A problem. Estimate \( S(A, \theta) \) 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 \( e(z) = e(-z) \). Let \( a_{n+1}, \ldots, a_{n+N} \in \mathbb{C} \) and consider the exponential sum

\[
S(x) = \sum_{n=M+1}^{M+N} a_n e(nx).
\]

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

\[
\int_0^1 |S(x)|^2 dx = \int_0^1 S(x) \overline{S(x)} dx
\]

\[
= \int_0^1 \left( \sum_n a_n e(nx) \right) \left( \sum_n \overline{a_n} e(-nx) \right) dx
\]

\[
= \sum_{n,n'} a_n \overline{a_{n'}} \int_0^1 e((n-n')x) dx
\]

\[
= \sum_n |a_n|^2.
\]

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

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

**Theorem 6.1** If \( \{ x_1, \ldots, x_r \} \) is \( \delta \)-spaced and \( S(x) \) is defined by (6.1), then

\[
\sum_{i=1}^r |S(x_i)|^2 \leq C \left( N + \frac{1}{\delta} \right) \sum_{n=M+1}^{M+N} |a_n|^2.
\]

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 $S = \frac{1}{r}$. If $d = \frac{1}{r}$, then $x_1, x_2, \ldots, x_r$ 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 $r \to \infty$, $\delta \sum_{i=1}^{r} |S(x_i)|^2 \to \sum_{n=\pm 1}^{\infty} \lambda_n |x_n|^2$, i.e. the term $\frac{1}{r}$ cannot be removed.

Also, if $r \geq 1$, $\lambda_n = 1 \forall n$ and $x_i = 0$, then

$|S(x_i)|^2 = N^2 = N \sum_{n=\pm 1}^{\infty} |a_n|^2$, 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 $i$,

$|S(x_i)| \ll \left( \frac{1}{r} (N + \frac{1}{r}) N \right)^{\frac{1}{2}} \ll \frac{N}{\sqrt{r}}$ if $\delta \gg \frac{1}{N}$.

In particular, this holds for at least one $i$. This is a savings of $1/r$ 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

$|S(x)| = \left| \sum_{n=M+1}^{N} a_n e(nx) \right| = |S^*(x)| = \left| \sum_{n=1}^{N} a_{nm} e(nx) \right|$, where $S^*(x) = e(-Mx) S(x)$.

Proof idea

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

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

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

**Lemma 6.1** (Gallagher, 1967)

If $f : \mathbb{R} \to \mathbb{C}$ has continuous derivative on $[x-\frac{\delta}{2}, x+\frac{\delta}{2}]$, then

$|f(x)| \leq \frac{1}{\delta} \int_{x-\frac{\delta}{2}}^{x+\frac{\delta}{2}} |f(y)| dy + \frac{1}{2} \int_{x-\frac{\delta}{2}}^{x+\frac{\delta}{2}} |f'(y)| dy$.
Proof. WLOG $x = 0$. Using integration by parts,

\[
\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \left( \frac{\pi}{2} - y \right) f'(y) \, dy = -\frac{\pi}{2} f(0) + \int_{0}^{\frac{\pi}{2}} f(y) \, dy
\]

and

\[
\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \left( \frac{\pi}{2} + y \right) f'(y) \, dy = \frac{\pi}{2} f(0) - \int_{-\frac{\pi}{2}}^{0} f(y) \, dy.
\]

Subtracting the two equations gives

\[
\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} f'(y) \, dy = \frac{\pi}{2} f(0) + \int_{-\frac{\pi}{2}}^{0} f(y) \, dy + \frac{\pi}{2} f(0) - \int_{0}^{\frac{\pi}{2}} f(y) \, dy.
\]

Hence

\[
|f(0)| \leq \frac{\pi}{2} \int_{-\frac{\pi}{2}}^{0} f(y) \, dy + \frac{\pi}{2} \int_{0}^{\frac{\pi}{2}} |f'(y)| \, dy.
\]

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

\[
|S(x_i)|^2 \leq \frac{1}{\delta} \int_{I_i} |S(y)|^2 \, dy + \frac{1}{\delta} \int_{I_i} 2S(y)S'(y) \, dy, \quad I_i = [x_i - \frac{\delta}{2}, x_i + \frac{\delta}{2}].
\]

Since the $x_i$ are $\delta$-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,

\[
\sum_{i=1}^{N} |S(x_i)|^2 \leq \frac{1}{\delta} \int_{0}^{1} |S(y)|^2 \, dy + \int_{0}^{1} |S(y)S'(y)| \, dy.
\]

By Parseval's identity,

\[
\int_{0}^{1} |S(y)|^2 \, dy = \sum_{n=1}^{N} |\alpha_n|^2.
\]

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

\[
\int_{0}^{1} |S(y)S'(y)| \, dy \leq \left( \int_{0}^{1} |S(y)|^2 \, dy \right)^{1/2} \left( \int_{0}^{1} |S'(y)|^2 \, dy \right)^{1/2}
\]

\[
= \left( \sum_{n=1}^{N} |\alpha_n|^2 \right)^{1/2} \left( \sum_{n=1}^{N} (\pi n |\alpha_n|^2) \right)^{1/2}
\]

\[
\leq 2\pi N \sum_{n=1}^{N} |\alpha_n|^2.
\]
Therefore,
\[ \sum_{l=1}^{c} |s(x_l)|^2 \leq \left( \frac{1}{5} + 2\pi N \right) \sum_{n=1}^{N} |a_n|^2. \]

2. Arithmetic version

Let \( a_{M+1}, \ldots, a_{M+N} \in \mathbb{C} \) and put \( S(q,a) = \sum_{\substack{m \leq n \leq M+N \\text{}} \quad n \equiv a \pmod{q}^{n}} a_n \).

E.g. if \( A \) is a finite set of integers \( \{M+1, \ldots, M+N\} \), \( a_n = \{1 \text{ if } n \in A, \quad 0 \text{ if } n \notin A \) then \( S(q,A) \) is the number of elements of \( A \) in the residue class \( a \pmod{q} \).

**Theorem 6.2** For any \( Q \geq 1 \),
\[
\sum_{q \leq Q} q \sum_{\substack{\chi \neq \chi' \pmod{q} \\text{}} \quad \left| \sum_{d \mid q} \mu(d) S\left( \frac{q}{d}, a \right) \right|^2 \leq C(N+Q^2) \sum_{M \leq n \leq M+N} |a_n|^2,
\]

where \( C \) is the constant from Theorem 6.1.

