19

The Large Sieve

19.1 Analytic principles

Bessel's inequality asserts that if $\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \dots, \boldsymbol{\phi}_R$ are orthonormal vectors in an inner product space V, then

$$\sum_{r=1}^{R} |(\boldsymbol{\xi}, \boldsymbol{\phi}_r)|^2 \ \le \ \|\boldsymbol{\xi}\|^2 \tag{19.1}$$

for all $\boldsymbol{\xi} \in V$. The proof of this is quite simple: For arbitrary y_r,

$$0 \ \le \ \Big\|\boldsymbol{\xi} - \sum_{r=1}^{R} y_r \boldsymbol{\phi}_r\Big\|^2 \ = \ \|\boldsymbol{\xi}\|^2 \ - \ 2\Re \sum_{r=1}^{R} \overline{y_r}(\boldsymbol{\xi}, \boldsymbol{\phi}_r) \ + \ \Big\|\sum_{r=1}^{R} y_r \boldsymbol{\phi}_r\Big\|^2$$

$$= \ \|\boldsymbol{\xi}\|^2 \ - \ 2\Re \sum_{r=1}^{R} \overline{y_r}(\boldsymbol{\xi}, \boldsymbol{\phi}_r) \ + \ \sum_{r=1}^{R} |y_r|^2. \tag{19.2}$$

Set $y_r = (\boldsymbol{\xi}, \boldsymbol{\phi}_r)$. Then the expression (19.2) is $\|\boldsymbol{\xi}\|^2 - \sum_r |(\boldsymbol{\xi}, \boldsymbol{\phi}_r)|^2$, so the proof is complete. However, in analytic number theory we often need to estimate a sum such as the one in (19.1) but with vectors $\boldsymbol{\phi}_r$ that are not quite orthogonal. It is therefore fortunate that we can extend Bessel's inequality to arbitrary vectors $\boldsymbol{\phi}_r$ with a constant that we can characterize in terms of the extent that the inner product matrix $[(\boldsymbol{\phi}_r, \boldsymbol{\phi}_s)]$ resembles the identity matrix.

Theorem 19.1 *Let $\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \dots, \boldsymbol{\phi}_R$ be arbitrary vectors in an inner product space V. For nonnegative real numbers Δ, the following three assertions are equivalent:*
(i) *For every vector $\boldsymbol{\xi} \in V$,*

$$\sum_{r=1}^{R} |(\boldsymbol{\xi}, \boldsymbol{\phi}_r)|^2 \ \le \ \Delta^2 \|\boldsymbol{\xi}\|^2; \tag{19.3}$$

(ii) *For every vector $\boldsymbol{\xi} \in V$ and every vector $\boldsymbol{y} \in \mathbb{C}^R$,*

$$\Big|\sum_{r=1}^{R} (\boldsymbol{\xi}, \boldsymbol{\phi}_r) y_r\Big| \ \le \ \Delta \|\boldsymbol{\xi}\| \Big(\sum_{r=1}^{R} |y_r|^2\Big)^{1/2}. \tag{19.4}$$

(iii) *For every vector* $\boldsymbol{y} \in \mathbb{C}^R$,

$$\sum_{r=1}^{R}\sum_{s=1}^{R}(\boldsymbol{\phi}_r,\boldsymbol{\phi}_s)y_r\overline{y_s} \;\le\; \Delta^2\sum_{r=1}^{R}|y_r|^2\,. \tag{19.5}$$

This contains Bessel's inequality as a special case, for if the $\boldsymbol{\phi}_r$ happen to be orthonormal, then the inequality (19.5) holds as an identity with $\Delta = 1$, and then (19.3) is Bessel's inequality. The coefficient matrix $C = [(\boldsymbol{\phi}_r, \boldsymbol{\phi}_s)]$ in (19.5)is Hermitian, and so by Corollary F.11 the best constant Δ for which the inequality (19.5) holds is the modulus of the largest eigenvalue of C. This quantity is known as the *spectral radius* of C; in symbols, $\Delta = \rho(C)$.

Proof (i) $\implies$ (ii). By Cauchy's inequality,

$$\Big|\sum_{r=1}^{R}(\boldsymbol{\xi},\boldsymbol{\phi}_r)y_r\Big| \le \Big(\sum_{r=1}^{R}|(\boldsymbol{\xi},\boldsymbol{\phi}_r)|^2\Big)^{1/2}\Big(\sum_{r=1}^{R}|y_r|^2\Big)^{1/2}.$$

We apply the bound (19.3) to the first sum on the right above to obtain (19.4).
(ii) $\implies$ (iii). Take $\boldsymbol{\xi} = \sum_{r=1}^{R} y_r\boldsymbol{\phi}_r$. Then

$$\sum_{r=1}^{R}\sum_{s=1}^{R}(\boldsymbol{\phi}_r,\boldsymbol{\phi}_s)y_r\overline{y_s} \;=\; \|\boldsymbol{\xi}\|^2\,. \tag{19.6}$$

But

$$\|\boldsymbol{\xi}\|^2 = \sum_{s=1}^{R}(\boldsymbol{\xi},\boldsymbol{\phi}_s)\overline{y_s} \le \Delta\|\boldsymbol{\xi}\|\Big(\sum_{s=1}^{R}|y_s|^2\Big)^{1/2}$$

by (19.4). If $\boldsymbol{\xi} = \boldsymbol{0}$, then the left hand side of (19.5) is 0, so there is nothing to prove. Otherwise, $\|\boldsymbol{\xi}\| > 0$, so we may cancel $\|\boldsymbol{\xi}\|$ from both sides above, and then square both sides. This gives (19.5), in view of (19.6).
(iii) $\implies$ (i). We take the proof of Bessel's inequality as a model. For arbitrary y_r,

$$0 \;\le\; \Big\|\boldsymbol{\xi} - \sum_{r=1}^{R} y_r\boldsymbol{\phi}_r\Big\|^2 \;=\; \|\boldsymbol{\xi}\|^2 \;-\; 2\Re\sum_{r=1}^{R}\overline{y_r}(\boldsymbol{\xi},\boldsymbol{\phi}_r) \;+\; \Big\|\sum_{r=1}^{R} y_r\boldsymbol{\phi}_r\Big\|^2.$$

Here the last term is

$$\sum_{r=1}^{R}\sum_{s=1}^{R}(\boldsymbol{\phi}_r,\boldsymbol{\phi}_s)y_r\overline{y_s}\,.$$

Thus by (iii) we see that

$$0 \;\le\; \|\boldsymbol{\xi}\|^2 \;-\; 2\Re\sum_{r=1}^{R}\overline{y_r}(\boldsymbol{\xi},\boldsymbol{\phi}_r) \;+\; \Delta^2\sum_{r=1}^{R}|y_r|^2\,.$$

By taking $y_r = (\boldsymbol{\xi}, \boldsymbol{\phi}_r)/\Delta^2$ we find that

$$0 \;\le\; \|\boldsymbol{\xi}\|^2 \;-\; \frac{1}{\Delta^2}\sum_{r=1}^{R} |(\boldsymbol{\xi}, \boldsymbol{\phi}_r)|^2,$$

which gives (i). □

If the $\boldsymbol{\phi}_r$ are nearly orthonormal in the sense that the inner product matrix C is nearly the identity matrix, then we would expect that (19.3) holds with a constant not much larger than 1. The most immediate observation in this direction is as follows.

Theorem 19.2 *In the notation of Theorem* 19.1*, the inequalities* (19.3)–(19.5) *hold with*

$$\Delta^2 = \max_{1\le r\le R} \sum_{s=1}^{R} |(\boldsymbol{\phi}_r, \boldsymbol{\phi}_s)|\,. \tag{19.7}$$

Proof By the arithmetic–geometric mean inequality we know that $|y_r y_s| \le \frac{1}{2}|y_r|^2 + \frac{1}{2}|y_s|^2$. Thus

$$\begin{aligned}
\sum_{r=1}^{R}\sum_{s=1}^{R} (\boldsymbol{\phi}_r, \boldsymbol{\phi}_s) y_r \overline{y_s} \;&\le\; \sum_{r=1}^{R}\sum_{s=1}^{R} |(\boldsymbol{\phi}_r, \boldsymbol{\phi}_s) y_r \overline{y_s}| \\
&\le\; \sum_{r=1}^{R} |y_r|^2 \;\sum_{s=1}^{R} |(\boldsymbol{\phi}_r, \boldsymbol{\phi}_s)| \\
&\le\; \Big(\max_{1\le r\le R} \sum_{s=1}^{R} |(\boldsymbol{\phi}_r, \boldsymbol{\phi}_s)| \Big) \sum_{r=1}^{R} |y_r|^2\,.
\end{aligned}$$

Thus (19.5) holds with Δ as in (19.7), so the proof is complete. □

Of the various situations in which near orthogonality occurs, we select three for detailed treatment.

