Math 259: Introduction to Analytic Number Theory

Introduction to exponential sums; Weyl equidistribution

The "exponential" in question is the complex exponential, which we normalize with a factor of 2π and abbreviate by $e(\cdot)$:

$$e(x) := e^{2\pi i x}$$

(with $x \in \mathbf{R}$ in most cases). On occasion we also use the notation

$$e_m(x) := e(mx) = e^{2\pi i m x};$$

note that $e_1(x) = e(x)$ and $e_0(x) = 1$ for all x. An "exponential sum" is a sum of the form $\sum_{n=1}^{N} e(x_n)$ for some real numbers x_n, or more generally $\sum_{n=1}^{N} \chi(a_n) e(x_n)$ for some real x_n, integral a_n, and character χ. (We have already seen the examples of Gauss and Jacobi sums.) The general problem is to find a nontrivial estimate on such a sum, which usually means an upper bound significantly smaller than N on its absolute value. Such problems are ubiquitous in number theory, analytic and otherwise, and occasionally arise in other branches of mathematics (we mentioned [CEP 1996] in the Introduction). Sometimes these sums arise directly or nearly so; for instance, the Lindelöf conjecture concerns the size of

$$\zeta(1/2 + it) = \sum_{n=1}^{N} n^{-1/2-it} + \frac{N^{1/2-it}}{it - 1/2} + O(tN^{-1/2}),$$

so it would follow from a proof of

$$\sum_{n=1}^{\lfloor t^2 \rfloor} n^{-1/2-it} \ll |t|^{\epsilon},$$

which in turn would follow by partial summation from good estimates on

$$\sum_{n=1}^{M} n^{-it} = \sum_{n=1}^{M} e\left(\frac{t \log n}{2\pi}\right).$$

Likewise the Lindelöf conjecture for a Dirichlet L-series $L(s, \chi)$ hinges on upper bounds on $\sum_{n=1}^{M} \chi(n) e(t \log n/(2\pi))$. Often the translation of a problem to estimating exponential sums takes more work. We have already seen one example, the Pólya-Vinogradov estimate on $\sum_{n=1}^{N} \chi(n)$ (which is already an "exponential sum" as we have defined the term, with all $x_n = 0$, but whose analysis required the Gauss exponential sums). Our next example is Weyl's criterion for equidistribution mod 1.

A sequence $c_1, c_2, c_3, \ldots$ of real numbers is said to be *equidistributed mod* 1 if the fractional parts $\langle c_n \rangle$ cover each interval in $\mathbf{R}/\mathbf{Z}$ in proportion to its length; that is, if

$$\lim_{N\to\infty} \frac{1}{N} \#\{n \le N : a \le \langle c_n \rangle \le b\} = b - a \tag{1}$$

for all a, b such that $0 \le a \le b \le 1$. This is connected with exponential sums via a famous result of Weyl [1914]:

Theorem. *For a sequence* $\{c_n\}_{n=1}^{\infty}$ *in* $\mathbf{R}$ *(or equivalently in* $\mathbf{R}/\mathbf{Z}$*), the following are equivalent:*

(i) Condition (1) holds for all a, b *such that* $0 \le a \le b \le 1$*;*

(ii) For any continuous function $f : (\mathbf{R}/\mathbf{Z}) \to \mathbf{C}$*,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(c_n) = \int_0^1 f(t)\, dt; \tag{2}$$

(iii) For each $m \in \mathbf{Z}$*,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e_m(c_n) = \delta_m \left[= \int_0^1 e_m(t)\, dt \right]. \tag{3}$$

Note that (iii) is precisely the problem of nontrivially estimating an exponential sum.