**Proof.** For the points \( x_i \), we take the Farey fractions
\[
\left\{ \frac{a}{b} : 1 \leq a \leq Q, 1 \leq b \leq Q, (a,b) = 1 \right\} = \left\{ \frac{1}{Q}, \frac{2}{Q}, \ldots, \frac{Q-1}{Q}, 1 \right\}.
\]

Since \( \| \frac{a}{b} - \frac{a'}{b'} \| = \frac{1}{bb'} \geq \frac{1}{Q^2} \) for any \( \frac{a}{b} \neq \frac{a'}{b'} \), these points are \( \delta \)-spaced with \( \delta = \frac{1}{Q^2} \). By Theorem 6.1,
\[
\sum_{q \leq Q} \sum_{\chi \neq \chi' \pmod{q}} \left| S\left( \frac{q}{d}, a \right) \right|^2 \leq C(N+Q^2) \sum_{M \leq n \leq M+N} |a_n|^2.
\]

We must massage the left side of (6.4). For brevity, write \( \sum_{a}^{*} \) for \( \sum_{\substack{a \neq 1 \pmod{q} \\text{}} \quad \sum_{(a,q)}=1} \).
We interpret $\sum_a^* |S(\frac{a}{b})|^2$ in terms of a discrete Parseval identity.

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

$$\sum_{h=1}^g |T(\ell, h)|^2 = \sum_{h=1}^g \sum_a^* \sum_{\alpha'}^* S\left(\frac{a}{b}\right) S\left(\frac{-a'}{b}\right) e\left(-\frac{ha}{b}\right) e\left(\frac{ha'}{b}\right)$$

$$= \sum_a^* \sum_{\alpha'}^* S\left(\frac{a}{b}\right) S\left(\frac{-a'}{b}\right) \sum_{h=1}^g e\left(\frac{(a-a')h}{b}\right)$$

$$= g \sum_a^* |S(\frac{a}{b})|^2 .$$

Using the identity for Ramanujan sums

$$c_6(n) = \sum_a^* e\left(\frac{an}{b}\right) = \sum_{d|\ell, n} d \mu(\frac{\ell}{d}) ,$$

we have

$$T(\ell, h) = \sum_a^* S\left(\frac{a}{b}\right) e\left(-\frac{ha}{b}\right)$$

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

$$= \sum_n a_n c_6(n-h)$$

$$= \sum_n a_n \sum_{d|\ell, n-h} d \mu\left(\frac{n}{d}\right)$$

$$= g \sum_{\ell|\ell} \mu\left(\frac{\ell}{f}\right) \sum_{n=h \mod \frac{\ell}{f}} a_n$$

$$= g \sum_{\ell|\ell} \mu\left(\frac{\ell}{f}\right) S\left(\frac{\ell}{f}, h\right).$$

Therefore, the left side of (6.4) is

$$\sum_{\ell|\ell} \frac{1}{\ell} \sum_{h=1}^g |T(\ell, h)|^2 = \sum_{\ell|\ell} g \left| \sum_{\ell|\ell} \frac{\mu(\ell)}{f} S\left(\frac{\ell}{f}, h\right) \right|^2 ,$$

as desired.
Corollary 6.3

We have

\[ \sum_{p \leq \sqrt{N}} \frac{1}{p} \left| \sum_{a=1}^{p} \left( \frac{1}{p} \sum_{n \equiv a \pmod{p}} \frac{1}{N} \sum_{N < n < N+M} a_n \right)^2 \right| \leq \frac{2C}{N} \sum_{n} \left| a_n \right|^2. \]

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

Remarks. Writing \( D(p,a) = \frac{1}{N} \sum_{M < n < M+M} a_n - \frac{1}{N} \sum_{M < n < M+M} a_n \), the left side of (6.5) becomes

\[ \sum_{p \leq \sqrt{N}} \frac{1}{p} \left( \sum_{a=1}^{p} \left| D(p,a) \right|^2 \right). \]

\( D(p,a) \) 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 \( p \).

An important case is when \( a_n \) is the characteristic function of a set \( \mathcal{A} \subseteq \mathbb{Z} \), where \( \mathcal{A} = \{ n \in \mathbb{Z} : n \equiv a \pmod{M} \} \).

Corollary 6.4. For any \( Q \geq 1 \),

\[ \sum_{\frac{M}{Q} < p \leq \sqrt{N}} \frac{1}{p} \sum_{a=1}^{p} \left| \sum_{\frac{M}{Q} < d | p} \frac{\mu(d)}{d} Z\left( \frac{d}{a}, p \right) \right|^2 \leq C \left( N + Q^2 \right) Z. \]

Also,

\[ \sum_{p \leq Q} \frac{1}{p} \sum_{a=1}^{p} \left| pZ(p,a) - Z \right|^2 \leq C \left( N + Q^2 \right) Z. \]

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

\[ \left| pZ(p,a) - Z \right| \ll \sqrt{ZN^{\frac{1}{2}} \log N} \ll N^{\frac{3}{2} \frac{1}{\sqrt{\log N}}}, \]

i.e., for most \( a \) and \( p \), \( Z(p,a) \approx \frac{Z}{p} \), so \( \mathcal{A} \) contains the expected number of elements in the residue class \( a \pmod{p} \). If \( \left| pZ(p,a) - Z \right| \) is large for many \( a \) and \( p \), (6.6) implies that \( Z \) must be small.
Theorem 6.5 (Large Sieve - Sieve version)

Let $N \in \{M+1, \ldots, M+N\}$ and define $Z, Z(p, a)$ as above. Suppose, for each prime $p$, there are $\mathfrak{g}(p)$ residue classes $a \bmod p$ with $Z(p, a) = 0$. Assume $\mathfrak{g}(p) < p$ for all $p$ and for squarefree $g$, write

$$h(g) = \frac{\mathfrak{g}(p)}{p}.$$ 

Then

$$Z \leq \frac{c(N+Q^2)}{J}, \quad J = \sum_{g \leq Q} \mu^2(g) h(g) \quad (= G(\mathfrak{q}) \text{ from Selberg sieve})$$

Remarks: If $\mathfrak{g}(p) = p$ 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 $\mathfrak{g}(p)$ is bounded on average. When $\mathfrak{g}(p)$ is quite large, the error term in Selberg’s sieve is difficult to manage, while the error in Theorem 6.5 (the $Q^2$ term) is quite easy.