1. Trigonometric polynomials. If we need to know that a trigonometric polynomial is not often large, then we might seek a bound for

$$\sum_{r=1}^{R} \Big| \sum_{n=1}^{N} c_n e(n x_r) \Big|^2$$

where the x_r are well-spaced (mod 1). Here we take $\boldsymbol{\xi} = (c_n) \in \mathbb{C}^N$, and the $\boldsymbol{\phi}_r = (e(-n x_r)) \in \mathbb{C}^N$ are nearly orthogonal if $\|x_r - x_s\|$ is large compared with $1/N$ whenever $r \ne s$.

2. Arithmetic progressions. If we want to understand how some numbers c_n are distributed when n is restricted to various arithmetic progressions $a_r \pmod{q_r}$, then we might seek a bound for the expression

$$\sum_{r=1}^{R} \Big| \sum_{\substack{n=1 \\ n\equiv a_r\ (q_r)}}^{N} c_n - \frac{1}{q_r}\sum_{n=1}^{N} c_n \Big|^2.$$

Here $\boldsymbol{\xi} = (c_n) \in \mathbb{C}^N$ and the $\boldsymbol{\phi}_r = (\phi_{r\,n}) \in \mathbb{C}^N$ given by

$$\phi_{r\,n} = \begin{cases} 1 - 1/q_r & \text{if } n \equiv a_r \pmod{q_r} \\ -1/q_r & \text{otherwise} \end{cases}$$

are nearly orthogonal if the q_r are pairwise coprime.

3. Character sums. In order to show that a character sum is not too large on average, we might seek a bound for the expression

$$\sum_{r=1}^{R} \Big| \sum_{n=1}^{N} c_n \chi_r(n) \Big|^2$$

where the χ_r run over a family of Dirichlet characters. Then we take $\boldsymbol{\xi} = (c_n) \in \mathbb{C}^N$, and we expect the $\boldsymbol{\phi}_r = (\overline{\chi_r}(n)) \in \mathbb{C}^N$ to be nearly orthogonal if $\overline{\chi_r}\chi_s$ is nonprincipal whenever $r \neq s$.

The desired approximate orthogonality is a little elusive in the second two cases above, but is easy to establish in the first. Thus we start by treating trigonometric polynomials, and then derive information concerning arithmetic progressions by means of the finite Fourier transform, and for characters by means of Gauss sums.

19.1.1 Exercises

1. The object of this exercise is to derive Theorem 19.1 as an application of the duality principle of Theorem F.1. Let $\boldsymbol{e}_1, \boldsymbol{e}_2, \dots, \boldsymbol{e}_K$ be an orthonormal basis for $W = \operatorname{span}(\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \dots, \boldsymbol{\phi}_R)$, and write

$$\boldsymbol{\phi}_r = \sum_{k=1}^{K} a_{rk} \boldsymbol{e}_k$$

(a) Show that

$$\sum_{r=1}^{R} \sum_{s=1}^{R} (\boldsymbol{\phi}_r, \boldsymbol{\phi}_s) y_r \overline{y_s} = \Big\| \sum_{r=1}^{R} y_r \boldsymbol{\phi}_r \Big\|^2 = \sum_{k=1}^{K} \Big| \sum_{r=1}^{R} a_{rk} y_r \Big|^2 .$$

(b) Put $v_k = (\boldsymbol{\xi}, \boldsymbol{e}_k)$, and define $\boldsymbol{\zeta}$ so that

$$\boldsymbol{\xi} = \boldsymbol{\zeta} + \sum_{k=1}^{K} v_k \boldsymbol{e}_k \, .$$

Thus $\boldsymbol{\zeta} \in W^{\perp}$. Show that

$$(\boldsymbol{\xi}, \boldsymbol{\phi}_r) = \sum_{k=1}^{K} \overline{a_{rk}}\, v_k \, .$$

(c) Deduce that

$$\sum_{r=1}^{R}(\boldsymbol{\xi},\boldsymbol{\phi}_r)y_r = \sum_{r=1}^{R}\sum_{k=1}^{K}\overline{a_{rk}}y_r v_k,$$

and also that

$$\sum_{r=1}^{R}|(\boldsymbol{\xi},\boldsymbol{\phi}_r)|^2 = \sum_{r=1}^{R}\Big|\sum_{k=1}^{K}\overline{a_{rk}}v_k\Big|^2.$$

(d) Show that

$$\sum_{k=1}^{K}|v_k|^2 \le \|\boldsymbol{\xi}\|^2.$$

(e) Use Theorem F.1 to prove Theorem 19.1.

2. The object of this exercise is to use Theorem 19.1 to prove Theorem F.1. Let $\boldsymbol{\xi} = (x_1, x_2, \dots, x_N) \in \mathbb{C}^N$, and for $r = 1, 2, \dots, R$ take $\boldsymbol{\phi}_r = (a_{r1}, a_{r2}, \dots, a_{rN})$.
(a) Explain why

$$\sum_{r=1}^{R}|(\boldsymbol{\xi},\boldsymbol{\phi}_r)|^2 = \sum_{r=1}^{R}\Big|\sum_{n=1}^{N}a_{rn}x_n\Big|^2.$$

(b) Show that

$$\sum_{r=1}^{R}(\boldsymbol{\xi},\boldsymbol{\phi}_r)y_r = \sum_{r=1}^{R}\sum_{n=1}^{N}a_{rn}x_n y_r\,.$$

(c) Explain why

$$\Big\|\sum_{r=1}^{R}y_r\boldsymbol{\phi}_r\Big\|^2 = \sum_{n=1}^{N}\Big|\sum_{r=1}^{R}a_{rn}y_r\Big|^2.$$

(d) Use Theorem 19.1 to prove Theorem F.1.

3. (Selberg, unpublished; cf Bombieri 1971) Let $\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \dots, \boldsymbol{\phi}_R$ be elements of an inner product space V.
(a) Show that for any $\boldsymbol{\xi} \in V$,

$$\sum_{r=1}^{R}|(\boldsymbol{\xi},\boldsymbol{\phi}_r)|^2\Big(\sum_{s=1}^{R}|(\boldsymbol{\phi}_r,\boldsymbol{\phi}_s)|\Big)^{-1} \;\le\; \|\boldsymbol{\xi}\|^2\,.$$

(b) Use the above to derive Theorem 19.2.

