

# Analytic Number Theory

## Problem Set 1

### Solutions

#### Problem 1

Evaluate the function  $f(n) = \sum_{d^2|n} \mu(d)$  (where the summation runs over all positive integers  $d$  such that  $d^2|n$ ), in the sense of expressing it in terms of familiar arithmetic functions. Be sure to give a complete proof.

#### Solution

The given identity for  $f$  may be written as  $f = g * 1$ , where  $g(n) = s(n)\mu(\sqrt{n})$  and  $s(n)$  is the characteristic function of the squares. We first show that  $g$  is multiplicative. Since  $g(1) = s(1)\mu(1) = 1$ , it suffices to show that if  $n_1$  and  $n_2$  are coprime positive integers, then  $g(n_1n_2) = g(n_1)g(n_2)$ , i.e.,

$$(1) \quad s(n_1n_2)\mu(\sqrt{n_1n_2}) = s(n_1)\mu(\sqrt{n_1})s(n_2)\mu(\sqrt{n_2}).$$

If at least one of  $n_1$  and  $n_2$  is *not* a square, then, by the coprimality of  $n_1$  and  $n_2$ ,  $n_1n_2$  is not a square either; in this case therefore both sides of (1) are equal to 0. On the other hand, if both  $n_1$  and  $n_2$  are squares, say  $n_i = m_i^2$  with  $m_i \in \mathbb{N}$  ( $i = 1, 2$ ), then all  $s$ -functions in (1) are equal to 1, and (1) is equivalent to

$$(2) \quad \mu(m_1m_2) = \mu(m_1)\mu(m_2).$$

Now note that the coprimality of  $n_1 = m_1^2$  and  $n_2 = m_2^2$  implies that of  $m_1$  and  $m_2$ . Thus, since  $\mu$  is multiplicative, (2) holds and the function  $g$  is indeed multiplicative.

Since  $g$  is multiplicative, so is  $f = g * 1$ , and it therefore suffices to evaluate  $f(p^m)$ . The definition of  $g$  implies that  $g(p^k) = -1$  if  $k = 2$  and  $g(p^k) = 0$  if  $k \in \mathbb{N}$  and  $k \neq 2$ , and, of course,  $g(p^0) = g(1) = 1$ . Thus,

$$f(p^m) = \sum_{k=0}^m g(p^k) = \begin{cases} g(1) = 1 & \text{if } m = 1, \\ g(1) + g(p^2) = 1 - 1 = 0 & \text{if } m \geq 2, \end{cases}$$

and we see that  $f$  agrees with  $\mu^2$  on prime powers. Since both  $f$  and  $\mu^2$  are multiplicative, it follows that  $f(n) = \mu^2(n)$  for every  $n \in \mathbb{N}$ .

## Problem 2

Determine an arithmetic function  $f$  such that

$$\frac{1}{\phi(n)} = \sum_{d|n} \frac{1}{d} f\left(\frac{n}{d}\right) \quad (n \in \mathbb{N}).$$

## Solution

The equation determining  $f$  can be written as  $(1/\phi) = (1/\text{id}) * f$ . Since  $1/\phi$  and  $1/\text{id}$  are multiplicative functions (as reciprocals of known multiplicative functions), the function  $f$  must be multiplicative, and it suffices to determine its values at prime powers. Setting  $n = p^m$ , the above equation becomes

$$\frac{1}{p^m(1 - 1/p)} = \sum_{k=0}^m \frac{1}{p^k} f(p^{m-k}),$$

which implies

$$\begin{aligned} f(p^m) &= \frac{1}{p^m(1 - 1/p)} - \sum_{k=1}^m f(p^{m-k})p^{-k} \\ &= \frac{1}{p^m(1 - 1/p)} - \frac{1}{p^m} - \sum_{k=1}^{m-1} f(p^{m-k})p^{-k} \\ &= \frac{1}{p^m(p - 1)} - \sum_{k=1}^{m-1} f(p^{m-k})p^{-k}, \end{aligned}$$