Proof. We shall prove that for any $a_{m+1}, \ldots, a_{m+n} \in C$, s.t. $S(p, a) = 0$ for $p(r) \mod p$-value

$$\sum_{\mathfrak{a}} |S(\mathfrak{a}/p)|^2 \geq S(p)^2 h(g). \quad (\mu^2(g) = 1).$$

Then, by (6.4),

$$c(N+Q^2)Z = \sum_{g \leq Q} Z^2 h(g),$$

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

$$\sum_{\mathfrak{a}} |S(\mathfrak{a}/p)|^2 = \frac{1}{p} \sum_{h=1}^{p} |T(p, h)|^2,$$

where $T(p, h) = p(S(p, h) - \frac{1}{p} S)$, $S = S(1, 1) = \sum_{n} a_n$. Then

$$\sum_{\mathfrak{a}} |S(\mathfrak{a}/p)|^2 = p \sum_{h=1}^{p} \left| S(p, h) - \frac{S}{p} \right|^2 = p \sum_{h=1}^{p} S(p, h)^2 - 2p \sum_{h=1}^{p} S(p, h) + |S|^2 \geq p \sum_{h=1}^{p} |S(p, h)|^2 - |S|^2.$$
By Cauchy-Schwarz,
\[
|S|^2 = \left( \sum_{h=1}^{p} S(p,h) \right)^2 = \left( \sum_{\substack{1 \leq h \leq p \\text{s.t.} \; S(p,h) \neq 0}} S(p,h) \right)^2
\]
\[
\leq \left( \sum_{1 \leq h \leq p} 1 \right) \left( \sum_{1 \leq h \leq p} |S(p,h)|^2 \right) \leq \left( p - g(p) \right) \sum_{h=1}^{p} |S(p,h)|^2.
\]

Thus
\[
\sum_{\alpha} |S(\alpha)|^2 \geq \frac{p}{p-g(p)} |S|^2 - |S|^2 = h(p) |S|^2 = h(p) |S(o)|^2.
\]

Next, suppose (6.7) holds for \( g=r \) and \( g=s \), where \((r,s)=1\).
Every \( c, 1 \leq c \leq rs \), \((c, rs)=1\) may be written uniquely as \( c = er + fs \) (mod rs) with \( 1 \leq e \leq s, 1 \leq f \leq r \), \((e,s)=1, (f,r)=1\). Then
\[
\sum_{1 \leq c \leq rs \atop (c, rs)=1} |S(\frac{e}{s} + \frac{f}{r})|^2 = \sum_{1 \leq e \leq s \atop (e,s)=1} \sum_{1 \leq f \leq r \atop (f,r)=1} |S(\frac{e}{s} + \frac{f}{r})|^2.
\]

Since (6.7) holds with \( g=s \) and all sets \( a_{n+1}, \ldots, a_{n+m} \) of complex numbers, it holds with \( a_n \) replaced by \( a_n e^{2\pi i n/r} \), i.e.,
\[
\sum_{1 \leq e \leq s \atop (e,s)=1} \left| S(\frac{e}{s} + \frac{f}{r}) \right|^2 = \sum_{1 \leq e \leq s \atop (e,s)=1} \left| S*(\frac{e}{s}) \right|^2 ; \quad S*(x) = \sum_n (a_n e^{\frac{2\pi i n x}{r}}) e^{\frac{2\pi i nx}{r}}
\]
\[
\geq h(s) \left| S*(0) \right|^2 = h(s) \left| S(\frac{f}{r}) \right|^2.
\]

Thus
\[
\sum_{1 \leq c \leq rs \atop (c, rs)=1} \left| S(\frac{c}{rs}) \right|^2 \geq h(s) \sum_{1 \leq f \leq r \atop (f,r)=1} \left| S(\frac{f}{r}) \right|^2 \geq h(s) g(r) \left| S(0) \right|^2,
\]

i.e. (6.7) holds with \( g=rs \). By induction on the number of prime factors of \( g \), (6.7) holds for all square-free \( g \).

App. primes in \((x, y, x)\), Brun-Titchmarsh thm.
Applications

A. "pseudo-squares." Suppose \( \mathcal{N} \subseteq [1, \ldots, N] \), and for \( 3 \leq p \leq \sqrt{N} \), \( \mathcal{N} \) avoids \( \frac{p-1}{2} \) residue classes modulo \( p \), and let \( Z = |\mathcal{N}| \). In the notation of Theorem 6.5, for odd squarefree \( q \),

\[
\nu(q) = \prod_{p | q} \frac{p-1}{p-2} = \frac{\phi(q)}{\sigma(q)}
\]

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

\[
Z \leq 2CN \frac{L}{L} \equiv \sum_{\substack{q \leq Q \text{ odd} \atop \mathcal{N} \text{ avoids } q}} \frac{\nu(q) \phi(q)}{\sigma(q)} \Rightarrow Q = \sqrt{N}.
\]

Hence

\[
(6.8) \quad Z = \sqrt{N}.
\]

An example of such a set \( \mathcal{N} \) is the set of squares \( \leq N \). 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.

---

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

Theorem Suppose \( Q \geq 3 \). Then

\[
\left| \sum_{p \leq Q} \sum_{p' \leq Q} \left( \frac{p'}{p} \right) \right| \ll Q^{1/4} \left( \log Q \right)^{-5/4}.
\]

Remark. The trivial bound is \( \pi(Q)^2 \ll Q^2 (\log Q)^{-2} \).

Proof. Denote by \( H \) the double sum on the left side. By Cauchy–Schwarz,

\[
H^2 \leq \left( \sum_{3 \leq p \leq Q} 1 \right) \left( \sum_{3 \leq p' \leq Q} \left| \sum_{3 \leq p'' \leq Q} \left( \frac{p'}{p} \right) \right|^2 \right)
\]

\[
\leq \pi(Q) \sum_{3 \leq p \leq Q} \sum_{3 \leq p' \leq Q} \left( \frac{p'}{p} \right) \left( \frac{p''}{p'} \right)
\]

\[
\leq \pi(Q) \sum_{3 \leq p \leq Q} \left\{ \pi(Q) + 2 \sum_{3 \leq p' \leq Q} \left( \frac{p''}{p} \right) \right\}.
\]
Let \( \mathcal{N} = \{ p^m \} \) for \( 3 \leq p < P' \leq Q \in \mathbb{Z}_+ \), so \( \mathcal{N} = \frac{1}{2} \pi(a) \pi(a) - 1 \). Then
\[
H^2 \leq \pi(a)^3 + 2 \pi(a) \sum_{3 \leq p \leq a} \left| \sum_{n \in \mathcal{N}} \left( \frac{n}{p} \right) \right|.
\]