4. Let $\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \dots, \boldsymbol{\phi}_R$ and $\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \dots, \boldsymbol{\psi}_S$ be any members of an inner product space V. Show that

$$\sum_{r=1}^{R}\sum_{s=1}^{S}|(\boldsymbol{\phi}_r,\boldsymbol{\psi}_s)|^2 \le \Big(\sum_{r_1=1}^{R}\sum_{r_2=1}^{R}|(\boldsymbol{\phi}_{r_1},\boldsymbol{\phi}_{r_2})|^2\Big)^{1/2}\Big(\sum_{s_1=1}^{S}\sum_{s_2=1}^{S}|(\boldsymbol{\psi}_{s_1},\boldsymbol{\psi}_{s_2})|^2\Big)^{1/2}.$$

19.2 Trigonometric polynomials

Let

$$T(x) = \sum_{n=M+1}^{M+N} c_n e(nx) \tag{19.8}$$

be a trigonometric polynomial. Suppose that $\delta > 0$, and that the points x_r are well-spaced (mod 1) in the sense that

$$\|x_r - x_s\| \geq \delta \tag{19.9}$$

whenever $r \neq s$. We seek an inequality of the form

$$\sum_{r=1}^{R} |T(x_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |c_n|^2, \tag{19.10}$$

which is to hold for all possible choices of the c_n. Our object is to determine how Δ must depend on N and δ. When $R = 1$ it is easy to establish an inequality of this form, since by Cauchy's inequality

$$|T(x_1)|^2 \leq N \sum_{n=M+1}^{M+N} |c_n|^2. \tag{19.11}$$

This is best possible, for if $c_n = e(-nx_1)$, then $T(x_1) = N$. Thus if (19.10) holds for all c_n, then $\Delta \geq N$. We also observe that

$$\int_0^1 \sum_{r=1}^{R} |T(x + r/R)|^2 \, dx = R \int_0^1 |T(x)|^2 \, dx = R \sum_{n=M+1}^{N} |c_n|^2.$$

Hence there is an x for which

$$\sum_{r=1}^{R} |T(x + r/R)|^2 \geq R \sum_{n=M+1}^{N} |c_n|^2.$$

For any given $\delta > 0$ we can choose $R = [1/\delta]$, and then the points $x + r/R$ satisfy (19.9). Hence if Δ satisfies (19.10), then $\Delta \geq R \geq 1/\delta - 1$.

We now show that (19.10) holds with a value of Δ not much larger than necessitated by the above considerations. Our first result in this direction is somewhat inferior, but the approach is very direct, and generalizes usefully to other situations. For each r let $\mathfrak{M}_r = (x_r - \delta/2, x_r + \delta/2)$ be a short interval centred at x_r. We note that if the x_r satisfy (19.9), then the intervals $\mathfrak{M}_r$ are disjoint (mod 1). The idea is that $|T(x_r)|^2$ approximately the average of $|T(x)|^2$ over $\mathfrak{M}_r$ unless $T'(x)$ is very large, in which case the integral of $|T'(x)|^2$ over $\mathfrak{M}_r$ is large. To put this intuitive principle on a sound footing we prove

Lemma 19.3 *If $f'(x)$ is continuous on $[-a,a]$, then*

$$|f(0)| \le \frac{1}{2a}\int_{-a}^{a} |f(x)|\,dx + \frac{1}{2}\int_{-a}^{a} |f'(x)|\,dx.$$

Proof By integration by parts we see that

$$\int_0^a f(x)\,dx = f(x)(x-a)\Big|_0^a - \int_0^a f'(x)(x-a)\,dx = af(0) - \int_0^a f'(x)(x-a)\,dx,$$

and similarly that

$$\int_{-a}^0 f(x)\,dx = f(x)(x+a)\Big|_{-a}^0 - \int_{-a}^0 f'(x)(x+a)\,dx = af(0) - \int_{-a}^0 f'(x)(x+a)\,dx.$$

On summing we deduce that

$$2af(0) = \int_{-a}^a f(x)\,dx + \int_{-a}^0 f'(x)(x+a)\,dx + \int_0^a f'(x)(x-a)\,dx.$$

Hence by the triangle inequality

$$|f(0)| \le \frac{1}{2a}\int_{-a}^{a} |f(x)|\,dx + \frac{1}{2a}\int_{-a}^{0} |f'(x)(x+a)|\,dx + \frac{1}{2a}\int_{0}^{a} |f'(x)(x-a)|\,dx.$$

Since $|x+a| \le a$ for $-a \le x \le 0$ and $|x-a| \le a$ for $0 \le x \le a$, this gives the result. □

Suppose that $U(x)$ is a trigonometric polynomial of the special form

$$U(x) = \sum_{k=-K}^{K} b_k e(kx).$$

By applying the Lemma with $f(x) = U(x+x_r)^2$, $a = \delta/2$, and summing, we deduce that

$$\begin{aligned}\sum_{r=1}^R |U(x_r)|^2 &\le \frac{1}{\delta}\sum_{r=1}^R \int_{\mathfrak{M}_r} |U(x)|^2\,dx + \sum_{r=1}^R \int_{\mathfrak{M}_r} |U(x)U'(x)|\,dx \\ &\le \frac{1}{\delta}\int_0^1 |U(x)|^2\,dx + \int_0^1 |U(x)U'(x)|\,dx\end{aligned}$$

since the intervals $\mathfrak{M}_r$ are non-overlapping (mod 1). Here the first integral is $\sum |b_k|^2$. By the Cauchy–Schwarz inequality the second integral is

$$\le \Big(\int_0^1 |U(x)|^2\,dx\Big)^{1/2}\Big(\int_0^1 |U'(x)|^2\,dx\Big)^{1/2} = \Big(\sum_{-K}^K |b_k|^2\Big)^{1/2}\Big(\sum_{-K}^K |2\pi i k b_k|^2\Big)^{1/2}.$$

Since $|2\pi ik| \le 2\pi K$ for $-K \le k \le K$, the above is $\le 2\pi K \sum |b_k|^2$. That is,

$$\sum_{r=1}^R \Big|\sum_{k=-K}^K b_k e(kx_r)\Big|^2 \le \Big(\frac{1}{\delta} + 2\pi K\Big)\sum_{k=-K}^K |b_k|^2.$$

This is a special case of (19.10). To obtain the general case let $K = [N/2]$, put $L = K + M + 1$, and set $U(x) = T(x)e(-Lx)$. Then $U(x)$ is of the required shape, $|U(x)| = |T(x)|$, and $2K \le N$, so we have proved

Theorem 19.4 *Suppose that M and N are integers, $N \geq 1$, and that $T(x)$ is a trigonometric polynomial as given in* (19.8)*. Suppose that $\delta > 0$, and that the points x_r are well-spaced in the sense that* (19.9) *holds. Then*

$$\sum_{r=1}^{R} |T(x_r)|^2 \leq \Big(\frac{1}{\delta} + \pi N\Big) \sum_{n=M+1}^{M+N} |c_n|^2.$$

For purposes of estimating character sums, the above estimate is perfectly satisfactory, but when dealing with arithmetic progressions the coefficient of N on the right hand side becomes important. To optimize this dependence we adopt a different line of attack. The quantity to be estimated is a bilinear form in the coefficients c_n. Often when presented with the problem of estimating a bilinear form we simply expand, take the outer summation inside, and estimate the resulting innermost sum:

$$\sum_{r=1}^{R} \Big| \sum_{n=M+1}^{M+N} c_n e(nx_r)\Big|^2 = \sum_{m=M+1}^{M+N} \sum_{n=M+1}^{M+N} c_m \overline{c_n} \sum_{r=1}^{R} e((m-n)x_r).$$

Unfortunately, we have little control over the inner sum on the right, so this approach, in its most direct form, leads nowhere. However, every bilinear form inequality has a dual, and we have the option of passing to the dual before performing the above manipulations. More precisely, by Theorem F.1 we see that the inequality (19.10) holds for all choices of the c_n if and only if

$$\sum_{n=M+1}^{M+N} \Big| \sum_{r=1}^{R} y_r e(nx_r)\Big|^2 \leq \Delta \sum_{r=1}^{R} |y_r|^2 \tag{19.12}$$

for all y_r. On expanding and taking the sum over n inside we find that the above is

$$\sum_{r=1}^{R} \sum_{s=1}^{R} y_r \overline{y_s} \sum_{n=M+1}^{M+N} e(n(x_r - x_s)).$$

By applying (18.30) to estimate the innermost sum we could demonstrate that $\Delta \leq N + O(\delta^{-1} \log \delta^{-1})$, which is good for N but inferior for δ. The extra logarithm results from the the inverse first power decay of the exponential sum, which in turn is attributable to the jump discontinuity of the characteristic function $\chi_{\mathcal{J}}(x)$ of the interval $\mathcal{J} = [M+1, M+N]$. To obtain an exponential sum that decays faster, we introduce a smooth weighting factor.

