189-346/377B: Number Theory

Assignment 5

Solutions

1. An integer n is said to be *square-free* if its prime factorisation is of the form

$$n = p_1 p_2 \cdots p_r,$$

where $p_1, \ldots, p_r$ are *distinct* primes. Show that for all real $s > 1$,

$$\frac{\zeta(s)}{\zeta(2s)} = \sum_{n \in S} \frac{1}{n^s},$$

where

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

is the Riemann zeta function, and S is the set of positive square free integers.

Solution: By the Euler product factorisation for the Riemann zeta-function,

$$\frac{\zeta(s)}{\zeta(2s)} = \prod_p (1 - p^{-s})^{-1}(1 - p^{-2s}) = \prod_p (1 + p^{-s}),$$

the products being taken as usual over all the primes. Expanding the last product as an infinite sum, one observes that one obtains a term of $1/n^s$ exactly once for each n which admits a factorisation as a product of distinct primes with multiplicity one:

$$\prod_p (1 + p^{-s}) = \sum_{n \in S} \frac{1}{n^s}.$$

2. Using a Sieve argument (or otherwise), show that the number of square-free integers that are less than or equal to x is equal to

$$\zeta(2)^{-1} x + o(x).$$

Solution: For any integer r, let $p_1, \ldots, p_r$ denote the first r primes, and let $s_r(x)$ denote the number of integers $\leq x$ that are not divisible by any of p_1^2, p_2^2, up to p_r^2. Then by the same sieve argument as was used in class to show that $\pi(x)$ grows at most like $x/\log\log x$, we can see that

$$s_r(x) = x\prod_{j=1}^{r}(1-p_j^{-2}) + e(r,x),$$

where $e(r,x) \leq 2^r$. Now, letting $r = [\log(x)]$, we have $2^r = o(x)$ as was seen in class, and $\prod_{j=1}^{r}(1-p_j^{-2}) = 1/\zeta(s) + o(1)$. The result follows. (Note that this proof is less delicate than the argument we carried out in class, essentially because the infinite sum defining $\zeta(s)$ converges at $s=2$ while it diverges at $s=1$.

3. Show that any integer of the form $4n+3$ always has a prime divisor of the form $4k+3$. Use this to give a proof that there are infinitely many primes of the form $4k+3$, analogous to Euclid's proof of the infinitude of primes that was recalled in class. Show by a similar argument that there are infinitely many primes of the form $3k+2$.

Solution: If all the prime divisors of an integer are of the form $4k+1$, then the same is true of the integer itself. Hence any integer of the form $4n+3$ must have a prime divisor of the form $4k+3$. To see that there are infinitely many primes of the form $4k+3$, let $q_1, \ldots, q_n$ be any finite set of such primes and observe that the integer $4q_1\cdots q_n - 1$ is necessarily divisible by a prime q of the form $4k+3$ which is not already in that set. The argument for primes of the form $3k+2$ is identical (and was also seen again in class.)

4. Let d be a prime. Show that any prime p which does not divide d but divides the integer

$$n^{d-1} + n^{d-2} + \cdots + 1$$

($n \in \mathbf{Z}$) is necessarily of the form $kd+1$. Use this to show that there are infinitely many primes of the form $kd+1$. (Hint: assume otherwise, and study the asymptotics of $\#\{n^{d-1}+\cdots+n+1, \quad n \leq x^{1/d}\}$ as $x \longrightarrow \infty$ in two different ways to derive a contradiction.)

Solution. If p divides $n^{d-1}+\cdots+1$, then it also divides $(n-1)(n^{d-1}+\cdots+1) =$

$n^d - 1$. Hence the residue class of n modulo p is an element of order dividing d, hence either $n = 1$ or n is of order (exactly) d. If $n \equiv 1 \pmod{p}$, then p would have to divide $n^{d-1} + \cdots + 1 \equiv 1 + \cdots + 1 = d \pmod{p}$, which we have assumed is not the case. Hence the class of n is of order d in $(\mathbf{Z}/p\mathbf{Z})^\times$. In particular, the group $(\mathbf{Z}/p\mathbf{Z})^\times$ has cardinality divisible by d, and therefore $p \equiv 1 \pmod{d}$.

