Math 531, Fall 2005
Analytic Number Theory
Problem Set 7
Solutions

Problem 1

Show that if f is a periodic, completely multiplicative arithmetic function, then f is a Dirichlet character to some modulus q.

Solution

Since, by assumption, f is completely multiplicative and periodic, to show that f is a Dirichlet character, it remains to show that, for some q, we have (i) $f(n) \neq 0$ if $(n, q) = 1$ and (ii) $f(n) = 0$ if $(n, q) > 1$.

We define q to be the minimal positive period of f. Relation (i) follows from the generalized Fermat theorem: If $(n, q) = 1$, then $n^{\phi(q)} \equiv 1 \bmod q$, so $f(n)^{\phi(q)} = f(n^{\phi(q)}) = f(1) = 1$, by the multiplicativity and periodicity of f, and hence $f(n) \neq 0$.

To prove (ii), suppose $(n, q) = d > 1$. Then $n = n'd$ with $d|q$ and a positive integer n'. Hence $f(n) = f(n'd) = f(n')f(d)$, so to show that $f(n) = 0$, it suffices to show that $f(d) = 0$ for any divisor $d|q$ with $d > 1$. Given such a d, let $d' = q/d$, so that $d' < q$, since $d > 1$. Then, for any positive integer m, we have $f(m)f(d) = f(md) = f(md+q) = f((m+d')d) = f(m + d')f(d)$. If $f(d) \neq 0$, this would imply that $f(m) = f(m + d')$ for all m, contradicting our assumption that q is the smallest period of f. This proves the claim.

Problem 2

Show that if every arithmetic progression a mod q with $(a, q) = 1$ contains at least one prime, then every such progression contains *infinitely* many primes.

Solution

For each progression a modulo q, with $(a, q) = 1$, let $p(a, q)$ denote the prime in that progression guaranteed by the assumption. Given a and q with $(a, q) = 1$, choose a sequence of primes $p_1 < p_2 < \cdots$ with $p_i \nmid q$, and consider the simultaneous congruence $n \equiv a \bmod q$, $n \equiv 1 \bmod p_i$. By the Chinese Remainder Theorem, this system of congruences is equivalent to a single congruence $a_i \bmod qp_i$, with $(a_i, qp_i) = 1$. Then the numbers $q_n = p(a_n, qp_n)$ are primes that lie in the progressions a mod q and 1 mod p_n. The latter condition forces q_n to be greater than p_n, so that $q_n \to \infty$ as $n \to \infty$. Hence the q_n form an infinite set of primes, all congruent to a mod q, as desired.

Problem 3

Given a rational number a with $0 < a \le 1$, define $\zeta(s, a) = \sum_{n=0}^{\infty}(n + a)^{-s}$. Show that any Dirichlet L-function can be expressed in terms of the functions $\zeta(s, a)$, and that, conversely, any such function $\zeta(s, a)$ with rational a can be expressed in terms of Dirichlet L-functions.

Solution

To express $L(s, \chi)$ in terms of $\zeta(s, a)$, use the periodicity of χ to get

$$\begin{aligned} L(s,\chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{h=1}^{q} \chi(h) \sum_{n=1, n \equiv h \bmod q}^{\infty} \frac{1}{n^s} \\ &= \sum_{h=1}^{q} \chi(h) \sum_{m=0}^{\infty} \frac{1}{(qm+h)^s} = \frac{1}{q^s} \sum_{h=1}^{q} \chi(h) \zeta(s, h/q). \end{aligned}$$

For the other direction, given $a = h/q$ with $h, q, \in \mathbb{N}$, $(h, q) = 1$, write

$$\begin{aligned}\zeta(s,a) &= \sum_{n=0}^{\infty} \frac{1}{(n+h/q)^s} = q^s \sum_{n=0}^{\infty} \frac{1}{(nq+h)^s} \\ &= q^s \sum_{m=1, m\equiv h \bmod q}^{\infty} \frac{1}{m^s} = q^s \sum_{m=1}^{\infty} \frac{1}{m^s} \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi}(h)\chi(m) \\ &= \frac{q^s}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi}(h) \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} = \frac{q^s}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi}(h) L(s,\chi).\end{aligned}$$

Problem 4*

Define the Dirichlet resp. logarithmic densities of a set $A \subset \mathbb{N}$ by the formulas

$$D(A) = \lim_{\sigma \to 1+} (\sigma - 1) \sum_{n \in A} \frac{1}{n^\sigma}$$

and

$$\delta(A) = \lim_{x \to \infty} \frac{1}{\log x} \sum_{n \le x, n \in A} \frac{1}{n},$$

if the limits exist. Show that if $\delta(A)$ exists then $D(A)$ exists.