Theorem 19.5 *Suppose that M and N are integers, $N \geq 1$, and that $T(x)$ is a trigonometric polynomial as given by* (19.8)*. Suppose that $0 < \delta \leq 1$, and that the points x_r are well-spaced in the sense that* (19.9) *holds. Then*

$$\sum_{r=1}^{R} |T(x_r)|^2 \leq \Big(N + \frac{1}{\delta} - 1\Big) \sum_{n=M+1}^{M+N} |c_n|^2.$$

Proof If $R = 1$, then we have the stated result by Cauchy's inequality, as in (19.11). If $R \geq 2$, then $\delta \leq 1/2$. We proceed to (19.12), but before expanding we introduce a weighting factor $w(n)$. If $\chi_{\mathcal{J}}(n) \leq w(n)$ for all n, then the left hand side of (19.12) is

$$\leq \sum_n w(n) \Big| \sum_{r=1}^{R} y_r e(nx_r) \Big|^2 = \sum_{r=1}^{R} \sum_{s=1}^{R} y_r \overline{y_s} \sum_n w(n) e(n(x_r - x_s)).$$

Let the innermost sum be $W(x_r - x_s)$. If $w(n)$ is piecewise linear, then $W(x)$ decays like an inverse square, and by choosing parameters carefully one may show that $\Delta \leq N + 2/\delta$. However, by employing the more sophisticated weighting given in Theorem E.4 we find that we can actually ensure that $W(x) = 0$ for $\|x\| \geq \delta$, so that the bilinear form above consists only of diagonal terms. Moreover, with this choice of the $w(n)$ we find that $W(0) = N - 1 + 1/\delta$, so the proof is complete. □

In most arithmetic applications of the large sieve, the x_r are rational numbers whose denominators are limited in size, as below.

Corollary 19.6 *Let M and N be integers, $N \geq 1$, and suppose that $T(x)$ is a trigonometric polynomial of the form* (19.8)*. Then for any positive integer Q,*

$$\sum_{q=1}^{Q} \sideset{}{^*}\sum_{a=1}^{q} |T(a/q)|^2 \leq (N + Q^2) \sum_{n=M+1}^{M+N} |c_n|^2.$$

Proof If a/q and a'/q' are distinct rational numbers, then

$$\Big| \frac{a}{q} - \frac{a'}{q'} \Big| = \Big| \frac{aq' - a'q}{qq'} \Big| \geq \frac{1}{qq'}$$

since $aq' - a'q$ is a non-zero integer. If $q \leq Q$ and $q' \leq Q$, then the above is $\geq 1/Q^2$, so we may apply Theorem 19.5 with $\delta = 1/Q^2$. □

19.2.1 Exercises

1. Suppose that $f'(x)$ is continuous for $0 \leq x \leq 1$.
   (a) Show that if $0 \leq x \leq 1$, then

$$f(x) = \int_0^1 f(u)\, du + \int_0^x f'(u) u\, du + \int_x^1 f'(u)(u-1)\, du.$$

   (b) Deduce that

$$\max_{0 \leq x \leq 1} |f(x)| \leq \int_0^1 |f(u)|\, du + \int_0^1 |f'(u)|\, du.$$

2. Suppose that $f(x,y)$ has continuous derivatives through the second order on $[0,1]^2$.
(a) Show that if $0 \le x \le 1$ and $0 \le y \le 1$, then

$$|f(x,y)| \le \int_0^1 \int_0^1 |f(u,v)| + |f_1(u,v)| + |f_2(u,v)| + |f_{12}(u,v)|\, du\, dv.$$

(b) Show that

$$|f(1/2,1/2)| \le \int_0^1 \int_0^1 |f(u,v)| + \frac{1}{2}|f_1(u,v)| + \frac{1}{2}|f_2(u,v)| + \frac{1}{4}|f_{12}(u,v)|\, du\, dv.$$

3. (a) Suppose that $\int_0^\infty f(x)\, dx$ is a convergent improper Riemann sum. Show that if $f'(x) \to 0$ as $x \to \infty$, then $f(x) \to \infty$.
(b) Show that if $f(x) \to 0$ as $x \to \infty$ and $f''(x) \to 0$ as $x \to \infty$, then $f'(x) \to 0$ as $x \to \infty$.

4. Let $x_1, x_2, \dots, x_R$ be points in $\mathbb{T}$. For $\delta > 0$ let $N_\delta(x)$ denote the number r for which $\|x_r - x\| < \delta$.
(a) Show that

$$\sum_{\substack{1 \le r \le R \\ \|x_r - x\| \le \delta/2}} \frac{1}{N_\delta(x_r)} \le 1$$

for all $x \in \mathbb{T}$.
(b) Show that if M and N are integers, $N \ge 1$, and $T(x)$ is given by (19.8), then

$$\sum_{r=1}^R \frac{|T(x_r)|^2}{N_\delta(x_r)} \le \Big(\frac{1}{\delta} + \pi N\Big) \sum_{n=M+1}^{M+N} |c_n|^2$$

for all $\delta > 0$.
(c) Show that the above includes Theorem 19.2.

5. Let μ be a non-negative measure on $\mathbb{T}$.
(a) Show that if $T(x)$ is given as in (19.8), and if $\delta > 0$, then

$$\int_{\mathbb{T}} |T(x)|^2\, d\mu(x) \le \Big(\max_{x \in \mathbb{T}} \mu((x - \delta/2, x + \delta/2))\Big)\Big(\frac{1}{\delta} + \pi N\Big) \sum_{n=M+1}^{M+N} |c_n|^2.$$

(b) Derive Theorem 19.4 from the above.

6. Suppose that $\delta > 0$ and that the points x_r satisfy (19.9). Show that for any y_r there is a number θ, $-1 \le \theta \le 1$ such that

$$\sum_{n=M+1}^{M+N} \Big| \sum_{r=1}^R y_r e(n x_r) \Big|^2 = \Big(N - 1 + \frac{\theta}{\delta}\Big) \sum_{r=1}^R |y_r|^2.$$

7. (Montgomery 1978) Let M and $N \geq 1$ be integers, and suppose that $T(x)$ is given by (19.8). For given positive integers Q, X, let $\Delta = \Delta(N, Q, X)$ be the optimal constant in the inequality

$$\sum_{q \in \mathcal{Q}} \sideset{}{^*}\sum_{a=1}^{q} |T(a/q)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |c_n|^2$$

where the c_n are arbitrary and $\mathcal{Q}$ is a set of X positive integers not exceeding Q. Show that $\Delta(N, Q, X) \asymp \min(N + Q^2, X(N + Q))$.

8. (Burgess 1971) Let $N_\delta(x)$ be defined as in Exercise 4, but take the x_r to be as in the preceding exercise, namely the points a/q with $(a, q) = 1$ and $q \in \mathcal{Q}$.
(a) Show that if $\delta = (QX)^{-1}$, then

$$\sum_{q \in \mathcal{Q}} \sideset{}{^*}\sum_{a=1}^{q} N_\delta(a/q) \ll QX.$$

(b) By using Cauchy's inequality and applying the above and Exercise 4, show that

$$\sum_{q \in \mathcal{Q}} \sideset{}{^*}\sum_{a=1}^{q} |T(a/q)| \ll \left(QX(N + QX) \sum_{n=M+1}^{M+N} |c_n|^2 \right)^{1/2}.$$

19.3 Mean square distribution in arithmetic progressions

Suppose that we have a sequence of numbers c_n for $M+1 \leq n \leq M+N$. We now consider how these numbers are distributed when n falls in various arithmetic progressions. Let

$$Z(q, h) = \sum_{\substack{n=M+1 \\ n \equiv h \ (q)}}^{M+N} c_n. \tag{19.13}$$

If $T(x)$ is given as in (19.8), then

$$T(a/q) = \sum_{h=1}^{q} Z(q, h) e(ah/q),$$

and hence by the orthogonality of the additive characters (mod q) (or, in other words, Parseval's identity for the finite Fourier transform, as we treated in §4.1) it follows that

$$\sum_{a=1}^{q} |T(a/q)|^2 = q \sum_{h=1}^{q} |Z(q, h)|^2.$$

In Corollary 19.6 the $a \pmod q$ are restricted to reduced residue classes, so some alteration is required before we can appeal to that estimate. To that end, put

$$Z = Z(1,0) = T(0) = \sum_{n=M+1}^{M+N} c_n. \tag{19.14}$$

Thus the average of the $Z(q,h)$ is Z/q. It is natural to consider the mean square difference of the $Z(q,h)$ from its mean (called the 'variance' in probability theory). We note that

$$\sum_{h=1}^{q} |Z(q,h) - Z/q|^2 = \sum_{h=1}^{q} |Z(q,h)|^2 - 2\Re\frac{\overline{Z}}{q}\sum_{h=1}^{q} Z(q,h) + \frac{|Z|^2}{q}.$$