since  $f(p^0) = f(1) = 1$  by the multiplicativity of  $f$ . This is an infinite system of linear equations for  $f(p^m)$ , which can be solved iteratively. Setting  $m = 1$  gives  $f(p) = 1/(p(p-1))$ . Next, taking  $m = 2$  we get  $f(p^2) = 1/(p^2(p-1)) - f(p)p^{-1} = 0$ , and in the same way it follows that  $f(p^m) = 0$  for all  $m \geq 2$ . Thus,  $f(p^m) = \mu^2(p^m)/(p^m\phi(p^m))$  for all  $m \geq 1$ . Therefore we have  $f = \mu^2/(\text{id} \cdot \phi)$ .

**Remark.** An alternative way to do this problem is to multiply the original identity by  $n$  and write the resulting relation as  $(\text{id}/\phi) = 1 * (\text{id} \cdot f)$ , then apply the Moebius inversion formula to conclude  $\text{id} \cdot f = (\text{id}/\phi) * \mu$  and show, by evaluating at prime powers, that the right hand side is equal to  $\mu^2/\phi$ .

### Problem 3

Let  $f(n) = \#\{(n_1, n_2) \in \mathbb{N}^2 : [n_1, n_2] = n\}$ , where  $[n_1, n_2]$  is the least common multiple of  $n_1$  and  $n_2$ . Show that  $f$  is multiplicative and evaluate  $f$  at prime powers.

### Solution

**Proof of the multiplicativity of  $f$ .** Clearly,  $f(1) = 1$ , so it remains to show that  $f(n_1n_2) = f(n_1)f(n_2)$  for coprime  $n_1, n_2 \in \mathbb{N}$ . To this end, we show that, given  $n_1, n_2 \in \mathbb{N}$  with  $(n_1, n_2) = 1$ , there is a bijection between pairs of the form

$$(1) \quad (h, k) \in \mathbb{N}^2 : [h, k] = n_1n_2$$

and quadruples

$$(2) \quad (h_1, k_1, h_2, k_2) \in \mathbb{N}^4 : [h_i, k_i] = n_i \quad (i = 1, 2).$$

We first note that, since  $n_1$  and  $n_2$  are coprime, any divisor  $d$  of  $n_1n_2$  can be factored uniquely as  $d = d_1d_2$  with  $d_i|n_i$  for  $i = 1, 2$ . Applying this with  $d = h$  and  $d = k$ , we see that any pair  $(h, k)$  with  $[h, k] = n_1n_2$  can be written uniquely in the form  $(h, k) = (h_1h_2, k_1k_2)$  with  $h_i, k_i|n_i$  for  $i = 1, 2$ . Thus, we have a well-defined map  $(h, k) \rightarrow (h_1, k_1, h_2, k_2)$  for each tuple  $(h, k)$  of the form (1). We will show that this map gives a bijection between the set of tuples of the form (1) and the set of quadruples of the form (2).

First note that, since  $n_1$  and  $n_2$  are coprime, each of  $h_1, k_1$  is coprime with each of  $h_2, k_2$ . Hence  $[h, k] = [h_1 h_2, k_1 k_2] = [h_1, k_1][h_2, k_2]$ . But since  $[h, k] = n_1 n_2$  and  $[h_i, k_i] | n_i$  for each  $i$ , this forces  $[h_i, k_i] = n_i$  for each  $i$ , i.e.,  $(h_1, k_1, h_2, k_2)$  is a quadruple counted in (2). Conversely, a quadruple  $(h_1, k_1, h_2, k_2)$  counted in (2) is the image of the tuple  $(h, k) = (h_1 h_2, k_1 k_2)$  under this map, and since  $[h, k] = [h_1, k_1][h_2, k_2] = n_1 n_2$ , the tuple  $(h, k)$  is counted in (1).

This completes the proof of the multiplicativity of  $f$ .

**Evaluation at prime powers.** When  $n = p^m$ , then the pairs  $(n_1, n_2)$  in the definition of  $f(p^m)$  are  $(p^k, p^m)$ ,  $0 \leq k \leq m-1$ ,  $(p^m, p^k)$ ,  $0 \leq k \leq m-1$ , and  $(p^m, p^m)$ . There are a total of  $2m+1$  of these, so  $f(p^m) = 2m+1$ .

