)$$
$$= \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{u^s}{s} \underbrace{\Big(\sum_{m=1}^{M} a_m \chi(m) m^{-s} \Big)}_{A(s,\chi)} \underbrace{\Big(\sum_{n=1}^{N} b_n \chi(n) n^{-s} \Big)}_{B(s,\chi)} ds$$
$$+ O\Big(\frac{1}{T} \sum_{m,n} \frac{(u/mn)^c}{|\log u/mn|} |a_m b_n| \Big).$$

In the error term,
$$\Big|\log \frac{u}{mn}\Big| \gg \frac{1}{mn} \gg \frac{1}{MN}.$$

Put $c = \frac{1}{\log(2MN)}$, so that $|u^s| \ll 1$ and $(u/mn)^c \ll 1$. Then the left side above is
$$\ll \int_{c-iT}^{c+iT} \frac{1}{|s|} |A(s,\chi)| \cdot |B(s,\chi)| \, |ds| + \frac{MN}{T} \sum_{m,n} |a_m b_n|$$

<u>uniformly in u.</u> Hence, the left side of (6.9) is, by the Cauchy-Schwarz inequality,

$$\ll \int_{c-iT}^{c+iT} \frac{1}{|s|} \Big(\sum_{q \leq Q} \frac{q}{\phi(q)} \sum_{\chi \in C^*(q)} |A(s,\chi)|^2 \Big)^{\frac{1}{2}} \Big(\sum_{q \leq Q} \frac{q}{\phi(q)} \sum_{\chi \in C^*(q)} |B(s,\chi)|^2 \Big)^{1/2} ds$$
$$+ \underbrace{\sum_{q \leq Q} \frac{q}{\phi(q)} \sum_{\chi \in C^*(q)}}_{O(Q^2)} \frac{(MN)^{\frac{3}{2}}}{T} \Big(\sum_m |a_m|^2 \Big)^{1/2} \Big(\sum_n |b_n|^2 \Big)^{1/2}.$$

By Theorem 6.8,

$$\sum_{q \le Q} \frac{q}{\phi(q)} \sum_{\chi \in C^*(q)} |A(s,\chi)|^2 \le C(M+Q^2) \sum_{m=1}^{M} |a_m m^{-s}|^2 \ll (M+Q^2) \sum_{m=1}^{M} |a_m|^2$$

and similarly

$$\sum_{q \le Q} \frac{q}{\phi(q)} \sum_{\chi \in C^*(q)} |B(s,\chi)|^2 \ll (N+Q^2) \sum_{n=1}^{N} |b_n|^2 .$$

Finally, $\displaystyle\int_{c-iT}^{c+iT} \frac{|ds|}{|s|} = \int_{-T}^{T} \frac{dt}{|c+it|} \le \frac{2}{c} + 2\int_1^T \frac{dt}{t} \le 2\log(2TMN).$

Therefore, the left side of (6.9) is

$$\ll \left(\sum_{m=1}^{M} |a_m|^2\right)^{\frac{1}{2}} \left(\sum_{n=1}^{N} |b_n|^2\right)^{\frac{1}{2}} \left((M+Q^2)^{\frac{1}{2}}(N+Q^2)^{\frac{1}{2}} \log(2TMN) + Q^2 \frac{(MN)^{\frac{3}{2}}}{T}\right).$$

Taking $T = (MN)^{\frac{3}{2}}$ completes the proof ∎

<u>Theorem BV</u> (Bombieri; A.I. Vinogradov, 1965)

For every $A > 0$ there is a B so that

$$\sum_{q \le x^{\frac{1}{2}}(\log x)^{-B}} \max_{(a,q)=1} \max_{y \le x} \left| \pi(y;q,a) - \frac{li(y)}{\phi(q)} \right| \ll \frac{x}{(\log x)^A}.$$

<u>Theorem BV*</u>

For every $A > 0$ there is a B so that

$$\sum_{q \le x^{\frac{1}{2}}(\log x)^{-B}} \max_{(a,q)=1} \max_{y \le x} \left| \psi(y;q,a) - \frac{y}{\phi(q)} \right| \ll \frac{x}{(\log x)^A}, \qquad \psi(y;q,a) = \sum_{\substack{n \le y \\ n \equiv a \pmod q}} \Lambda(n).$$

<u>Exercise</u> Show Theorems BV, BV* are equivalent.