Here the second sum on the right hand side is Z, so the above is

$$= \sum_{h=1}^{q} |Z(q,h)|^2 - \frac{|Z|^2}{q} = \frac{1}{q}\sum_{a=1}^{q} |T(a/q)|^2 - \frac{|T(0)|^2}{q} = \frac{1}{q}\sum_{a=1}^{q-1} |T(a/q)|^2. \tag{19.15}$$

This is a step in the right direction, since now the a are restricted to non-zero residue classes (mod q). Moreover, if q is prime, then the reduced residue classes and the non-zero residue classes coincide. This permits us to prove

Theorem 19.7 *Let $\mathcal{N}$ be a set of Z integers in the interval $[M+1, M+N]$. Let $Z(q,h)$ denote the number of $n \in \mathcal{N}$ such that $n \equiv h \pmod q$. Then for any positive integer Q,*

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

Proof Take $c_n = 1$ if $n \in \mathcal{N}$, and $c_n = 0$ otherwise. In (19.15), replace q by p, sum over $p \le Q$, and then apply Corollary 19.6. □

From the above estimate we see that most of the numbers $Z(p,h)$ are near their mean, Z/p. In particular, we note the following consequence.

Corollary 19.8 *Let $\mathcal{N}$ be a set of Z integers in the interval $[M+1, M+N]$. Choose τ, $0 < \tau \le 1$, and let $\mathcal{P}$ denote the set of primes $p \le Q$ such that $Z(p,h) = 0$ for at least τp residue classes $h \pmod p$. Put $P = \mathrm{card}(\mathcal{P})$. Then*

$$Z \le \frac{N + Q^2}{\tau P}.$$

Here we at last see how the large sieve got its name: We are estimating how many integers remain in an interval after a large amount of sifting has been done. We find, not surprisingly, that Z must be small if P is large, and *vice versa*.

Proof If $p \in \mathcal{P}$, then the inner sum in Theorem 19.7 is $(Z/p)^2$ for at least τp values of h. Hence the prime p contributes at least τZ^2 to the left hand side, so we see that

$$\tau P Z^2 \le (N + Q^2)Z.$$

If $Z = 0$, then there is nothing to prove. Otherwise $Z > 0$, and we may cancel Z from both sides to obtain the stated inequality. □

To exemplify the sorts of arithmetic applications that these tools might find, we apply Corollary 19.8 to show that the least quadratic non-residue of a prime $p > 2$ is not often very large. For an odd prime p, let $n_2(p)$ denote the least positive quadratic non-residue. The distribution of this quantity is quite easy to determine: We first observe that $n_2(p)$ is a prime number, for if $n_2(p) = ab$, then $\left(\frac{ab}{p}\right) = -1$, and hence $\left(\frac{a}{p}\right) = -1$ or $\left(\frac{b}{p}\right) = -1$. We note by quadratic reciprocity that $n_2(p) = 2$ if $p \equiv \pm 1 \pmod 8$, which by the prime number theorem for arithmetic progressions is the case for asymptotically $1/2$ of the primes p. Also, $n_2(p) = 3$ if $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = -1$. That is, either $p \equiv 3 \pmod 8$ and $\left(\frac{p}{3}\right) = 1$ or if $p \equiv 5 \pmod 8$ and $\left(\frac{p}{3}\right) = -1$. Hence $n_2(p) = 3$ for asymptotically $1/4$ of the primes. Let $p_1 < p_2 < p_3 < \dots$ be the prime numbers listed in increasing order. Then by continuing in this way we see that $n_2(p) = p_k$ for asymptotically 2^{-k} of the primes. Using the Siegel-Walfisz theorem (Corollary 11.19) to the modulus $q = 4\prod_{j=1}^{k} p_j < e^{(1+\varepsilon)k\log k}$, we can state this quantitatively:

$$\operatorname{card}\{p \le x : n_2(p) = p_k\} = \frac{\operatorname{li} x}{2^k} + O\big(x\exp(-c\sqrt{\log x})\big) \tag{19.16}$$

for $p_k \ll \log\log x$. For somewhat larger k we can appeal to the Brun–Titchmarsh inequality (Theorem 3.9). Thus we see that

$$\operatorname{card}\{p \le x : n_2(p) \ge p_k\} \ll \frac{x}{2^k \log x} \tag{19.17}$$

uniformly for $p_k \le \frac{1}{2}\log x$. The presumption that this bound might hold for still larger p_k suggests the conjecture that

$$n_2(p) \le (1 + o(1))(\log p)\log\log p \tag{19.18}$$

for all odd primes p. This is stronger than the bound we derived from the Generalized Riemann Hypothesis (cf Theorem 13.11). To bound the frequency with which $n_2(p)$ might be larger, we employ Corollary 19.8.

Theorem 19.9 *Let a be fixed, $a > 2$. The number of primes $p \le x$ for which $n_2(p) > (\log p)^a$ is $< x^{2/a+o(1)}$.*

Proof We apply Corollary 19.8 with $N = Q^2$, $\mathcal{N} = \{n \in [1, N] : p|n \Rightarrow p < (\log Q/2)^a\}$, and $\mathcal{P} = \{p \in (Q/2, Q] : n_2(p) > (\log p)^a\}$. Thus if $n \in \mathcal{N}$ and $p \in \mathcal{P}$, then all the prime factors of n are so small that they are quadratic residues (mod p), and hence $\left(\frac{n}{p}\right) = 1$. Hence $Z(p, h) = 0$ for at least $(p + 1)/2$ residue classes $h \pmod p$, and so we may take $\tau = 1/2$. By Corollary 7.9 we know that $Z = N^{1-1/a+o(1)}$. Consequently $P \ll N^{1/a+o(1)} = Q^{2/a+o(1)}$. To complete the proof it suffices to set $Q = 2^{-j}x$ and sum over $j = 0, 1, 2, \dots$. □

We recall from Chapter 9 that Vinogradov's Hypothesis asserts that $n_2(p) \ll_\varepsilon p^\varepsilon$ for all $\varepsilon > 0$. Although this has not yet been proved for all p, we can use the above method to show that any possible exceptions are exceedingly rare.

Theorem 19.10 (Linnik) *If $\delta > 0$, then the number of primes $p \le x$ for which $n_2(p) > p^\delta$ is $\ll_\delta \log\log x$.*

Proof Let $\mathcal{P}$ be the set of primes p, $Q^{1/2} < p \le Q$, for which $n_2(p) > p^\delta$. We show that $P \ll_\delta 1$; then the stated result follows on summing over $Q = x^{1/2^j}$. Put $N = Q^2$, and let $\mathcal{N}$ be the set of integers n, $1 \le n \le N$, composed entirely of prime numbers not exceeding $N^{\delta/4}$. As in the preceding proof we may take $\tau = 1/2$ in Corollary 19.8. By Dickman's theorem (Theorem 7.2) we know that $Z \gg_\delta N$. Hence by Corollary 19.8 we see that $P \ll_\delta 1$, and the proof is complete. □

Since we have determined the distribution function of the $n_2(p)$, and have also shown that large values of $n_2(p)$ are rare, we can deduce that a moment of the $n_2(p)$ tends to the moment of the distribution function.

Theorem 19.11 (Erdős) *Suppose that $\delta \ge 0$ is chosen so that $n_2(p) < p^{\delta+\varepsilon}$ for all $p > p_0(\varepsilon)$. Let γ be a fixed real number such that $\gamma < 1/\delta$. Then*

$$\sum_{2<p\le x} n_2(p)^\gamma \sim c(\gamma)\pi(x) \tag{19.19}$$

as x tends to infinity, where

$$c(\gamma) = \sum_{k=1}^{\infty} p_k^\gamma / 2^k.$$

From (19.19) it is easy to deduce that $n_2(p) \ll p^{1/\gamma}$, so it is to be expected that we can prove (19.19) only under the assumption that $\gamma < 1/\delta$. By our remarks following Theorem 9.27 we may take $\delta = 1/(4\sqrt{e})$. Thus it follows that (19.19) holds for all $\gamma < 4\sqrt{e} = 6.59\ldots$.