By Cauchy–Schwarz again,
\[
\sum_{3 \leq p \leq a} \left| \sum_{n \in \mathcal{N}} \left( \frac{n}{p} \right) \right| \leq \pi(a)^3 \left\{ \sum_{3 \leq p \leq a} \left( \sum_{n \in \mathcal{N}} \left( \frac{n}{p} \right) \right)^2 \right\}^{1/2}.
\]

Using \( \sum_{h=1}^{p} \left( \frac{h}{p} \right) = 0 \), we have
\[
\sum_{n \in \mathcal{N}} \left( \frac{n}{p} \right) = \sum_{h=1}^{p} \sum_{n \in \mathcal{N} \mod p} \left( \frac{n}{p} \right) = \sum_{h=1}^{p} \left( \frac{h}{p} \right) Z(p, h)
\]
\[
= \sum_{h=1}^{p} \left( \frac{h}{p} \right) \left( Z(p, h) - \frac{Z}{p} \right).
\]

By another application of Cauchy–Schwarz,
\[
\left( \sum_{n \in \mathcal{N}} \left( \frac{n}{p} \right) \right)^2 \leq \left( \sum_{h=1}^{p} \left( \frac{h}{p} \right)^2 \right) \left( \sum_{h=1}^{p} \left| Z(p, h) - \frac{Z}{p} \right|^2 \right)
\]
\[
\leq p \sum_{h=1}^{p} \left| Z(p, h) - \frac{Z}{p} \right|^2.
\]

Hence
\[
H^2 \leq \pi(a)^3 + 2 \pi(a) \left\{ \sum_{3 \leq p \leq a} \left( \frac{Z}{p} \right)^2 \right\}^{1/2}.
\]

By Corollary 6.4, (6.6), the expression in braces is \( \leq C Q^2 Z \leq C Q^2 \pi(a)^2 \).

Hence
\[
H^2 \ll \left( \frac{a}{\log Q} \right)^3 + \left( \frac{Q}{\log Q} \right)^{3/2} \left( \frac{Q}{\log^2 Q} \right)^{1/2} \ll \frac{Q}{(\log Q)^{5/2}}.
\]

C. Least quadratic non-residue modulo a prime

\[
n(p) = \min \left\{ n \in \mathbb{N} : \left( \frac{n}{p} \right) = -1 \right\}
\]

Estimates:
\[
n(p) \ll p \log p \quad \text{(from Pólya–Vinogradov Thm)}
\]
\[
n(p) \ll p \frac{\log^2 p}{p} \quad \text{(best known; Burgess est. + "Vinogradov trick")}
\]
\[
n(p) \ll \log p \quad \text{(Ankeny; assumes ERH for Dirichlet L-funct.)}
\]
Theorem 6.6 (Linnik)

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

$$\left| \{3 \leq p \leq N : n(p) > N^{\varepsilon^2} \} \right| \leq C(\varepsilon).$$

Corollary

Fix any fixed $\varepsilon > 0$,

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

Proof of Corollary

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

$$\left| \{3 \leq p \leq N : n(p) > p^{\varepsilon^3} \} \right| = \sum_{j=1}^{\varepsilon} \left| \{N^{2-j} < p \leq N^{2-j+1} : n(p) > p^{\varepsilon^3} \} \right|$$

$$\leq \sum_{j=1}^{\varepsilon} \left| \{p \leq N^{2-j+1} : n(p) > (N^{2-j+1})^{\varepsilon/2} \} \right|$$

$$\leq C(\varepsilon)J \ll \varepsilon \log \log N.$$

Proof of Theorem 6.6

Apply Theorem 6.5 with the set $\mathcal{N} = \{1 \leq n \leq N^2 : p^\varepsilon(n) \leq N^{\varepsilon^2} \}$.

If $p > 3$ and $n(p) > N^\varepsilon$, then $\left( \frac{n}{p} \right) = 1$ for primes $g \leq N^\varepsilon$. Hence,

$(\frac{n}{p}) = 1$ for all $n \in \mathcal{N}$. Hence $\mathcal{N}$ avoids $\frac{p-1}{2} = g(p)$ residue classes mod $p$, for every such prime $p$. Take $a = N$. Also

$$L = \sum_{\substack{g \leq a \ \text{mod} \ p_b \ \text{are} \ \frac{p-1}{2} \ \text{and} \ \frac{p+1}{2}?}} \frac{p(\mathcal{P})}{p} \geq \sum_{3 \leq p \leq N} \frac{p-1}{p+1} \geq \frac{1}{2} \# \{3 \leq p \leq N : n(p) > N^{\varepsilon^2} \}.$$

Theorem 6.5 gives

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

On the other hand, $|\mathcal{N}| = \psi(N^2, N^\varepsilon) \gg \varepsilon N^2$ by Theorem 5, and the theorem follows.
3. Character sum version of large sieve, Bombieri-Vinogradov Theorem

Recall that a Dirichlet character $\chi$ mod $q$ is **primitive** if there is no character $\psi$ mod $q'$, $q' | q$, so that $\chi = \psi \chi_0$, where $\chi_0$ is the principal character mod $q$. Equivalently, for all $q', q', q' < q$, there is an $l$ so that $\chi(lq' + 1) \neq \{0, 1\}$.

**Lemma 6.2** If $\chi$ is a primitive character mod $q > 1$, then for any $n$,

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

where

$$\tau(\chi) = \sum_{m=1}^{q} \overline{\chi}(m) e\left(\frac{m}{q}\right) = \sum_{q=1}^{q} \overline{\chi}(m) e\left(\frac{m}{q}\right)$$

is the Gauss sum for $\chi$.

**Proof** If $(n, q) = 1$, then

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

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

$$\sum_{h=1}^{q} \overline{\chi}(h) e\left(\frac{nh}{q}\right) = \sum_{c=0}^{\frac{q}{d_1}} c\left(\frac{cn}{q_1}\right) \sum_{l=0}^{d-1} \overline{\chi}(q_1 l + c).$$

Note $S(c + q_1) = S(c)$ (replace $l$ with $l - 1$). Thus, if $(n, q) = 1$ and $n \equiv 1 \mod q_1$ then

$$\overline{\chi}(n) S(c) = \sum_{l=0}^{d-1} \overline{\chi}(q_1 l + vc) = \sum_{l=0}^{d-1} \overline{\chi}(q_1 + vc) = S(vc) = S(c).$$

If $S(c) \neq 0$, then $\overline{\chi}(n) \notin \{0, 1\}$ for all such $n \Rightarrow \chi$ is primitive.