Proof: (i)⇒(ii) Condition (i) means that (ii) holds when f is the characteristic function of an interval (NB such a function is not generally continuous, but it is integrable, which is enough for the sequel); also both sides of (2) are linear in f, so (ii) holds for finite linear combinations of such characteristic functions, a.k.a. step functions. If $|f(t)| < \epsilon$ for all $t \in \mathbf{R}/\mathbf{Z}$ then both sides of (2) are bounded by ϵ for all N. Thus (ii) holds for any function on $\mathbf{R}/\mathbf{Z}$ uniformly approximable by step functions. But this includes all continuous functions.

(ii)⇒(i) Estimate the characteristic function of $[a, b]$ from below and above by continuous functions whose integral differs from $b - a$ by at most ϵ.

(ii)⇒(iii) is clear because (iii) is a special case of (ii).

(iii)⇒(ii) follows from Fejér's theorem: every continuous function on $\mathbf{R}/\mathbf{Z}$ is uniformly approximated by a finite linear combination of the functions e_m. □

[NB the approximation is in general *not* an initial segment of the Fourier series for f. See [Körner 1988], chapters 1–3 (pages 3–13). The existence of uniform approximations is also a special case of the Stone-Weierstrass theorem.]

Interlude on the "little oh" notation $o(\cdot)$**.** We have gotten this far without explicitly using the "little oh" notation; this is as good a place as any to

introduce it. The notation $f = o(g)$ means that[1] ($g > 0$ and) $(f/g) \to 0$. This begs the question "approaches zero as what?", whose answer should usually be clear from context if it is not stated explicitly. Thus Weyl's theorem states that $\{c_n\}$ is equidistributed mod 1 if and only if $\sum_{n=1}^{N} e_m(c_n) = o(N)$ as $N \to \infty$ for each nonzero $m \in \mathbf{Z}$; that is, if and only if for each $m \neq 0$ we can improve on the trivial bound $|\sum_{n=1}^{N} e_m(c_n)| \leq N$ by a factor that tends to ∞ with N. For instance, we have Weyl's first application of this theorem: *For $r \in \mathbf{R}$ the sequence $\{nr\}$ is equidistributed* mod 1 *if and only if $r \notin \mathbf{Q}$*. Indeed if r is rational then $\langle nr \rangle$ takes only finitely many values; but if r is irrational then for each m we have $e_m(r) \neq 1$ and thus

$$\sum_{n=1}^{N} e_m(nr) = \frac{e_m((N+1)r) - e_m(r)}{e_m(r) - 1} = O_m(1) = o_m(N).$$

(As with $O_m(\cdot)$, the subscript in $o_m(\cdot)$ emphasizes that the convergence to 0 may not be uniform in m.) In general, we cannot reasonably hope that $\sum_{n=1}^{N} e_m(c_n)$ is bounded for each m, but we will be often able to show that the sum is $o(N)$, which suffices to prove equidistribution. For instance, we'll see that if $P \in \mathbf{R}[x]$ is a polynomial at least one of whose nonconstant coefficients is irrational then $\{P(n)\}$ is equidistributed mod 1. (This was Weyl's main application of his theorem in [Weyl 1914]; the example of $\{nr\}$ is the special case of linear polynomials.) We'll also show this for $\{\log_{10}(n!)\}$ and thus obtain the distribution of the first d digits of $n!$ for each d.

Exercises

1. (An easy variation on Weyl's theorem.) Let $A_n \subset \mathbf{R}$ be finite subsets with $\#(A_n) \to \infty$, and say that A_n is *asymptotically equidistributed modulo* 1 if

$$\lim_{n \to \infty} \frac{\#\{t \in A_n : a \leq \langle t \rangle \leq b\}}{\#(A_n)} = b - a$$

for all a, b such that $0 \leq a \leq b \leq 1$. Prove that this is the case if and only if

$$\lim_{n \to \infty} \frac{1}{\#(A_n)} \sum_{t \in A_n} e_m(t) = \delta_m.$$

Show that this condition is satisfied by A_n constructed as follows: let e_n be some positive integers, $q_n = c_n e_n + 1$ be primes such that $q_n / e_n^2 \to \infty$, and a_n arbitrary elements of $(\mathbf{Z}/q_n\mathbf{Z})^*$; and let A_n be the set of $a_n r / q_n$ for representatives r of the c_n residue classes of nonzero e_n-th powers mod q_n.