Proof By (19.16) we see that the primes $p \le x$ for which $n_2(p) \le \log\log x$ contribute to the left hand side of (19.19) an amount that is asymptotic to the right hand side of (19.19). Thus it remains to show that those p for which $n_2(p)$ is larger make a smaller contribution. Suppose that $\log\log x < p_k \le \frac{1}{2}\log x$. By (19.17) we see that the number of $p \le x$ for which $n_2(p) = p_k$ is $\ll 2^{-k}\pi(x)$. On summing this over the appropriate range of k we obtain a contribution that is $o(\pi(x))$. Next suppose that $\frac{1}{2}\log x < p_k \le (\log x)^C$ where C is to be determined later. By (19.17) we see that the number of $p \le x$ for which $n_2(p)$ falls in this range is $\ll x\exp(-c(\log x)/\log\log x)$. The maximum contribution made by such a prime is $(\log x)^C$. Since the product of these last two quantities is $o(\pi(x))$ this suffices. Finally consider primes p for which $n_2(p) > (\log x)^C$. By Theorem 19.9 the number of such primes is $< x^{2/C+\varepsilon}$. The maximum contribution made by such a prime is $< x^{\gamma(\delta+\varepsilon)}$. Hence the total contribution by all such primes is $< x^{\gamma(\delta+\varepsilon)+2/C+\varepsilon}$. Now $\gamma\delta < 1$, so we may choose $\varepsilon > 0$ so small that $\gamma(\delta+\varepsilon) \le 1-3\varepsilon$. If we take $C = 2/\varepsilon$, then the contribution in question is $< x^{1-\varepsilon} = o(\pi(x))$, so the proof is complete. □

Suppose that we try to use Theorem 19.7 as a small sieve. For example, suppose that $\mathcal{N} = \{p : N^{1/2} < p \le N\}$ and that $Q = N^{1/2}$. Then $Z(p, 0) = 0$ for all $p \le Q$, and hence we obtain the estimate

$$Z \ll \frac{N}{\sum_{p\le Q} 1/p} \ll \frac{N}{\log\log N},$$

which is vastly inferior to the bounds we obtained by Selberg's method (cf Theorem 3.3). Of course the $\log\log N$ arises because the sum is restricted to primes. If we were able to sum over all $q \le Q$, then we might expect to get a bound $O(N/\log N)$, comparable to our prior estimates. We now show that this can be done.

Lemma 19.12 *For $M+1 \le n \le M+N$ let the numbers c_n be given. For each prime p let $\mathcal{D}(p)$ be the collection of those residue classes $d \pmod p$ for which $c_n = 0$ whenever $n \equiv d \pmod p$. Let $\delta(p) = \operatorname{card}\mathcal{D}(p)$, and let $\mathcal{R}(p)$ be the complementary set of $p-\delta(p)$ residue classes $\pmod p$. For general q let $\mathcal{R}(q)$ be the collection of those residue classes $r \pmod q$ such that $r \in \mathcal{R}(p)$ for all $p|q$. Put $r(q) = \operatorname{card}\mathcal{R}(q)$. Finally, let $T(x)$, $Z(q,h)$, and Z be defined as in* (19.8), (19.13), *and* (19.14). *If q is squarefree, then*

$$\sum_{a=1}^{q}{}^{*} |T(a/q)|^2 = |Z|^2 \prod_{p|q} \frac{\delta(p)}{p-\delta(p)} + \sum_{a=1}^{q}{}^{*} \Big| \sum_{r\in\mathcal{R}(q)} e(ar/q)\big(Z(q,r) - Z/r(q)\big)\Big|^2. \tag{19.20}$$

We think of the residue classes $\mathcal{D}(p)$ as being *deleted*, so that $\mathcal{R}(q)$ is the set of residue classes that *remain*.

Proof We first show that if $k \in \mathcal{R}(q)$, then

$$\sum_{h\in\mathcal{R}(q)} c_q(h-k) = \prod_{p|q} \delta(p) \tag{19.21}$$

where $c_q(n)$ is Ramanujan's sum. By Theorem 4.1, the left hand side above is

$$\sum_{h\in\mathcal{R}(q)} \sum_{\substack{d|q \\ d|(h-k)}} d\mu(q/d) = \sum_{d|q} d\mu(q/d) \sum_{\substack{h\in\mathcal{R}(q) \\ h\equiv k\ (d)}} 1.$$

In the inner sum, $h \pmod p$ is fixed if $p|d$, but is free take on any value in $\mathcal{R}(p)$ if $p \nmid d$. Thus there are $\prod_{p|q/d}(p-\delta(p))$ such h, and hence the expression above is

$$= \sum_{d|q} d\mu(q/d) \prod_{p|q/d} \big(p-\delta(p)\big) = \prod_{p|q} \big(p - (p-\delta(p))\big),$$

and so we have (19.21).

To establish (19.20) we expand the second term on the right hand side, and find that it is

$$\begin{aligned}\sum_{a=1}^{q}{}^{*} \Big| \sum_{h\in\mathcal{R}(q)} Z(q,h)e(ah/q)\Big|^2 - 2\Re\frac{\overline{Z}}{r(q)} \sum_{a=1}^{q}{}^{*} \sum_{h\in\mathcal{R}(q)} Z(q,h) \sum_{k\in\mathcal{R}(q)} e(a(h-k)/q) \\ + \frac{|Z|^2}{r(q)^2} \sum_{a=1}^{q}{}^{*} \Big| \sum_{h\in\mathcal{R}(q)} e(ah/q)\Big|^2 \\ = T_1 - 2\Re T_2 + T_3,\end{aligned}$$

say. Clearly T_1 is equal to the left hand side of (19.20). By taking the sum over a inside and applying (19.21) we see that

$$T_2 = \frac{\overline{Z}}{r(q)} \sum_{h \in \mathcal{R}(q)} Z(q,h) \prod_{p|q} \delta(p) = \overline{Z} \Big(\prod_{p|q} \frac{\delta(p)}{p - \delta(p)} \Big) \sum_{h \in \mathcal{R}(q)} Z(q,h) = |Z|^2 \prod_{p|q} \frac{\delta(p)}{p - \delta(p)}.$$

Finally, we see that

$$T_3 = \frac{|Z|^2}{r(q)^2} \sum_{k \in \mathcal{R}(q)} \sum_{h \in \mathcal{R}(q)} c_q(h-k),$$

which by (19.21) is

$$= \frac{|Z|^2}{r(q)^2} \sum_{k \in \mathcal{R}(q)} \prod_{p|q} \delta(p).$$

The number of terms in the sum is $r(q)$, so

$$T_3 = |Z|^2 \prod_{p|q} \frac{\delta(p)}{p - \delta(p)}.$$

On combining these observations we obtain (19.20), and the proof is complete. □

Theorem 19.13 *Let $\mathcal{N}$ be a set of Z integers in the interval $M+1 \le n \le M+N$. For each prime p let $\delta(p)$ denote the number of residue classes* (mod p) *not represented by any member $n \in \mathcal{N}$. Then for any integer $Q \ge 1$,*

$$Z \le \frac{N + Q^2}{L}$$

where

$$L = \sum_{q \le Q} \mu^2(q) \prod_{p|q} \frac{\delta(p)}{p - \delta(p)}.$$

Precisely the same estimate can be obtained by Selberg's λ^2 method, if Theorem E.4 is used to eliminate the non-diagonal terms (see Exercise 5 below).