Hence $S(c) = 0$ for every $c$, hence

$$\sum_{h=1}^{q} \overline{\chi}(h) e\left(\frac{nh}{q}\right) = 0 = \chi(n) \tau(\chi).$$
Lemma 6.3  If $\chi$ is a primitive character mod $g$, then
$$|\tau(\chi)| = \sqrt{g}.$$  

Proof  By Lemma 6.2,
$$|\chi(n)|^2 \cdot |\tau(\chi)|^2 = \sum_{h_1=1}^{g} \sum_{h_2=1}^{g} \overline{\chi}(h_1) \chi(h_2) e\left(\frac{n(h_1-h_2)}{g}\right).$$

Summing over $1 \leq n \leq g$ gives
$$\phi(g) |\tau(\chi)|^2 = \sum_{h_1=1}^{g} \sum_{h_2=1}^{g} \overline{\chi}(h_1) \chi(h_2) \sum_{h=1}^{g} e\left(\frac{n(h_1-h_2)}{g}\right).$$

The sum an $n$ is zero unless $h_1 = h_2$, in which case the sum is $g$. Hence
$$\phi(g) |\tau(\chi)|^2 = g \sum_{h=1}^{g} |\overline{\chi}(h)|^2 = g \phi(g),$$

hence $|\tau(\chi)| = \sqrt{g}$.

Theorem 6.7  (Polya & Vinogradov 1918)

For any non-primitive Dirichlet character $\chi$ mod $g$, and any $A, B \in \mathbb{R},$
$$\left| \sum_{A \leq n \leq B} \chi(n) \right| \ll \sqrt{g} \log g.$$

Proof  (For primitive characters)

By Lemma 6.2,
$$\sum_{A \leq n \leq B} \chi(n) = \frac{1}{\tau(\chi)} \sum_{h=1}^{g-1} \overline{\chi}(h) \sum_{A \leq n \leq B} \frac{e\left(\frac{n h}{g}\right)}{\frac{h}{g}}.$$

Next, 
$$\left| \sum_{A \leq n \leq B} e\left(\frac{n h}{g}\right) \right| = \left| \frac{e\left(\frac{hB}{g}\right)\overline{\chi}(h+1) - 1}{e\left(\frac{hB}{g}\right) - 1} \right| \leq \frac{2}{|e(hB/2) - 1|} \leq \frac{1}{2\|hB\|},$$

where $\|x\|$ = distance from $x$ to the nearest integer. Therefore,
$$\left| \sum_{A \leq n \leq B} \chi(n) \right| \leq \frac{1}{\tau(\chi)} \sum_{h=1}^{g-1} \frac{1}{2\|hB\|}$$
$$= \frac{1}{2\sqrt{g}} \left( \sum_{1 \leq h \leq \sqrt{g}/2} \frac{g}{h} + \sum_{\sqrt{g}/2 < h \leq g-1} \frac{g}{g-h} \right)$$
$$\leq \frac{g}{2\sqrt{g}} \left( \log \frac{g}{2} + 1 + \log \frac{g}{2} + 1 \right) \ll \sqrt{g} \log g.$$

Corollary

(i) $n(p) \ll \sqrt{p} \log p$ (show details)

(ii) $n(p) \ll p^{1/8+\epsilon}$ for all $\epsilon > 0$ (exercise)
Let \( \mathcal{C}(q) = \text{set of Dirichlet characters modulo } q \)
\( \mathcal{C}^*(q) = \text{set of primitive characters } \in \mathcal{C}(q). \)

**Theorem 6.8** Let \( a_{m+1}, \ldots, a_{m+N} \in \mathcal{C} \) and put

\[
U(X) = \sum_{m+1 \leq n \leq m+N} a_n \chi(n).
\]

For any \( Q \geq 1, \) we have

\[
\sum_{q \leq Q} \frac{q}{\varphi(q)} \sum_{\chi \in \mathcal{C}^*(q)} |U(X)|^2 \leq C(N+Q^2) \sum_{m+1 \leq n \leq m+N} |a_n|^2.
\]

**Proof.** Apply Lemma 6.2 and sum over \( n :\)

\[
\mathcal{C}(X) U(X) = \sum_{h=1}^{g} \overline{\chi}(h) \sum_{m+1 \leq n \leq m+N} a_n \xi \left( \frac{n}{q} \right) = \sum_{h=1}^{g} \overline{\chi}(h) S(h/q),
\]

where

\[
S(x) = \sum_{m+1 \leq n \leq m+N} a_n \xi(x).
\]

Therefore,

\[
\sum_{\chi \in \mathcal{C}^*(q)} |\mathcal{C}(X) U(X)|^2 = \sum_{\chi \in \mathcal{C}^*(q)} \left| \sum_{h=1}^{g} \overline{\chi}(h) S(h/q) \right|^2
\]

\[
\leq \sum_{\chi \in \mathcal{C}(q)} \left| \sum_{h=1}^{g} \overline{\chi}(h) S(h/q) \right|^2
\]

\[
= \sum_{h_1, h_2 = 1 \atop (h_1, q) = 1}^{g} s(h_1/q) S(h_2/q) \sum_{\chi \in \mathcal{C}(q)} \overline{\chi}(h_1) \chi(h_2).
\]

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

\[
\sum_{\chi \in \mathcal{C}^*(q)} |U(X)|^2 \leq \phi(q) \sum_{h=1 \atop (h, q) = 1}^{g} |S(h/q)|^2.
\]

By Theorem 6.1,

\[
\sum_{q \leq Q} \frac{q}{\varphi(q)} \sum_{\chi \in \mathcal{C}^*(q)} |U(X)|^2 \leq \sum_{g \leq Q} \left( \sum_{h=1 \atop (h, q) = 1}^{g} |S(h/q)|^2 \right) \leq C(N+Q^2) \sum_{m+1 \leq n \leq m+N} |a_n|^2.
\]
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 \(Q > 1\), we have

\[
\sum_{q \leq Q} \left| \hat{f}(q) \int_{\mathbb{R}} f(x) \frac{x}{q} \, dx \right| \leq \frac{M \log(1 + Q)}{(4\pi)^{1/2}} \sqrt{(\sum_{m=1}^{M} |a_m|^2)^{1/2} (\sum_{n=1}^{N} |b_n|^2)^{1/2} \log(2MN)}.
\]

Remark: double sum on \(m, n\) is \(\sum_{m \equiv u \pmod{u}} a_m \chi(m), \sum_{n \equiv v \pmod{v}} b_n \chi(n)\).