Let $\psi(y,\chi) = \sum_{n\le y} \chi(n)\Lambda(n)$

Lemma 6.4 For $1 \le Q \le X$,

$$\sum_{q\le Q} \max_{(a,q)=1} \max_{y\le X} \left|\psi(y;q,a) - \frac{y}{\phi(q)}\right| \ll Q\log^2 X + Xe^{-c\sqrt{\log X}} + \log X \sum_{2\le q\le Q} \frac{1}{\phi(q)} \sum_{\chi\in C^*(q)} \max_{y\le X} |\psi(y,\chi)|.$$

Here $c>0$ is a constant.

Proof Start with the orthogonality relation

$$\psi(y;q,a) = \frac{1}{\phi(q)} \sum_{\chi\in C(q)} \overline{\chi}(a)\psi(y,\chi),$$

which implies

$$\left|\psi(y;q,a) - \frac{y}{\phi(q)}\right| \le \frac{1}{\phi(q)}\Big(|\psi(y,\chi_0)-y| + \sum_{\substack{\chi\in C(q)\\ \chi\ne\chi_0}} |\psi(y,\chi)|\Big).$$

Now reduce the problem to sums $\psi(y,\chi)$ with χ primitive. For general $\chi\in C(q)$, if χ is induced by the primitive character $\chi_1 \bmod q_1$, then $\chi(p)=\chi_1(p)$ for all primes p except those with $p|q, p\nmid q_1$. Hence

$$|\psi(y,\chi) - \psi(y,\chi_1)| \le \sum_{\substack{p^k\le y\\ p|q, p\nmid q_1}} \log p \le \sum_{p|q, p\nmid q_1} \log p \cdot \left\lfloor \frac{\log y}{\log p}\right\rfloor$$
$$\ll \log q \cdot \log y \ll \log^2 X.$$

Setting $E^*(X,q) = \max_{(a,q)=1} \max_{y\le X} \left|\psi(y;q,a) - \frac{y}{\phi(q)}\right|$, we obtain

$$E^*(X,q) \le \max_{y\le X} \frac{1}{\phi(q)}\Big[|\psi(y)-y| + \sum_{\substack{\chi\in C(q)\\ \chi\ne\chi_0}} |\psi(y,\chi_1)| + O(\phi(q)\log^2 X)\Big]$$
$$\ll \log^2 X + \frac{Xe^{-c_0\sqrt{\log X}}}{\phi(q)} + \frac{1}{\phi(q)} \max_{y\le X} \sum_{\substack{\chi\ne\chi_0\\ \chi\in C(q)}} |\psi(X;\chi_1)|$$

by the Prime Number Theorem, where $c_0>0$ is a constant. A given $\chi_1 \bmod q_1$ induces characters $\chi \bmod q$ only for $q_1|q$. Hence

$$\sum_{q\le Q} E^*(X,q) \ll Q\log^2 X + Xe^{-c_0\sqrt{\log X}} \underbrace{\sum_{q\le Q}\frac{1}{\phi(q)}}_{O(\log Q)} + \sum_{2\le q_1\le Q} \sum_{\chi_1\in C^*(q_1)} \max_{y\le X} |\psi(y,\chi_1)| \cdot \underbrace{\sum_{\ell\le Q/q} \frac{1}{\phi(\ell q_1)}}_{O\left(\frac{\log Q}{\phi(q)}\right)}.$$

Lastly, $\phi(\ell q) \ge \phi(\ell)\phi(q)$ and

$$\sum_{m\le Z} \frac{1}{\phi(m)} \le \sum_{P^+(m)\le Z} \frac{1}{\phi(m)} = \prod_{p\le Z}\left(1 + \frac{1}{p-1} + \frac{1}{p(p-1)} + \cdots\right) = \prod_{p\le Z}\left(1-\frac{1}{p}\right)^{-1}\left(1+\frac{1}{p^2-p}\right)$$
$$\ll \log Z.$$

#38(2007)

Theorem SW (Siegel-Walfisz theorem)

For any fixed $C>0$, and uniformly for primitive χ mod q, $q \le (\log y)^C$, we have

$$|\psi(y,\chi)| \ll_C y e^{-c'\sqrt{\log y}}, \quad c' \text{ depends on } C,\ c'>0.$$

Remark For $C>1$, the implied constant is ineffective - it depends on C only, but a specific value cannot be found. For a proof, see H. Davenport, Multiplicative number thery.

