Integration Workshop 2003
Project on Primes in an Arithmetic Progression

Douglas Ulmer

It's not hard to show using elementary calculus that there are infinitely many primes and more precisely that the series $\sum_p p^{-1}$ diverges. The aim of this project is to use group theory and complex analysis to show that if m and a are relatively prime integers, then $\sum_{p\equiv a \mod m} p^{-1}$ diverges and so there are infinitely many primes in the arithmetic progression $a, a+m, a+2m, \dots$. Remarkably, the only known proofs of this fact use analytic methods.

1. (Partial summation) If $a_1, a_2, \dots$ and $b_1, b_2, \dots$ are sequences of complex numbers and $A_N = a_1 + \dots + a_N$, then
$$\sum_{n=1}^{N} a_n b_n = A_N b_N + \sum_{n=1}^{N-1} A_n (b_n - b_{n+1}).$$

2. (Dirichlet series) With notation as above, if there are constants C and σ_1 such that $|A_n| \le C n^{\sigma_1}$ then the series
$$\sum_{n=1}^{\infty} a_n n^{-s}$$
converges for $\Re s > \sigma_1$ and the convergence is uniform on compact subsets. Hint: Apply the Cauchy criterion, using partial summation and the formula $(k^{-s} - (k+1)^{-s})/s = \int_k^{k+1} x^{-s-1}\,dx$.

3. (Riemann ζ) Define $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. By the previous part, this defines an analytic function in the region $\Re s > 1$. For positive integers r, define $\zeta_r(s) = (1 - r^{1-s})\zeta(s)$. Using ζ_2 and ζ_3, prove that there is a meromorphic function defined in the region $\Re s > 0$ which has a simple pole (with residue 1) at $s = 1$, no other singularities, and agrees with $\zeta(s)$ in the region $\Re s > 1$. Hint: Look at the Dirichlet series expansion of ζ_r and use part (2) above. Pay attention to convergence vs. absolute convergence. To see the residue at $s = 1$, compare $\zeta(s)$ with $\int_1^{\infty} x^{-s}\,dx$. We let $\zeta(s)$ denote the extended function.

4. (Euler product) Prove that for $\Re s > 1$,
$$\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1}$$

where the product is over all prime numbers p.

5. ($\sum_p p^{-1}$ diverges) In $\Re s > 1$,

$$\log \zeta(s) = \sum_p \sum_{k \geq 1} \frac{p^{-ks}}{k}.$$

Show that

$$\left| \sum_p \sum_{k \geq 2} \frac{p^{-ks}}{k} \right| \leq 1$$

in $\Re s \geq 1$ and conclude that $\sum_p p^{-1}$ diverges.

6. (Characters) Let G be a finite abelian group and let $\hat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ (complex-valued characters of G). Prove that G and $\hat{G}$ are isomorphic (but not canonically) as groups. We write e for the identity element of G and χ_0 for the identity element of $\hat{G}$. Show that for all $\chi \in \hat{G}$

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases}$$

and for all $g \in G$

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = e \\ 0 & \text{otherwise} \end{cases}.$$

7. (Dirichlet L-functions) Let $G = (\mathbb{Z}/m\mathbb{Z})^\times$ (invertible elements in the ring of integers modulo m). Any $\chi \in \hat{G}$ can naturally be viewed as a function of integers relatively prime to m. We extend χ to a function on $\mathbb{Z}$ by setting $\chi(a) = 0$ if a and m are not relatively prime. Define

$$L(s, \chi) = \sum_{n \geq 1} \chi(n) n^{-s}$$

and show that $L(s, \chi) = \prod_p (1 - \chi(p) p^{-s})^{-1}$ in $\Re s > 1$. Show that $L(s, \chi_0) = \prod_{p|m} (1 - p^{-s}) \zeta(s)$ (and so it extends to a meromorphic function on $\Re s > 0$). Show that if $\chi \neq \chi_0$ then $L(s, \chi)$ is holomorphic in $\Re s > 0$. Hint: The series converges there, although not absolutely.

8. (Strategy) In $\Re s > 1$ we have

$$\frac{1}{\phi(m)} \sum_{\chi \in \hat{G}} \chi^{-1}(a) \log L(s, \chi) = \sum_{\substack{p,k \\ p^k \equiv a \mod m}} \frac{p^{-ks}}{k} \sim \sum_{p \equiv a \mod m} p^{-s}$$

where $\sim$ means the two sides differ by a function which is bounded as s tends to 1 from the right and $\phi(m)$ is the order of $(\mathbb{Z}/m\mathbb{Z})^\times$. Since $\log L(s, \chi_0) \to \infty$ as $s \to 1$, if we can show that $L(1, \chi) \neq 0$ for all $\chi \neq \chi_0$, this would imply that $\sum_{p \equiv a \mod m} p^{-s} \to \infty$ as $s \to 1$ which is our desired result.

9. ($\prod_\chi L(s,\chi)$ non-zero near 1) Show that

$$\frac{1}{\phi(m)} \sum_\chi \log L(s,\chi) \geq 0$$

for $s \in (1,\infty)$ and conclude that $\prod_\chi L(s,\chi) \geq 1$ on the same set.

10. (Non-vanishing for complex χ) Note that $\chi \in \hat{G}$ has order 2 if and only if it has only real values. If not, then $\chi^{-1} \neq \chi$. Show that $L(1,\chi) = 0$ implies $L(1,\chi^{-1}) = 0$. If this were the case, then $\prod_\chi L(s,\chi)$ would have a zero at $s = 1$ contradicting the previous part.

11. (Non-vanishing for real χ) This case is harder and we resort to a trick. Suppose that χ is real-valued and that $L(1,\chi) = 0$. Then $L(s,\chi)L(s,\chi_0)$ is analytic in $\Re s > 0$. Set

$$\psi(s) = \frac{L(s,\chi)L(s,\chi_0)}{L(2s,\chi_0)}$$

and note that ψ is meromorphic in $\Re s > 0$, analytic in a neighborhood of $1/2$, and has a zero at $s = 1/2$. In $\Re s > 1$ we have

$$\psi(s) = \prod_{p \text{ with } \chi(p)=1} \frac{1+p^{-s}}{1-p^{-s}} = \sum_{n\geq 1} a_n n^{-s}$$

where the a_n are non-negative. Form the Taylor expansion around $s = 2$ and show that

$$\psi(s) = \sum b_n (2-s)^n$$

where the b_n are non-negative. Conclude that for $s \in (1/2, 2)$, $\psi(s) \geq \psi(2) \geq 1$, contradicting the fact that $\psi(s) \to 0$ as $s \to 1/2$. Thus $L(1,\chi) \neq 0$.

Amazingly, the actual values $L(1,\chi)$ have great number-theoretic significance. For example, if m is a prime congruent to $3 \mod 4$ and χ is the unique character modulo m of order exactly 2, then $L(1,\chi)$ is $\pi/m^{3/2}$ times an integer and the integer is, on the one hand, the number of (equivalence classes of) binary quadratic forms of discriminant m and on the other, a measure of the failure of unique factorization in the field $\mathbb{Q}(\sqrt{-m})$. The study of the arithmetic meaning of special values of L-functions is one of the major currents in modern number theory.