Solution

Let

$$L(x) = \sum_{n \le x, n \in A} \frac{1}{n}.$$

Suppose that $\delta(A)$ exists, i.e.,

$$\lim_{x \to \infty} \frac{L(x)}{\log x} = \delta(A). \tag{1}$$

Let $\sigma > 1$ be given. By the summation by parts formula formula (with $a_n = 1/n$ if $n \in A$ and $a_n = 0$ otherwise, and $f(n) = n^{1-\sigma}$, we have for every $N \ge 1$,

$$\sum_{n \le N, n \in A} \frac{1}{n^\sigma} = L(N)N^{1-\sigma} + (\sigma - 1) \int_1^N L(x)x^{-\sigma} dx.$$

Now let $N \to \infty$. Since $L(x) = O(\log x)$ and $\sigma > 1$, the first term on the right tends to 0 and the integral converges absolutely when extended to infinity. We thus get

$$\sum_{n=1, n\in A}^{\infty} \frac{1}{n^\sigma} = (\sigma - 1)\int_1^\infty L(x)x^{-\sigma}dx = (\sigma - 1)I(\sigma),$$

say. To prove the existence of $D(A)$, we need to show that the limit $\lim_{\sigma\to 1+}(\sigma - 1)^2 I(\sigma)$ exists. In fact, we will show that

$$\lim_{\sigma\to 1+}(\sigma - 1)^2 I(\sigma) = \delta(A). \tag{2}$$

To prove (2), let $\epsilon > 0$ be given. By the hypothesis (1) there exists an $x_0 = x_0(\epsilon) \geq 1$ such that

$$|L(x) - \delta(A)\log x| \leq \epsilon \log x \quad (x \geq x_0). \tag{3}$$

Moreover, we have trivially

$$|L(x) - \delta(A)\log x| \leq M(\epsilon) \quad (1 \leq x \leq x_0) \tag{4}$$

with some constant $M(\epsilon)$. (E.g., since $L(x) \leq x$ for all x, we could take $M(\epsilon) = x_0 + \delta(A)\log x_0$.) Thus, if we define

$$I_0(\sigma) = \int_1^\infty (\log x)x^{-\sigma}dx = \int_0^\infty ue^{-(\sigma-1)u}du = \frac{1}{(\sigma - 1)^2},$$

then we have

$$\begin{aligned}
\left| I(\sigma) - \frac{\delta(A)}{(\sigma - 1)^2} \right| &= |I(\sigma) - \delta(A)I_0(\sigma)| \\
&\leq \int_1^\infty |L(x) - \delta(A)\log x|\, x^{-\sigma}dx \\
&\leq \int_1^{x_0} M(\epsilon)x^{-\sigma}dx + \int_{x_0}^\infty \epsilon(\log x)x^{-\sigma}dx \\
&\leq M(\epsilon)x_0 + \epsilon I_0(\sigma) = M(\epsilon)x_0 + \frac{\epsilon}{(\sigma - 1)^2}.
\end{aligned}$$

It follows that

$$\limsup_{\sigma\to 1+} \left|(\sigma - 1)^2 I(\sigma) - \delta(A)\right| \leq \epsilon.$$

Since ϵ was arbitrary, this proves (2).

Remark: The converse is also true, i.e., the existence of $D(A)$ implies that of $\delta(A)$, but this implication lies much deeper, and the proof requires the use of so-called Tauberian theorems.

Problem 5

(Bonus problem) Last, but not least, here is one that seems hopelessly difficult at first sight (and which won't on the final and is quite unlikely to show up on comp exams), but ...

One of the most famous unsolved problems in number theory is Goldbach's conjecture according to which every even integer greater than 2 can be expressed as the sum of two primes. The conjecture has been numerically verified for all even numbers up to about 10^{14}, but a proof that the conjecture holds for all even numbers remains as elusive as ever. Prove that there exists a bound C, such that if the conjecture holds for even numbers up to C, then it holds for all even numbers.

Solution

The solution is so simple that it seems like cheating. Let E denote the set of exceptions to Goldbach's conjecture, i.e., the set of even integers ≥ 4 that are not representable as a sum of two primes, and define

$$C = \begin{cases} 1 & \text{if } E \text{ is empty,} \\ \min\{n : n \in E\} & \text{otherwise.} \end{cases}$$

Then C has the desired property. (Check it!)