Corollary. For any $C>0$,

$$\sum_{2\le q\le(\log x)^C} \frac{1}{\phi(q)} \sum_{\chi\in C^*(q)} \max_{y\le x} |\psi(y,\chi)| \ll_C x e^{-c''\sqrt{\log x}}, \text{ where } c''>0 \text{ depends on } C.$$

Proof Write

$$\max_{y\le x}|\psi(y,\chi)| \le \psi(x^{1/2}) + \max_{x^{1/2}<y\le x} |\psi(y,\chi)|$$

and apply Theorem SW (with C replaced by $C+1$) to right side.

Prime Decomposition (subatomic theory)

basic example: $\Lambda * 1 = \log \Rightarrow \Lambda = \log * \mu$

as Dirichlet series: $-\frac{\zeta'}{\zeta}(s) = -\zeta'(s)\frac{1}{\zeta(s)}$.

more sophisticated decomposition: parameter $u>1$.

$$\Lambda(n) = \sum_{ab=n} \mu(a)\log b.$$

separately consider $a\le u$ and $a>u$.

when $a>u$, write $\log b = \sum_{c|b}\Lambda(c)$, separately consider $c>u$, $c\le u$:

If $n>u^2$, then

$$\sum_{\substack{ab=n\\ a>u}} \mu(a)\log b = \sum_{c|n}\Lambda(c)\sum_{\substack{a|n/c\\ a>u}}\mu(a) \qquad \text{inner sum 0 if } c>n/u$$

$$= -\sum_{\substack{c|n\\ c<n/u}}\Lambda(c)\sum_{\substack{a|n/c\\ a\le u}}\mu(a) \qquad \text{since } \sum_{a|n/c}\mu(a)=0 \text{ for } c<n.$$

(6.10)
$$= -\sum_{\substack{c|n\\ c\le u}}\Lambda(c)\sum_{\substack{a|n/c\\ a\le u}}\mu(a) - \sum_{\substack{c|n\\ u<c<n/u}}\Lambda(c)\sum_{\substack{a|n/c\\ a\le u}}\mu(a)$$

Lemma 6.5 Let χ be a primitive character of conductor $q \geq 2$, $y \geq 2$ and $U > 1$. Then

$$\psi(y,\chi) = -\sum_{\substack{bc \leq y \\ b \geq U,\, c \geq U}} \Lambda(c)\chi(bc) \sum_{\substack{a \mid b \\ a \leq U}} \mu(a) + O\left(U^2 q^{1/2} \log q \log y\right)$$

Proof If $y \leq U^2$, then the lemma follows from

$$|\psi(y,\chi)| \leq \sum_{n \leq y} \Lambda(n) \ll y \ll U^2.$$

Now let $y > U^2$. By (6.10), we have

$$\psi(y,\chi) = \psi_1 + \psi_2 + \psi_3 + \psi_4,$$

where

$$\psi_1 = \sum_{n \leq U^2} \chi(n)\Lambda(n) \ll U^2,$$

$$\psi_2 = \sum_{\substack{U^2 < ab \leq y \\ a \leq U}} \mu(a)\chi(a) \log b\, \chi(b) \ll \sum_{a \leq U} \Big| \sum_{U^2/a < b \leq y/a} \chi(b) \log b \Big|,$$

$$\psi_3 = -\sum_{\substack{a \leq U \\ c \leq U}} \Lambda(c)\mu(a)\chi(ac) \sum_{U^2/ac < b \leq y/ac} \chi(b), \qquad (n=abc)$$

$$\psi_4 = -\sum_{\substack{bc \leq y \\ c \geq U,\, b \geq U}} \Lambda(c)\chi(bc) \sum_{\substack{a \mid b \\ a \leq U}} \mu(a) \qquad (n=bc)$$