**Remark.** In fact, we have  $f(n) = d(n^2)$  for all  $n$ , as can be seen by noting that both sides of this identity are multiplicative functions of  $n$  and that they have the same value (namely  $2m+1$ ) at a prime power  $p^m$ .

#### Problem 4

Let  $f(n) = \phi(n)/n$ , and let  $\{n_k\}_{k=1}^{\infty}$  be the sequence of values  $n$  at which  $f$  attains a “record low”; i.e.,  $n_1 = 1$  and, for  $k \geq 2$ ,  $n_k$  is defined as the smallest integer  $> n_{k-1}$  with  $f(n_k) < f(n)$  for all  $n < n_k$ . (For example, since the first few values of the sequence  $f(n)$  are  $1, 1/2, 2/3, 1/2, 4/5, 1/3, \dots$ , we have  $n_1 = 1$ ,  $n_2 = 2$ , and  $n_3 = 6$ , and the corresponding values of  $f$  at these arguments are  $1, 1/2$  and  $1/3$ .) Find (with proof) a general formula for  $n_k$  and  $f(n_k)$ .

#### Solution

Note first that  $f$ , as the quotient of two multiplicative functions, is multiplicative, and  $f(p^m) = (p^m - p^{m-1})/p^m = (1 - 1/p)$  for every prime power  $p$ . Hence, for  $n = \prod_{p^m | n} p^m$  we have  $f(n) = \prod_{p|n} (1 - 1/p)$ . In particular, the value of  $f(n)$  depends only on the set of prime factors of  $n$ , and not on the exponents of these prime factors. Hence, among all integers  $n$  having a given set of prime factors, only the smallest, namely the product of these primes, can yield a record value for  $f(n)$ .

Next, we claim that among all integers with a given number  $k (\geq 1)$  of distinct prime factors, only the smallest, namely the product of the *first*  $k$

primes, can yield a record value for  $f(n)$ . Indeed, if  $p_i$  denotes the  $i$ -th prime and  $n = \prod_{j=1}^k p_{i_j}$  with  $1 \leq i_1 < \dots < i_k$ , then  $p_{i_j} \geq p_j$  for all  $j$  and

$$f(n) = \prod_{j=1}^k \left(1 - \frac{1}{p_{i_j}}\right) \geq \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) = f(p_1 \dots p_k),$$

with equality if and only if  $n = p_1 \dots p_k$ .

Hence a record value can only occur at  $n = 1$  (which is a record by definition) or at integers  $n \geq 2$  of that are of the form  $P_k = \prod_{j=1}^k p_j$  for some  $k$ . Since  $1 = f(1) > f(P_1) > f(P_2) > \dots$ , each of the numbers  $P_k$  yields indeed a record value of  $f$ . Thus, if we set  $P_0 = 1$ , then the sequence  $\{n_k\}_{k=1}^{\infty}$  of record values sought in the problem is exactly the sequence  $\{P_k\}_{k=0}^{\infty}$ .

### Problem 5

A positive integer  $n$  is called squarefull if it satisfies  $(*) p|n \Rightarrow p^2|n$ . (Note that  $n = 1$  is squarefull according to this definition, since 1 has no prime divisors and the above implication is therefore trivially true.) Show that  $n$  is squarefull if and only if  $n$  can be written in the form  $n = a^2b^3$  with  $a, b \in \mathbb{N}$ . **Bonus question:** Find a similar characterization of “ $k$ -full” integers, i.e., integers  $n \in \mathbb{N}$  that satisfy  $(*)$  with 2 replaced by  $k$  (where  $k \geq 3$ ).