Proof. To handle the condition \(mn \equiv u\), recall an identity used in a truncated version of Perron’s formula:

\[
\int_{c-iT}^{c+IT} \frac{y^s}{s} ds = \delta(y) + O\left( \frac{y^c}{T \log y} \right) \quad (c > 0, y > 0, y \neq 1, T > 1)
\]

where \(\delta(y) = \begin{cases} 1 & 0 < y < 1 \\ 0 & y > 1 \end{cases}\). Without loss of generality (WLOG), let \(u = u_0 + \frac{1}{T}, u_0 \in \mathbb{Z}, 0 < u_0 < MN\).

Then

\[
\sum_{m=1}^{M} \sum_{n=1}^{N} a_m b_n \chi(mn) = \sum_{m=1}^{M} \sum_{n=1}^{N} a_m b_n \chi(mn) \delta\left(\frac{u}{mn}\right)
\]

\[
= \frac{1}{2\pi i} \int_{c-IT}^{c+IT} \frac{y^s}{s} \left( \sum_{m=1}^{M} a_m \chi(m) m^{-s} \right) \left( \sum_{n=1}^{N} b_n \chi(n) n^{-s} \right) ds
\]

\[
+ O\left( \frac{1}{T} \sum_{m,n} \frac{(y_{mn})^c}{|\log y_{mn}|} |a_m b_n| \right).
\]

In the error term,

\[
\left| \frac{1}{\log y_{mn}} \right| = \frac{1}{y_{mn}} \gg \frac{1}{MN}.
\]

Put \(c = \frac{1}{\log(2MN)}\) so that \(|u^s| \ll 1\) and \((y_{mn})^c \ll 1\). Then the left side above is

\[
\ll \int_{c-IT}^{c+IT} \frac{1}{|s|} |A(s, x)| \cdot |B(s, x)| \cdot |ds| + \frac{MN}{T} \sum_{m,n} |a_m b_n|
\]

uniformly in \(u\). Hence, the left side of (6.9) is, by the Cauchy–Schwarz inequality,

\[
\ll \int_{c-IT}^{c+IT} \left( \sum_{q \leq Q} \frac{q}{\phi(q)} \sum_{x \in \mathbb{C}(q)} |A(s, x)|^2 \right)^{1/2} \left( \sum_{q \leq Q} \frac{q}{\phi(q)} \sum_{x \in \mathbb{C}(q)} |B(s, x)|^2 \right)^{1/2} ds
\]

\[
+ \sum_{q \leq Q} \frac{q}{\phi(q)} \sum_{x \in \mathbb{C}(q)} \frac{(MN)^{3/2}}{T} \left( \sum_{m} |a_m|^2 \right)^{1/2} \left( \sum_{n} |b_n|^2 \right)^{1/2} O(Q^2).
\]
By Theorem 6.8,
\[ \sum_{g \leq Q} \frac{g}{\phi(g)} \sum_{\chi \in \chi^*(g)} |A(g, \chi)|^2 \leq C(M+Q^2) \sum_{m=1}^{M} |a_m m^{-s}|^2 \ll (M+Q^2) \sum_{m=1}^{M} |a_m|^2 \]
and similarly
\[ \sum_{g \leq Q} \frac{g}{\phi(g)} \sum_{\chi \in \chi^*(g)} |B(g, \chi)|^2 \ll (N+Q^2) \sum_{n=1}^{N} |b_n|^2 . \]
Finally,
\[ \int_{c-iT}^{c+iT} \frac{1}{s} ds = \int_{c-iT}^{c+iT} dt \frac{1}{1+it} \leq \frac{2}{C} + 2 \int_{c-iT}^{c+iT} dt \frac{1}{t} \leq 2 \log (2TMN) . \]
Therefore, the left side of (6.9) is
\[ \ll \left( \sum_{m=1}^{M} |a_m|^2 \right)^{\frac{1}{2}} \left( \sum_{n=1}^{N} |b_n|^2 \right)^{\frac{1}{2}} \left( (M+Q^2)^{\frac{1}{2}} (N+Q^2)^{\frac{1}{2}} \log (2TMN) + Q^{2} \frac{\log (2MN)}{T} \right) . \]
Taking \( T = (MN)^{1/2} \) completes the proof.

**Theorem BV** (Bombieri; A.I. Vinogradov, 1965)
For every \( A > 0 \) there is a \( B \) so that
\[ \sum_{g \leq x^{\frac{2}{3}}(\log x)^{-B}} \max_{\chi \neq 1} \max_{y \leq x} \left| \pi(y, \chi, g) - \frac{\xi(y)}{\phi(g)} \right| \ll \frac{x}{(\log x)^A} . \]

**Theorem BV**
For every \( A > 0 \) there is a \( B \) so that
\[ \sum_{g \leq x^{\frac{2}{3}}(\log x)^{-B}} \max_{\chi \neq 1} \max_{y \leq x} \left| \psi(y, \chi, g) - \frac{y}{\phi(g)} \right| \ll \frac{x}{(\log x)^A} , \quad \psi(y, \chi, g) = \sum_{n \leq y} \Lambda(n) . \]

**Exercise** Show Theorems BV, BV* are equivalent.
Let \( \psi(y, x) = \sum_{n \leq y} \chi(n) \Lambda(n) \).

**Lemma 6.4** For \( 1 \leq q \leq x \),

\[
\sum_{g \leq q} \max \max_{y \leq x} \left| \frac{\psi(y; g, \alpha)}{\phi(q)} - \frac{y}{\phi(q)} \right| \ll \frac{1}{\phi(q)} \sum_{\chi \in \mathcal{C}(g)} \max_{y \leq x} |\psi(y, x)|.
\]

Here \( c > 0 \) is a constant.