By the Polya–Vinogradov inequality (Theorem 6.7),

$$\sum_{A < b \leq B} \chi(b) \log b = \log B \cdot \sum_{b \leq B} \chi(b) - \log A \sum_{b \leq A} \chi(b) - \int_A^B \frac{1}{t} \sum_{b \leq t} \chi(b)\, dt$$

$$\ll \log B \max_t \Big| \sum_{b \leq t} \chi(b) \Big| \ll q^{\frac{1}{2}} \log q \log y.$$

Hence

$$|\psi_2| \ll U q^{\frac{1}{2}} \log q \log y.$$

Also by Theorem 6.7,

$$|\psi_3| \ll \sum_{c \leq U} \Lambda(c) \sum_{a \leq U} 1 \left(q^{1/2} \log q\right) \ll U^2 q^{\frac{1}{2}} \log q \;\blacksquare$$

Proof of Theorem BV

Start with Lemma 6.4. The corollary to Theorem SW takes care of the terms with $q \le (\log x)^c$. Suppose $x^{1/3} < Q \le x^{1/2}$, $1 < U \le Q$. By Lemma 6.5,

$$(6.11)\qquad \sum_{q\le Q} \max_{(a,q)=1} \max_{y\le x} \left|\psi(y;q,a) - \frac{y}{\phi(q)}\right| \ll x e^{-c'''\sqrt{\log x}} + \log x\,(D_1 + D_2),$$

where

$$D_1 = \sum_{2\le q\le Q} \frac{1}{\phi(q)} \sum_{\chi\in C^*(q)} U^2 q^{\frac12}\log q\,\log x \ll U^2 Q^{3/2}\log^2 x$$

and, using Theorem 6.9,

$$D_2 = \sum_{(\log x)^c \le q\le Q} \frac{1}{\phi(q)} \sum_{\chi\in C^*(q)} \max_{y\le x} \left| \sum_{\substack{bc\le y\\ b>U,\ c>U}} \Lambda(c)\chi(bc) \sum_{\substack{a|b\\ a\le U}} \mu(a)\right|$$

$$\ll \log^3 x \max_{(\log x)^c\le Q_0\le Q} \frac{1}{Q_0} \max_{\substack{U\le b_0\le \frac{x}{U}\\ U\le c_0\le\frac{x}{U}}} \sum_{Q_0<q\le 2Q_0} \frac{q}{\phi(q)} \sum_{\chi\in C^*(q)} \max_{y\le x} \left| \sum_{\substack{bc\le y\\ b_0<b\le 2b_0\\ c_0<c\le 2c_0}} \big(\Lambda(c)\chi(c)\big)\Big(\chi(b)\underbrace{\sum_{\substack{a|b\\ a\le U}}\mu(a)}_{\le \tau(b)}\Big)\right|$$

$$\ll \log^3 x \max_{Q_0, b_0, c_0} \frac{1}{Q_0}\left(b_0^{1/2}+Q_0\right)\left(c_0^{1/2}+Q_0\right)\Big(\sum_{c\le 2c_0}\Lambda(c)^2\Big)^{\frac12}\Big(\sum_{b\le 2b_0}\tau(b)^2\Big)^{\frac12}\log(8b_0c_0).$$

By Chebyshev's estimates,

$$\sum_{c\le 2c_0}\Lambda(c)^2 \ll c_0\log c_0.$$

Also,

$$\sum_{b\le 2b_0}\tau(b)^2 \le 2b_0\sum_{b\le 2b_0}\frac{\tau(b)^2}{b} \le 2b_0 \sum_{p^t(b)\le 2b_0}\frac{\tau(b)^2}{b}$$
$$= 2b_0\prod_{p\le 2b_0}\left(1+\frac4p+\frac{9}{p^2}+\frac{16}{p^3}+\cdots\right) \ll b_0(\log b_0)^4.$$