Proof By Lemma 19.12 it is clear that

$$\sum_{a=1}^{q}{}^{*} |T(a/q)|^2 \ge Z^2 \mu^2(q) \prod_{p|q} \frac{\delta(p)}{p - \delta(p)}. \tag{19.22}$$

We sum this over $q \le Q$ and apply Corollary 19.6 to see that

$$Z^2 L \le (N + Q^2) Z.$$

If $Z = 0$, then there is nothing to prove. If $Z > 0$, then we cancel Z from both sides to obtain the stated inequality. □

19.3.1 Exercises

1. Let $\mathcal{Q}$ be a set of pairwise coprime positive integers not exceeding Q, suppose that $T(x)$ is given as in (19.8), and that $Z(q,h)$ is defined by (19.13).
(a) Show that

$$\sum_{q\in\mathcal{Q}}\sum_{a=1}^{q-1}|T(a/q)|^2 \le (N+Q^2)\sum_{n=M+1}^{M+N}|c_n|^2.$$

(b) Show that

$$\sum_{q\in\mathcal{Q}} q\sum_{h=1}^{q}|Z(q,h)-Z/q|^2 \le (N+Q^2)\sum_{n=M+!}^{M+N}|c_n|^2.$$

(c) Show that this includes Theorem 19.7.

2. Let $\mathcal{R}(p)$ and $\delta(p)$ be defined as in Lemma 19.12. Show that if q is squarefree, then

$$\sum_{h=1}^{q}\Big(\prod_{\substack{p|q\\ h\in\mathcal{R}(p)}}\frac{\delta(p)}{p-\delta(p)}\Big)^2 = q\prod_{p|q}\frac{\delta(p)}{p-\delta(p)}.$$

3. Let $T(x)$ be defined as in (19.8), and $Z(q,h)$ be defined as in (19.13). Put $f(a)=T(a/q)$ if $(a,q)=1$, $f(a)=0$ otherwise. Let $\widehat{f}(h)=\frac{1}{q}\sum_{a=1}^{q}f(a)e(-ah/q)$ be the finite Fourier transform of f.
(a) Show that

$$\widehat{f}(h)=\frac{1}{q}\sum_{d|q}\mu(q/d)dZ(d,h).$$

(b) Deduce that

$$\sum_{a=1}^{q}{}^{*}|T(a/q)|^2=\frac{1}{q}\sum_{h=1}^{q}\Big|\sum_{d|q}\mu(q/d)dZ(d,h)\Big|^2.$$

4. Let $w_\pm(n)$ be defined as in Theorem E.4. Show that if $q\le 1/\delta$, then

$$\sum_{n\equiv a\,(q)} w_\pm(n) = W_\pm(0)/q$$

for all $a \pmod q$.

5. Let w_+ and W_+ be as in Theorem E.4, let $f(x)$ be a polynomial with integral coefficients, and let $\delta(p)$ denote the number of solutions of the congruence $f(x)\equiv 0 \pmod p$. Suppose that λ_d is real and subject to the conditions $\lambda_1=1$, $\lambda_d=0$ for

$d > z$. Assume that P is a positive squarefree integer.
(a) Explain why

$$\sum_{\substack{n=M+1\\(f(n),P)=1}}^{M+N} 1 \le \sum_{\substack{n\\(f(n),P)=1}} w_+(n) \le \sum_n w_+(n)\Big(\sum_{\substack{d|f(n)\\d|P}} \lambda_d\Big)^2. \tag{19.23}$$

(b) Show that if q is squarefree, then

$$\sum_{\substack{n\\q|f(n)}} w_+(n) = W_+(0)\frac{\delta(q)}{q}$$

if $q \le 1/\delta$, where $\delta(q) = \prod_{p|q}\delta(p)$.
(c) Explain why it may be assumed that $\delta(p) > 0$ for all $p|P$.
(d) Set $\delta = z^{-2}$, and show that the right hand side of (19.23) is

$$= (N - 1 + z^2)\sum_{\substack{d_i|P\\d_i\le z\\i=1,2}} \frac{\lambda_{d_1}\delta(d_1)}{d_1}\,\frac{\lambda_{d_2}\delta(d_2)}{d_2}\,\frac{(d_1,d_2)}{\delta((d_1,d_2))}. \tag{19.24}$$

(e) Put $g(q) = \prod_{p|q}(p - \delta(p))/\delta(p)$. Show that if q is squarefree, then

$$\sum_{d|q} g(d) = \frac{q}{\delta(q)}.$$

(f) Show that the right hand side of (19.24) is

$$= (N - 1 + z^2)\sum_{\substack{q|P\\q\le z}} g(q)y_q^2 \tag{19.25}$$

where

$$y_q = \sum_{\substack{d\\q|d|P\\d\le z}} \frac{\lambda_d\delta(d)}{d}. \tag{19.26}$$

(g) Show that if the y_q are given as above, then

$$\lambda_d = \frac{d}{\delta(d)}\sum_{\substack{q\\d|q|P\\q\le z}} \mu(q/d)y_q. \tag{19.27}$$

(h) Show that the y_q are real, that $y_q = 0$ if $q > z$, and that

$$\sum_{\substack{q|P\\ q\le z}} \mu(q) y_q = 1.$$

(i) Show that configurations of y_q with the properties described in the preceding part are in one-to-one correspondence with admissible choices of the λ_d.
(j) Show that the sum in (19.25) is

$$= \sum_{\substack{q|P\\ q\le z}} g(q)\Big(y_q - \frac{\mu(q)}{g(q)L}\Big)^2 + \frac{1}{L}$$

where

$$L = \sum_{\substack{q|P\\ q\le z}} \frac{\mu^2(q)}{g(q)}.$$

(k) Show that $y_q = \mu(q)/(g(q)L)$ is an admissible choice of the y_q, and hence deduce that

$$\operatorname{card}\{n \in [M+1, M+n] : (f(n), P) = 1\} \le \frac{N - 1 + z^2}{L}.$$

(l) Show that for each prime p a set $\mathcal{D}(p)$ of $\delta(p)$ residue classes is given. Show that there is a polynomial $f(x)$ such that if $p|P$, then $f(x) \equiv 0 \pmod p$ if and only if $x \in \mathcal{D}(p)$.

6. (The 'Larger Sieve' of Gallagher 1971) Let $\mathcal{N}$ be a subset of Z of the integers in an interval $[M+1, M+N]$, and let $Z(q,h)$ denote the number of $n \in \mathcal{N}$ such that $n \equiv h \pmod q$. For any primepower q let $r(q)$ denote the number of $h \pmod q$ for which $Z(q,h) > 0$.
(a) Explain why

$$Z^2 = \Big(\sum_{h=1}^{q} Z(q,h)\Big)^2 \le r(q) \sum_{h=1}^{q} Z(q,h)^2.$$

(b) Let $\mathcal{Q}$ be a finite set of primepowers. Deduce that

$$Z^2 \sum_{q\in\mathcal{Q}} \frac{\Lambda(q)}{r(q)} \le \sum_{q\in\mathcal{Q}} \Lambda(q) \sum_{\substack{n_1,n_2\in\mathcal{Q}\\ n_1\equiv n_2\ (q)}} 1.$$

(c) Group pairs n_1, n_2 of members of $\mathcal{N}$ according to their common difference, and hence show that the right hand side above is

$$= \sum_{d=-N+1}^{N-1} \sum_{\substack{n_1,n_2\in\mathcal{N}\\ n_1-n_2=d}} \sum_{\substack{q\in\mathcal{Q}\\ q|d}} \Lambda(q).$$

(d) Show that

$$\sum_{d\neq 0}\sum_{\substack{n_1,n_2\in\mathcal{N}\\ n_1-n_2=d}} 1 = Z^2 - Z.$$

(e) Deduce that the expression in (c) is

$$\leq Z\sum_{q\in\mathcal{Q}}\Lambda(q) + (Z^2-Z)\log N.$$

(f) Conclude that

$$Z \leq \frac{\sum_{q\in\mathcal{Q}}\Lambda(q) - \log N}{\sum_{q\in\mathcal{Q}}\Lambda(q)/r(q) - \log N}$$

provided that the denominator is positive.