### Solution

Writing the prime factorizations of  $a$ ,  $b$ , and  $n$  as  $a = \prod_p p^{\alpha(p)}$ ,  $b = \prod_p p^{\beta(p)}$ , and  $n = \prod_p p^{\gamma(p)}$  with  $\alpha(p), \beta(p), \gamma(p) \in \mathbb{N} \cup \{0\}$ , we see that  $n = a^2b^3$  holds if and only if, for every prime  $p$ ,

$$(2) \quad \gamma(p) = 2\alpha(p) + 3\beta(p).$$

Thus, given  $n \in \mathbb{N}$ , there exists a representation of the form  $n = a^2b^3$  with  $a, b \in \mathbb{N}$ , if and only if, for every  $p$ , (2) has a solution in nonnegative integers  $\alpha(p)$  and  $\beta(p)$ . On the other hand, by definition  $n$  is squarefull if and only if, for each prime  $p$ ,  $\gamma(p) \geq 2$  or  $\gamma(p) = 0$ . Thus, the first problem amounts to showing that the integers of the form  $2\alpha + 3\beta$  with nonnegative integers  $\alpha$  and  $\beta$  are precisely 0 and all integers  $\gamma \geq 2$ . This is seen as follows: If  $(\alpha, \beta) = (0, 0)$  then  $2\alpha + 3\beta = 0$ . If  $(\alpha, \beta) \neq (0, 0)$  then  $2\alpha + 3\beta \geq 2$ ; moreover, every integer  $\gamma \geq 2$  can be represented in this form, for example,

by taking  $(\alpha, \beta) = (\gamma/2, 0)$  if  $\gamma$  is even, and  $(\alpha, \beta) = ((\gamma - 3)/2, 1)$  if  $\gamma$  is odd (and thus  $\geq 3$ ).

To generalize this result to  $k$ -full integers for  $k \geq 3$ , we will try to find a set of coefficients  $\lambda_i \in \mathbb{N}$  ( $i = 1, \dots, r$ ) such that

$$\{\gamma \in \mathbb{N} : \gamma \geq k\} \cup \{0\} = \left\{ \sum_{i=1}^r \lambda_i \alpha_i : \alpha_i \in \mathbb{N} \cup \{0\} \right\};$$

then, by the same argument as above, an integer  $n$  is  $k$ -full if and only if it has a representation  $n = \prod_{i=1}^r a_i^{\lambda_i}$  with  $a_i \in \mathbb{N}$ .

The construction of suitable  $\lambda_i$  can be done in a variety of ways; one possibility is to take

$$\lambda_i = k + i - 1 \quad (i = 1, 2, \dots, k).$$

Since each  $\lambda_i$  is  $\geq k$ , any linear combination of  $\lambda_i$  with nonnegative integer coefficients is either 0 or  $\geq k$ . Conversely, any  $\gamma \geq k$  can be written as

$$\gamma = xk + y = (x - 1)k + (y + k)$$

with integers  $x \geq 1$  and  $0 \leq y \leq k - 1$ ; this representation is of the form  $\sum_{i=1}^k \alpha_i \lambda_i$  with the above choice of  $\lambda_i$ , and coefficients  $\alpha_i$  defined by  $\alpha_1 = (x - 1) \geq 0$ ,  $\alpha_{y+1} = 1$ , and  $\alpha_i = 0$  for  $i \neq 1, y + 1$ . (In the case  $y = 0$  this has to be modified to  $\alpha_1 = x$ ,  $\alpha_i = 0$  for  $2 \leq i \leq k$ .)

### Problem 6

Given an arithmetic function  $f$  such that  $\sum_{n=1}^{\infty} |f(n)|d(n) < \infty$ , define its “transform”  $\hat{f}$  by

$$\hat{f}(d) = \sum_{n=1}^{\infty} f(nd) \quad (d \in \mathbb{N}).$$

Find (with proof) the corresponding “inverse transform”, i.e., a formula expressing  $f(d)$  in terms of the values  $\hat{f}(n)$ .