**Proof** Start with the orthogonality relation

\[
\psi(y; g, \alpha) = \frac{1}{\phi(q)} \sum_{\chi \in \mathcal{C}(g)} \chi(\alpha) \psi(y, x),
\]

which implies

\[
\left| \frac{\psi(y; g, \alpha)}{\phi(q)} - \frac{y}{\phi(q)} \right| \leq \frac{1}{\phi(q)} \left( \left| \psi(y, x) - y \right| + \sum_{\chi \in \mathcal{C}(g)} \max_{y \leq x} |\psi(y, x)| \right).
\]

Now reduce the problem to sums \( \psi(y, x) \) with \( \chi \) primitive. For general \( \chi \in \mathcal{C}(g) \), if \( \chi \) is induced by the primitive character \( \chi_1 \mod q_1 \), then \( \chi(p) = \chi_1(p) \) for all primes \( p \) except those with \( p \equiv 1 \pmod{q_1} \). Hence

\[
\left| \psi(y, x) - \psi(y, x_1) \right| \leq \sum_{1 \leq p \leq y} \log p \leq \sum_{1 \leq p \leq y} \log p \cdot \left[ \frac{\log y}{\log p} \right]
\]

\[
\ll \log y \cdot \frac{\log y}{\log p} \ll \log^2 y.
\]

Setting \( E^*(x, g) = \max_{y \leq x} \frac{\psi(y; g, \alpha) - y}{\phi(q)} \), we obtain

\[
E^*(x, g) \leq \max_{\chi \in \mathcal{C}(g)} \left[ \left( \psi(y, x_1) - y \right) + \sum_{\chi \in \mathcal{C}(g)} \max_{y \leq x} |\psi(y, x)| + O\left( \frac{\log^2 y}{\log \phi(q)} \right) \right]
\]

\[
\ll \log^2 x + \frac{x e^{-c_0 \log x}}{\phi(q)} + \frac{1}{\phi(q)} \sum_{\chi \in \mathcal{C}(g)} \max_{y \leq x} |\psi(y, x)|
\]

by the Prime Number Theorem, where \( c_0 > 0 \) is a constant. A given \( \chi_1 \mod q_1 \) induces characters \( \chi \mod g \) only for \( g_1 \mid g \). Hence

\[
\sum_{g \leq q} E^*(x, g) \ll \frac{1}{\phi(q)} \sum_{g \leq q} \frac{1}{\phi(q)} \sum_{\chi \in \mathcal{C}(g)} \max_{y \leq x} |\psi(y, x)| = \sum_{\ell \leq q} \frac{1}{\phi(q)} \mathcal{O}\left( \frac{1}{\log \phi(q)} \right).
\]

Lastly, \( \phi(q) \mid \phi(q) \phi(q) \) and

\[
\sum_{m \leq z} \frac{1}{\phi(m)} \leq \sum_{p \mid (m) \leq z} \frac{1}{\phi(m)} = \prod_{p \leq z} \left( 1 + \frac{1}{p} + \frac{1}{p^2} + \ldots \right) = \prod_{p \leq z} \left( 1 - \frac{1}{p} \right)^{-1} \left( 1 + \frac{1}{p} + \frac{1}{p^2} \right)
\]

\[
\ll \log z.
\]
Theorem SW (Siegel-Walfisz theorem)

For any fixed \( C > 0 \), and uniformly for primitive \( x \mod q \), \( q \leq (\log x)^C \), we have
\[
|\Psi(y,x)| \ll y e^{-c' \sqrt{\log y}}, \quad c' > 0.
\]

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 theory.

Corollary For any \( C > 0 \),
\[
\sum_{2 \leq y \leq (\log x)^C} \frac{1}{\phi(y)} \sum_{\chi \leq C(y)} \max_{y \leq x} |\Psi(y,x)| \ll \sqrt{x} e^{-C \sqrt{\log x}}, \quad \text{where} \quad c'' > 0 \quad \text{depends on} \quad C.
\]

Proof Write
\[
\max_{y \leq x} |\Psi(y,x)| \leq \Psi(x^{1/2}) + \max_{x^{1/2} < y \leq x} |\Psi(y,x)|
\]
and apply Theorem SW (with \( C \) replaced by \( C/4 \)) to right side.

Prime Decomposition (subatomic theory)

basic example: \( \Lambda * 1 = \log \Rightarrow \Lambda = \log * \mu \)

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

more sophisticated decomposition: parameter \( U > 1 \).

\[
\Lambda(n) = \sum_{ab = n} \mu(a) \log b,
\]

separately consider \( a \leq U \) and \( a > U \).

If \( n > U \), then
\[
\sum_{ab = n} \mu(a) \log b = \sum_{cln} \Lambda(c) \sum_{a \leq n/c} \mu(a)
\]

where sum \( 0 \) if \( c > n/U \)

\[
= -\sum_{cln} \Lambda(c) \sum_{a \leq n/c} \mu(a)
\]
since \( \sum_{a \leq n/c} \mu(a) = 0 \) for \( c < n \).

(6.10)
Lemma 6.5. Let $\chi$ be a primitive character of conductor $g \geq 2$, $\gamma \geq 2$ and $u > 1$. Then

$$\psi(y, x) = -\sum_{b \leq y, c \leq u} \Lambda(c) \chi(bc) \sum_{a \leq u} \mu(a) + O\left(u^2 g^{1/2} \log g \log y\right)$$

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

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

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

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

where

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

$$\psi_2 = \sum_{a \leq u, b \leq y} \mu(a) \chi(a) \log b \chi(b) \ll \sum_{a \leq u} \left| \sum_{b \leq y/a} \chi(b) \log b \right|,$$

$$\psi_3 = -\sum_{a \leq u, c \leq u, b \leq y/a} \chi(c) \mu(a) \chi(ac) \sum_{b \leq y/ac} \chi(b), \quad (n = abc),$$

$$\psi_4 = -\sum_{b \leq u, c \leq u, b \geq y} \chi(c) \mu(b) \chi(bc) \sum_{a \leq u} \chi(a). \quad (n = abc)$$

By the Pólya–Vinogradov inequality (Theorem 6.7),

$$\sum_{A \leq b \leq B} \chi(b) \log b = \log B \sum_{A \leq b \leq B} \chi(b) - \log A \sum_{A \leq b \leq A} \chi(b) + \sum_{A \leq b \leq A} \chi(b) \log b \ll \log B \max_{b \leq B} |\sum_{A \leq b \leq B} \chi(b)| \ll g^{1/2} \log g \log y.$$  

Hence

$$|\psi_2| \ll u g^{1/2} \log g \log y.$$  

Also by Theorem 6.7,

$$|\psi_3| \ll \sum_{a \leq u} \Lambda(c) \sum_{a \leq u} \left( g^{1/2} \log g \right) \ll u^2 g^{1/2} \log g.$$
Proof of Theorem BV