To show that there are infinitely many primes of the form $kd+1$, suppose on the contrary that there are only finitely many such primes, $p_1, \ldots, p_r$, and consider the set $S(X,d)$ of integers $\leq X$ of the form $n^{d-1}+\cdots+1$. On the one hand, the cardinality of $S(X,d)$ grows asymptotically like $cX^{1/(d-1)}$ for some constant c as X gets large (as is true for the set of values of any polynomial of degree $d-1$). On the other hand, every integer in $S(X,d)$ is of the form $p_1^{e_1} \cdots p_r^{e_r}$ where the exponents e_j are bounded by $\log_{p_j}(X) = c_j \log(X)$. Hence there are at most $c' \log(X)^r$ such integers for some other constant c'. This is a contradiction since, for all $\alpha > 0$ (however small) and for all $M > 0$ (however large), we always have

$$\lim_{X \longrightarrow \infty} (X^\alpha - (\log(X))^M) = \infty.$$

Note that a similar idea was already used in a previous assignment...

The following exercises are taken from the textbook by Levesque.

5. (Section 6.2, exercise 7 from Levesque.)
Show that, for all $s > 1$,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1,$$

where $\mu(n)$ is the Möbius function defined by $\mu(n) = (-1)^t$ if n is a product of t distinct primes, and $\mu(n) = 0$ if t is divisible by the square of some prime.

Solution. This follows from the factorisation formula for $\zeta(s)$ after noting that

$$\zeta(s)^{-1} = \prod_p (1 - p^{-s}) = \sum_n \mu(n) n^{-s}.$$

6. Show that if $f(x)$ is a continuous, monotonically decreasing function which

tends to 0 as $x \longrightarrow \infty$, and if the series $\sum_{n=1}^{\infty} f(n)$ diverges, then the function

$$F(n) := \sum_{j=1}^{n} f(j)$$

satisfies

$$F(n) \sim \int_1^n f(x) dx.$$

Proof. This follows from the trick we have already used a number of times in class, in which we approximate $\int_1^n f(x)dx$ both from above and below by a Riemann sum:

$$F(n) - f(1) = \sum_{j=2}^{n} f(j) \le \int_1^n f(x)dx \le \sum_{j=1}^{n-1} f(j) \le F(n).$$

It follows from this that

$$|F(n) - \int_1^n f(x)dx| \le f(1),$$

and therefore the ratio $\int_1^n f(x)dx/F(n)$ tends to 1 as $n \longrightarrow \infty$.

7. (Section 6.4, exercise 9 from Levesque.)
Let $\log_k x$ be the k-th iterate of the logarithm function, defined recursively by

$$\log_1 x = \log x, \qquad \log_k x = \log \log_{k-1} x.$$

Is there a continuous increasing function $f(x)$ such that $\lim_{x \to \infty} f(x) = \infty$, yet $f(x) = o(\log_k x)$ for all $k \ge 1$? If so, exhibit such a function.

Solution: Let

$$h(m) = e^{e^{e^{\cdots}}} \quad (m \text{ times}),$$

and let

$$f(x) = \text{ least } m \text{ such that } h(m) > x.$$

To see that $f(x)$ grows more slowly than $\log_k(x)$, write

$$x = e^{e^{e^{\cdots y}}} \quad (k \text{ times}),$$

which is always possible once x is sufficiently large. Then it is not hard to see that

$$\log_k(x) = y, \qquad f(x) = f(y) + k,$$

and hence the result follows since clearly $f(y)/y$ tends to 0.

Math 377 only:
8. Section 6.8., exercise 4 in Levesque.

Solution: The method of proof is very similar to what was worked out in class for the case $q = 5$. (The fact that all Dirichlet characters *mod* 8 have values in $\mathbf{Z}$ makes it easier to work with products throughout rather than taking the logarithm of the Dirichlet L-series as we did in class, but otherwise the ideas are the same.)