## Solution

Ignoring questions of convergence for the moment, we have, using the identity  $\sum_{m|n} \mu(m) = e(n)$ ,

$$\begin{aligned} f(k) &= \sum_{n \geq 1} f(kn) e(n) = \sum_{n \geq 1} f(kn) \sum_{m|n} \mu(m) \\ &= \sum_{m \geq 1} \mu(m) \sum_{\substack{n \geq 1 \\ m|n}} f(kn) = \sum_{m \geq 1} \mu(m) \sum_{n' \geq 1} f(kmn') = \sum_{m \geq 1} \mu(m) \hat{f}(km). \end{aligned}$$

This is the desired formula for  $f(k)$  in terms of the values of  $\hat{f}$ . To justify the interchanging of the order of summations in this argument, it is sufficient that the double sum over  $m$  and  $n$  in the second line converges absolutely, i.e., that  $\sum_{m \geq 1} \sum_{n \geq 1, m|n} |f(kn)\mu(m)|$  converges. But the latter sum is bounded by

$$\leq \sum_{n \geq 1} |f(kn)| \sum_{m|n} 1 = \sum_{n \geq 1} |f(kn)| d(n) \leq \sum_{n \geq 1} |f(kn)| d(kn) \leq \sum_{n \geq 1} |f(n)| d(n),$$

which, by hypothesis, converges.

**Remark.** The given transformation can be written as  $\hat{f} = Af$ , where  $A$  is the infinite matrix, with columns and rows both indexed by the positive integers, whose  $(m, n)$ -th entry is 1 if  $m|n$  and 0 else. The problem therefore amounts to finding the inverse of this matrix. The above solution shows that this inverse is the matrix whose  $(m, n)$ -th entry is  $\mu(m)$  if  $m|n$ , and 0 else.

An alternative, and more systematic, approach consists of seeking coefficients  $c_{k,n}$  such that  $(*) f(k) = \sum_{n \in \mathbb{N}} \hat{f}(n) c_{n,k}$ . Taking  $k = 1$  and writing out the definition of  $\hat{f}(n)$ ,  $(*)$  becomes (ignoring questions of convergence)

$$\begin{aligned} f(1) &= \sum_{n \in \mathbb{N}} \sum_{n \in \mathbb{N}} \sum_{\substack{m \in \mathbb{N} \\ n|m}} f(m) c_{n,1} \\ &= \sum_{m \in \mathbb{N}} f(m) \sum_{n|m} c_{n,1}. \end{aligned}$$

Comparing coefficients of  $f(m)$  on each side, we see that we must have  $\sum_{n|m} c_{n,1} = 1$  if  $m = 1$  and 0 else. But this means that the function  $n \mapsto c_{n,1}$  is the convolution inverse of the function 1, and thus must be equal to the Moebius function. Thus, we have  $c_{n,1} = \mu(n)$  for all  $n$ . Similarly, applying  $(*)$  with a general  $k \geq 2$ , shows that  $c_{n,k}$  must be equal to  $\mu(n)$  if  $k|n$ , and 0 else.

**Problem 7\***

Let  $f$  be a multiplicative function satisfying  $\lim_{p^m \rightarrow \infty} f(p^m) = 0$ . Show that  $\lim_{n \rightarrow \infty} f(n) = 0$ .

**Solution**

Let  $q_1 < q_2 < \dots$  denote the sequence of prime powers. By hypothesis,  $f(q_i) \rightarrow 0$  as  $i \rightarrow \infty$ , so there exists  $k$  such that  $|f(q_i)| \leq 1$  for  $i > k$ .

By the multiplicativity of  $f$ , we have, for any  $n$ ,

$$|f(n)| = \prod_{q_i | n} |f(q_i)| = \prod_{q_i | n, i \leq k} |f(q_i)| \cdot \prod_{q_i | n, i > k} |f(q_i)|$$

Hence, if we set

$$K = \max_{I \subset \{1, \dots, k\}} \prod_{i \in I} |f(q_i)|,$$

and

$$i(n) = \max\{i : q_i | n\},$$

then

$$|f(n)| \leq K \prod_{q_i | n, i > k} |f(q_i)| \leq K |f(q_{i(n)})|,$$

provided  $i(n) > k$ . Now, the (obvious) inequality  $n \leq \prod_{i=1}^{i(n)} q_i$  implies that  $i(n) \rightarrow \infty$  and therefore also  $f(q_{i(n)}) \rightarrow 0$  as  $n \rightarrow \infty$ . Hence we obtain  $f(n) \rightarrow 0$  as claimed.