Start with Lemma 6.4. The corollary to Theorem SW takes care of the terms with \( g \neq (\log x)^c \). Suppose \( x^{1/2} < a \leq x^{1/2} \), \( 1 < u \leq Q \). By Lemma 6.5,

\[
(6.11) \quad \sum_{q \leq Q} \max_{a \leq q} \| \psi(y, s, q) - \frac{Q}{q} \psi \|_{s, \infty} \ll x e^{-c_{1} \sqrt{\log x}} + \log x \left( D_1 + D_2 \right),
\]

where

\[
D_1 = \sum_{a \leq q} \frac{1}{\phi(q)} \sum_{\chi \in C(q)} u^2 q \frac{1}{y} \log y \log x \ll \frac{Q^2 \log^2 x}{y},
\]

and, using Theorem 6.9,

\[
D_2 = \sum_{(y, x) \leq \frac{Q}{y}} \frac{1}{\phi(q)} \sum_{\chi \in C(p)} \max_{y \leq x} \left| \sum_{b \leq y, c \leq U} \Lambda(c) \chi(b c) \sum_{a \leq u} \mu(a) \right|
\ll \log^3 x \max_{y \leq \frac{Q}{y}} \frac{1}{Q_0} \max_{y \leq b \leq \frac{c}{y}} \frac{1}{U} \sum_{a \leq q} \frac{1}{\phi(q)} \sum_{\chi \in C(q)} \max_{y \leq x} \left| \sum_{b \leq y, c \leq U} \Lambda(c) \chi(b) \sum_{a \leq u} \mu(a) \right|
\ll \log^3 x \max_{a, b, c, c_0} \frac{1}{b_0} \left( \frac{b_0 + Q_0}{c_0} \right) \left( c_0^2 + Q_0 \right) \left( \sum_{c = 2c_0} \Lambda(c)^2 \right)^{1/2} \left( \sum_{b \leq 2b_0} \chi(b)^2 \right)^{1/2} \log \left( b_0 c_0 \right).
\]

By Chebyshev's estimates,

\[
\sum_{c \leq 2c_0} \Lambda(c)^2 \ll c_0 \log c_0.
\]

Also,

\[
\sum_{b \leq 2b_0} \chi(b)^2 \leq 2b_0 \sum_{b \leq 2b_0} \frac{\chi(b)^2}{b} \leq 2b_0 \sum_{p \leq 2b_0} \frac{\chi(b)^2}{b} \ll 2b_0 \prod_{p \leq 2b_0} \left( 1 + \frac{2}{p} + \frac{2}{p^2} \right) \ll b_0 \left( \log b_0 \right)^4.
\]

Thus,

\[
D_2 \ll \left( \log x \right)^{1/2} \max_{a, b, c, c_0} \frac{b_0 c_0}{Q_0} \left( \frac{b_0 + c_0}{c_0} + \frac{b_0 + c_0}{c_0} Q_0 + Q_0^2 \right)
\ll \left( \log x \right)^{1/2} \max_{a, b, c, c_0} \left( \frac{x}{Q_0} + \frac{x}{u^2} + x^{1/2} Q_0 \right)
\ll \left( \log x \right)^{1/2} \left( \frac{x}{Q_0} + \frac{x}{u^2} + x^{1/2} Q_0 \right).
\]

The left side of (6.11) is therefore

\[
\ll \frac{x}{\left( \log x \right)^{c - c_{1/2}}} + \frac{x}{\left( \log x \right)^{c_{1/2}}} + x^{1/2} \left( \log x \right)^{1/2} Q + Q^2 U^{3/2} \log^3 x + U^2 Q^{3/2} \log^3 x.
\]

Take \( C = A + 15/2 \), \( U = \left( \log x \right)^{2A + 15} \), \( Q = x^{1/2} \left( \log x \right)^{-B} \), \( B = A + 15/2 \), and the above is \( O \left( \frac{x}{\left( \log x \right)^{A}} \right) \).
Theorem BDH (Baker, Davenport - Halberstam (1966))

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

$$\sum_{g \leq Q} \frac{1}{\varphi(g)} \sum_{\substack{\alpha \leq 1 \\ (n, q) = 1}} \left( \psi(x, q, a) - \frac{x}{\varphi(q)} \right)^2 \ll xQ \log^2 x.$$  

Proof: Let $\psi^*(x, \chi) = \psi(x, \chi)$ if $\chi$ is nonprincipal, and $\psi^*(x, \chi_0) = \psi(x, \chi_0) - x$.

Start with $\psi(x, q, a) - \frac{x}{\varphi(q)} = \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{C}(q)} \chi(a) \psi^*(x, \chi)$.

Square both sides and sum over $a$:

$$\sum_{\alpha = 1}^q \left( \psi(x, q, a) - \frac{x}{\varphi(q)} \right)^2 = \frac{1}{\varphi(q)} \sum_{\chi_1, \chi_2 \in \mathcal{C}(q)} \psi(x, \chi_1) \psi(x, \chi_2) \sum_{\alpha = 1}^q \overline{\chi_1(a)} \chi_2(a)$$

$$= \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{C}(q)} \left| \psi(x, \chi) \right|^2.$$  

If $\chi$ is induced by primitive $\chi_1$, then (cf. proof of Lemma 6.4)

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

Summing on $g \leq Q$ we obtain

$$\sum_{g \leq Q} \sum_{\alpha = 1}^q \left| \psi(x, g, a) - \frac{x}{\varphi(g)} \right|^2 = \sum_{g \leq Q} \frac{1}{\varphi(g)} \sum_{\chi \in \mathcal{C}(g)} \left| \psi(x, \chi) \right|^2 + O(xQ \log^2 x)$$

since $|\psi^*(x, \chi)| \ll x$. The sum on the right is

$$\ll \sum_{g \leq Q} \frac{1}{\varphi(g)} \sum_{\chi \in \mathcal{C}(g)} \left| \psi^*(x, \chi) \right|^2 \sum_{\chi \in \mathcal{C}(g)} \frac{1}{\varphi(g)} = (\log x) \sum_{\chi \in \mathcal{C}(g)} \max_{\chi \leq \chi_0} \left| \psi^*(x, \chi) \right|^2 + \sum_{\chi \leq \chi_0} \frac{1}{\varphi(g)} \sum_{\chi \leq \chi_0} \left| \psi^*(x, \chi) \right|^2.$$

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

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

We find that the left side of (6.12) is

$$\ll xQ \log^2 x + (\log x) \sum_{\lambda \leq \lambda_0} \left( \frac{x^2 \log x}{2^j} + 2^i x \log x \right) \ll xQ \log^2 x.$$  

Remark: Montgomery (1970) showed that the left side of (6.12) is actually

$$\ll xQ \log x.$$