19.4 Character sums

Let

$$S(\chi) = \sum_{n=M+1}^{M+N} c_n\chi(n). \tag{19.28}$$

We recall (cf Theorem 9.7) that if χ is a primitive character (mod q), then $\chi(n)$ can be expressed in a simple way in terms of the additive characters $e(an/q)$, namely

$$\tau(\overline{\chi})\chi(n) = \sum_{a=1}^{q}\overline{\chi}(a)e(an/q) \tag{19.29}$$

for all n. On multiplying by c_n and summing, we see that

$$\tau(\overline{\chi})S(\chi) = \sum_{a=1}^{q}\overline{\chi}(a)T(a/q)$$

where $T(x)$ is defined as in (19.8). Since $|\tau(\chi)| = \sqrt{q}$ for all primitive χ, on taking the modulus-squared and summing over primitive χ it follows that

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

where $\sum_{\chi}^{*}$ denotes a sum over all primitive characters (mod q). On the right hand side we drop the condition that χ be primitive, and invoke the orthogonality of characters (as expressed in (4.14)) to see that the above is

$$\leq \varphi(q)\sum_{a=1}^{q}{}^{*}|T(a/q)|^2$$

where $\sum_{a}^{*}$ denotes a sum over reduced residue classes $a \pmod q$. On combining this with Corollary 19.6 we obtain

Theorem 19.14 *Let M and N be integers with $N \geq 1$, and let $S(\chi)$ be defined as in (19.28). Then for any integer $Q \geq 1$,*

$$\sum_{q \leq Q} \frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\chi} |S(\chi)|^2 \leq (N + Q^2) \sum_{n=M+1}^{M+N} |c_n|^2$$

where $\sideset{}{^*}\sum_{\chi}$ denotes a sum over all primitive characters $\chi \pmod q$.

19.4.1 Exercises

1. Let χ_1 be a primitive character (mod q_1), and suppose that $q_1 \leq N$. Set $c_n = \overline{\chi}_1(n)$ for all n. Show that

$$S(\chi_1) = \sum_{n=M+1}^{M+N} |c_n|^2 \asymp N\varphi(q_1)/q_1,$$

and hence that

$$\frac{q_1}{\varphi(q_1)} |S(\chi_1)|^2 \asymp N \sum_{n=M+1}^{M+N} |c_n|^2$$

for this particular choice of the c_n.

2. (a) Show that

$$\int_0^1 \Big| \sum_{n=M+1}^{M+N} e(n\theta)\chi(n) \Big|^2 d\theta = \sum_{\substack{n=M+1 \\ (n,q)=1}}^{M+N} 1 \asymp N\varphi(q)/q$$

if $q \leq N$.
(b) Show that

$$\sum_{q \leq Q} \sideset{}{^*}\sum_{\chi} 1 \asymp Q^2.$$

(c) Deduce that there exist unimodular c_n such that

$$\sum_{q \leq Q} \sideset{}{^*}\sum_{\chi} |S(\chi)|^2 \asymp Q^2 N$$

if $Q \leq N$.

3. Recall that (19.29) holds for all χ if $(n, q) = 1$.
(a) Show that if $c_n = 0$ whenever $(n, q) > 1$, then

$$\sum_{\chi} |\tau(\chi)|^2 |S(\chi)|^2 = \varphi(q) \sideset{}{^*}\sum_{a=1}^{q} |T(a/q)|^2.$$

(b) Suppose that $c_n = 0$ whenever n has a prime factor $\le Q$. Show that

$$\sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi}|\tau(\chi)|^2|S(\chi)|^2 \le (N+Q^2)\sum_{n=M+1}^{M+N}|c_n|^2.$$

(c) Suppose that $c_n = 0$ whenever $(n,q) > 1$, and that the character $\chi \pmod q$ is induced by the primitive character $\chi^* \pmod d$. Show that $S(\chi) = S(\chi^*)$. Recall also that $\tau(\chi) = \tau(\chi^*)\mu(q/d)$ if $(q/d, d) = 1$ and that $\tau(\chi) = 0$ otherwise.
(d) Show that if the c_n are as in (b), then

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\Big(\sum_{\chi}^{*}|S(\chi)|^2\Big)\Big(\sum_{\substack{k\le Q/q\\(k,q)=1}}\frac{\mu(k)^2}{\varphi(k)}\Big) \le (N+Q^2)\sum_{n=M+1}^{M+N}|c_n|^2.$$

(e) Show that if the c_n are as in (b), then

$$\sum_{q\le Q}\big(\log Q/q\big)\sum_{\chi}^{*}|S(\chi)|^2 \le (N+Q^2)\sum_{n=M+1}^{M+N}|c_n|^2.$$

(f) Let $\mathcal{N}$ be the set of those integers $n \in [M+1, M+N]$ such that $(n,q) = 1$ for all $q \le Q$. Put $Z = \operatorname{card}\mathcal{N}$. Show that

$$Z^2\log Q + \sum_{1<q\le Q}\big(\log Q/q\big)\sum_{\chi}^{*}\Big|\sum_{n\in\mathcal{N}}\chi(n)\Big|^2 \le (N+Q^2)Z.$$

4. (a) Use results from Chapter 9 as appropriate to show that if χ is a primitive character $\pmod q$ and $(k,q) = 1$, then

$$\sum_{\substack{a=1\\(a,qk)=1}}^{qk}\overline{\chi}(a)e(an/(qk)) = \overline{\chi}(k)\chi(n)\tau(\overline{\chi})c_k(n)$$

where $c_k(n)$ is Ramanujan's sum.
(b) Show that

$$\sum_{\substack{q,k\\qk\le Q\\(q,k)=1}}\frac{q}{\varphi(qk)}\sum{}^{*}\Big|\sum_{n=M+1}^{M+N}c_n\chi(n)c_k(n)\Big|^2 = \sum_{\substack{q,k\\qk\le Q\\(q,k)=1}}\frac{1}{\varphi(qk)}\sum{}^{*}\Big|\sum_{\substack{a=1\\(a,qk)=1}}^{qk}\overline{\chi}(a)T(a/(qk))|^2\Big|^2.$$

(c) Explain why

$$\sum_{\substack{q,k\\qk\le Q}}\frac{1}{\varphi(qk)}\sum{}^{*}\Big|\sum_{\substack{a=1\\(a,qk)=1}}^{qk}\overline{\chi}(a)T(a/(qk))|^2\Big|^2 = \sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi}\Big|\sum_{a=1}^{q}\overline{\chi}(a)T(a/q)\Big|^2$$

$$= \sum_{q\le Q}\sum_{a=1}^{q}{}^{*}|T(a/q)|^2.$$

(d) (Selberg; cf p. 27 of Bombieri 1974) Conclude that

$$\sum_{\substack{q,k\\ qk\le Q\\ (q,k)=1}} \frac{q}{\varphi(qk)} \sideset{}{^*}\sum_{\chi} \Big| \sum_{n=M+1}^{M+N} c_n \chi(n) c_k(n) \Big|^2 \le (N+Q^2) \sum_{n=M+1}^{M+N} |c_n|^2.$$

(e) Show that this includes both part (d) of the preceding Exercise and also Theorem 19.14 as special cases.

5. (Erdős & Shapiro 1957) Let χ be a primitive character modulo q.
(a) Show that

$$\sum_{m=1}^{q} \chi(m+n_1)\overline{\chi}(m+n_2) = c_q(n_1-n_2)$$

where c_q is Ramanujan's sum, as defined in (4.5).
(b) Deduce that for arbitrary numbers b_n,

$$\sum_{m=1}^{q} \Big| \sum_{n=1}^{q} b_n \chi(m+n) \Big|^2 = \sum_{\substack{a=1\\ (a,q)=1}}^{q} \Big| \sum_{n=1}^{q} b_n e(an/q) \Big|^2 .$$

(c) Explain why the right hand side above is

$$\le q \sum_{n=1}^{q} |b_n|^2 . \tag{19.30}$$

(d) Show that

$$\Big| \sum_{m=1}^{q} \sum_{n=1}^{q} a_m b_n \chi(m+n) \Big|^2 \le \sqrt{q} \Big(\sum_{m=1}^{q} |a_m|^2 \Big)^{1/2} \Big(\sum_{n=1}^{q} |b_n|^2 \Big)^{1/2}$$

for arbitrary numbers a_m and b_n.
(e) Show that equality holds in (19.30) if $b_n = e(cn/q)$ with $(c,q)=1$.
(f) Show that equality holds in (19.30) if $b_n = \chi(n)$.
(g) Compare the results here with those of Exercise F.2.15.