**Problem 8\***

Let  $\mathcal{P} = \{p_1, \dots, p_k\}$  be a finite set of primes, let

$$\mathbb{N}_{\mathcal{P}} = \{n \in \mathbb{N} : p | n \Rightarrow p \in \mathcal{P}\}$$

i.e.,  $\mathbb{N}_{\mathcal{P}}$  is the set of positive integers all of whose prime factors belong to the set  $\mathcal{P}$  (note that  $1 \in \mathbb{N}_{\mathcal{P}}$ ), and let

$$N_{\mathcal{P}}(x) = \#\{n \in \mathbb{N}_{\mathcal{P}} : n \leq x\} \quad (x \geq 1).$$

In class it was shown that one has  $N_{\mathcal{P}}(x) \leq c_1 (\log x)^k$  for a suitable constant  $c_1$  (depending on the set  $\mathcal{P}$ , but not on  $x$ ) and for all sufficiently large  $x$ ,

say  $x \geq x_1$ . This immediately implies that there must be infinitely many primes, since otherwise one could apply this result with  $\mathcal{P}$  the set of **all** primes, and consequently  $\mathbb{N}_{\mathcal{P}}$  the set of all positive integers, and would get a contradiction to the obvious fact that  $\mathbb{N}_{\mathcal{P}}(x) = [x]$  when  $\mathcal{P}$  consists of all primes. Show that a bound of the same type holds in the other direction, i.e., there exist constants  $c_2 > 0$  and  $x_2$ , depending on  $\mathcal{P}$ , such that  $N_{\mathcal{P}}(x) \geq c_2(\log x)^k$  holds for all  $x \geq x_2$ .

### Solution

We start out as in the proof of the upper bound by noting that

$$\mathbb{N}_{\mathcal{P}} = \{p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} : a_i \in \mathbb{N} \cup \{0\}\},$$

and that by the Fundamental Theorem of Arithmetic each element in  $\mathbb{N}_{\mathcal{P}}$  corresponds to a *unique*  $k$ -tuple  $(a_1, \dots, a_k)$  of nonnegative integers. Thus,

$$\begin{aligned} \mathbb{N}_{\mathcal{P}}(x) &= \#\{(a_1, \dots, a_k) : a_i \in \mathbb{N} \cup \{0\}, p_1^{a_1} \dots p_k^{a_k} \leq x\} \\ (1) \quad &= \#\{(a_1, \dots, a_k) : a_i \in \mathbb{N} \cup \{0\}, a_1 \log p_1 + \dots + a_k \log p_k \leq \log x\}. \end{aligned}$$

To get a lower bound for this quantity, let  $p$  denote the largest among the  $k$  primes. Then, by (1),

$$\begin{aligned} \mathbb{N}_{\mathcal{P}}(x) &\geq \#\{(a_1, \dots, a_k) : a_i \in \mathbb{N} \cup \{0\}, a_1 \log p + \dots + a_k \log p \leq \log x\} \\ &\geq \#\left\{(a_1, \dots, a_k) : 0 \leq a_i \leq \frac{\log x}{k \log p}\right\} \\ &= \left(\left[\frac{\log x}{k \log p}\right] + 1\right)^k \geq \left(\frac{1}{k \log p}\right)^k (\log x)^k \quad (x \geq 1), \end{aligned}$$

which is the desired lower bound with  $c_2 = (k \log p)^{-k}$  and  $x_2 = 1$ .

### Additional problems

One of the chief merits of Apostol's text (available on reserve in the library) is the large number of exercises that it contains. Below is a set of the problems from Chapter 2 of Apostol's text that I would recommend for additional practice. These problems are mostly routine drills, at an easy to medium level of difficulty (comparable to an exam problem), and they can all be done using only material we covered in class.

**Apostol, Chapter 2 (p. 46–51):** 1, 2, 3, 4, 5, 6, 8\*, 10, 11, 18, 19, 25, 27, 33.