Presumably such A_n remain asymptotically equidistributed mod 1 if we require only that $q_n \gg e_n^{\theta}$ for some $\theta > 1$, but this is much harder to prove.

[1] Sometimes $g = 0$ is allowed, in which case $f = o(g)$ means that $(f/g) \to 0$, except at points where $g = 0$, at which f must also vanish. Equivalently, for all $\epsilon > 0$ it is true that eventually $|f| \leq \epsilon g$. For instance, we could use this notation to write the definition of the derivative as follows: a function F is differentiable at x if there exists $F'(x)$ such that $F(y) = F(x) + F'(x)(y - x) + o(y - x)$ as $y \to x$.

2. (Recognizing other distributions mod 1.) In Weyl's theorem suppose condition (iii) holds for all nonzero $m \neq \pm 1$, but

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e_{\pm 1}(c_n) = 1/2.$$

What can you conclude about the limits in (i) and (ii)? Generalize.

3. (Weyl in higher dimensions.) What should it mean for a sequence of vectors in $\mathbf{R}^k$ to be equidistributed mod $\mathbf{Z}^k$? Generalize Weyl's theorem to give a necessary and sufficient condition for equidistribution of a sequence in $(\mathbf{R}/\mathbf{Z})^k$. Deduce a condition on the entries of a vector $r \in \mathbf{R}^k$ that is necessary and sufficient for $\{nr\}_{n=1}^{\infty}$ to be equidistributed mod $\mathbf{Z}^k$.

4. (An application of equidistribution mod $\mathbf{Z}^k$.) Prove that $\inf_{t\in\mathbf{R}} |\zeta(\sigma+it)| = \zeta(2\sigma)/\zeta(\sigma)$ for each $\sigma > 1$, and indeed that

$$\liminf_{|t|\to\infty} |\zeta(\sigma+it)| = \zeta(2\sigma)/\zeta(\sigma), \qquad \limsup_{|t|\to\infty} |\zeta(\sigma+it)| = \zeta(\sigma).$$

What can you say about the behavior of $\log \zeta(\sigma+it)$, or more generally of $\log L(\sigma+it,\chi)$, for fixed $\sigma > 1$ and Dirichlet character χ?

5. (Basic properties of $o(\cdot)$.) If $f = o(g)$ then $f = O(g)$. If $f = o(g)$ and $g = O(h)$, or $f \ll g$ and $g = o(h)$, then $f = o(h)$ (assuming that the same implied limit is taken in both premises). If $f_1 = o(g_1)$ and $f_2 = O(g_2)$ then $f_1 f_2 = o(g_1 g_2)$; if moreover $f_2 = o(g_2)$ then $f_1 + f_2 = o(g_1 + g_2) = o(\max(g_1, g_2))$. Given a positive function g, the functions f such that $f = o(g)$ constitute a vector space.

6. (Effective and ineffective $o(\cdot)$.) An estimate $f = o(g)$ is said to be *effective* if for each $\epsilon > 0$ we can compute a specific point past which $|f| < \epsilon g$ (or $|f| \leq \epsilon g$ if $g = 0$ is allowed); otherwise it is *ineffective*. Show that the transformations in the previous exercise preserve effectivity. Give an example of an ineffective $o(\cdot)$.

References

[Körner 1988] Körner, T.W.: *Fourier Analysis.* Cambridge, England: Cambridge University Press, 1988. [HA 9.88.14 / QA403.5.K67]

[Weyl 1914] Weyl, H.: Über ein Problem aus dem Gebiete der diophantischen Approximationen. *Ges. Abh.* I (Springer: Berlin 1968), 487–497. [O 9.68.1]