Thus,

$$D_2 \ll (\log x)^{\frac{13}{2}} \max_{Q_0,b_0,c_0} \frac{(b_0c_0)^{1/2}}{Q_0}\left((b_0c_0)^{1/2} + (b_0^{1/2}+c_0^{1/2})Q_0 + Q_0^2\right) \qquad \left(\begin{matrix} b_0c_0 \ll x \\ b_0^{1/2}+c_0^{1/2} \ll (x/U)^{1/2}\end{matrix}\right)$$

$$\ll (\log x)^{\frac{13}{2}} \max_{Q_0}\left(\frac{x}{Q_0} + \frac{x}{U^{1/2}} + x^{1/2}Q_0\right)$$

$$\ll (\log x)^{\frac{13}{2}}\left(\frac{x}{(\log x)^c} + \frac{x}{U^{1/2}} + x^{1/2}Q\right)$$

The left side of (6.11) is therefore

$$\ll \frac{x}{(\log x)^{c-15/2}} + \frac{x(\log x)^{15/2}}{U^{1/2}} + x^{1/2}(\log x)^{15/2}Q + U^2Q^{3/2}\log^3 x.$$

Take $c = A + 15/2$, $U = (\log x)^{2A+15}$, $Q = x^{1/2}(\log x)^{-B}$, $B = A + 15/2$, and the above is $O(x/(\log x)^A)$.

#39(2007

Theorem BDH (Barban; Davenport – Halberstam (1966))

For any $A>0$, uniformly for $x/(\log x)^A \le Q \le x$, we have

$$\sum_{q\le Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left(\psi(x;q,a) - \frac{x}{\phi(q)}\right)^2 \ll xQ\log^2 x. \tag{6.12}$$

Proof Let $\psi'(x,\chi)=\psi(x,\chi)$ if χ is nonprincipal, and $\psi'(x,\chi_0)=\psi(x,\chi_0)-x$.

Start with $\psi(x;q,a) - \frac{x}{\phi(q)} = \frac{1}{\phi(q)} \sum_{\chi\in C(q)} \overline{\chi}(a)\psi'(x,\chi)$,

square both sides and sum over a:

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} \left(\psi(x;q,a)-\frac{x}{\phi(q)}\right)^2 = \frac{1}{\phi^2(q)} \sum_{\chi_1,\chi_2\in C(q)} \psi'(x,\chi_1)\psi'(x,\overline{\chi}_2) \sum_{a=1}^{q} \overline{\chi}_1(a)\chi_2(a)$$

$$= \frac{1}{\phi(q)} \sum_{\chi\in C(q)} |\psi'(x,\chi)|^2.$$

If χ is induced by primitive χ_1, then (cf. proof of Lemma 6.4)

$$\psi'(x,\chi) = \psi'(x,\chi_1) + O(\log^2 x).$$

Summing on $q\le Q$ we obtain

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q} \left|\psi(x;q,a)-\frac{x}{\phi(q)}\right|^2 = \sum_{q\le Q}\frac{1}{\phi(q)}\sum_{\chi\in C(q)} |\psi'(x,\chi_1)|^2 + O(xQ\log^2 x)$$

since $|\psi'(x,\chi_1)| \ll x$. The sum on the right is

$$\le \sum_{q_1\le Q} \frac{1}{\phi(q_1)} \sum_{\chi_1\in C^*(q_1)} |\psi'(x,\chi_1)|^2 \cdot \sum_{r\le Q/q_1} \frac{1}{\phi(r)}$$

$$\ll (\log x)\sum_{q_1\le(\log x)^A} \max_{\chi_1\in C^*(q_1)} |\psi'(x,\chi_1)|^2 + (\log x)\sum_{(\log x)^A<2^j\le Q} \frac{1}{2^j} \sum_{2^{j-1}<q_1\le 2^j} \frac{q_1}{\phi(q_1)} \sum_{\chi\in C^*(q)} |\psi(x,\chi)|^2.$$

By Theorem SW, the first sum on q_1 is $\ll x^2 e^{-c'\sqrt{\log x}}$, $c'>0$. By Theorem 6.8, the 2nd sum on q_1 is

$$\ll (x+2^{2j})\sum_{n\le x}\Lambda(n)^2 \ll (x+2^{2j})\,x\log x.$$

We find that the left side of (6.12) is

$$\ll xQ\log^2 x + (\log x)\sum_{(\log x)^A<2^j\le Q}\left(\frac{x^2\log x}{2^j} + 2^j x\log x\right) \ll xQ\log^2 x.$$

Remark. Montgomery (1970) showed that the left side of (6.12) is actually $\sim xQ\log x$.