Math 255 - Spring 2022
Möbius inversion
20 points

Please read Section 6.2 of *Elementary Number Theory*, seventh edition, by David M. Burton, which I have scanned and attached below.

Then answer this question:

1. The *Mangoldt function* Λ is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \text{ where } p \text{ is a prime and } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

   (a) Prove that

$$\log(n) = \sum_{d|n} \Lambda(d).$$

   (b) Use part (a) to prove that

$$\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d = -\sum_{d|n} \mu(d) \log d.$$

   (You must prove both equalities in this statement.)

23. For any positive integer n, show the following:
(a) $\sum_{d \mid n} \sigma(d) = \sum_{d \mid n} (n/d)\tau(d)$.
(b) $\sum_{d \mid n} (n/d)\sigma(d) = \sum_{d \mid n} d\tau(d)$.
[*Hint:* Because the functions

$$F(n) = \sum_{d \mid n} \sigma(d) \qquad \text{and} \qquad G(n) = \sum_{d \mid n} \frac{n}{d}\tau(d)$$

are both multiplicative, it suffices to prove that $F(p^k) = G(p^k)$ for any prime p.]

6.2 THE MÖBIUS INVERSION FORMULA

We introduce another naturally defined function on the positive integers, the Möbius μ-function.

Definition 6.3. For a positive integer n, define μ by the rules

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where } p_i \text{ are distinct primes} \end{cases}$$

Put somewhat differently, Definition 6.3 states that $\mu(n) = 0$ if n is not a square-free integer, whereas $\mu(n) = (-1)^r$ if n is square-free with r prime factors. For example: $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$. The first few values of μ are

$$\mu(1) = 1 \quad \mu(2) = -1 \quad \mu(3) = -1 \quad \mu(4) = 0 \quad \mu(5) = -1 \quad \mu(6) = 1, \ldots$$

If p is a prime number, it is clear that $\mu(p) = -1$; in addition, $\mu(p^k) = 0$ for $k \geq 2$.

As the reader may have guessed already, the Möbius μ-function is multiplicative. This is the content of Theorem 6.5.

Theorem 6.5. The function μ is a multiplicative function.

Proof. We want to show that $\mu(mn) = \mu(m)\mu(n)$, whenever m and n are relatively prime. If either $p^2 \mid m$ or $p^2 \mid n$, p a prime, then $p^2 \mid mn$; hence, $\mu(mn) = 0 = \mu(m)\mu(n)$, and the formula holds trivially. We therefore may assume that both m and n are square-free integers. Say, $m = p_1 p_2 \cdots p_r$, $n = q_1 q_2 \cdots q_s$, with all the primes p_i and q_j being distinct. Then

$$\begin{aligned} \mu(mn) &= \mu(p_1 \cdots p_r q_1 \cdots q_s) = (-1)^{r+s} \\ &= (-1)^r(-1)^s = \mu(m)\mu(n) \end{aligned}$$

which completes the proof.

Let us see what happens if $\mu(d)$ is evaluated for all the positive divisors d of an integer n and the results are added. In the case where $n = 1$, the answer is easy; here,

$$\sum_{d \mid 1} \mu(d) = \mu(1) = 1$$

Suppose that $n > 1$ and put

$$F(n) = \sum_{d \mid n} \mu(d)$$

To prepare the ground, we first calculate $F(n)$ for the power of a prime, say, $n = p^k$. The positive divisors of p^k are just the $k + 1$ integers $1, p, p^2, \ldots, p^k$, so that

$$\begin{aligned} F(p^k) = \sum_{d \mid p^k} \mu(d) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ &= \mu(1) + \mu(p) = 1 + (-1) = 0 \end{aligned}$$

Because μ is known to be a multiplicative function, an appeal to Theorem 6.4 is legitimate; this result guarantees that F also is multiplicative. Thus, if the canonical factorization of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then $F(n)$ is the product of the values assigned to F for the prime powers in this representation:

$$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r}) = 0$$

We record this result as Theorem 6.6.

Theorem 6.6. For each positive integer $n \geq 1$,

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

where d runs through the positive divisors of n.

For an illustration of this last theorem, consider $n = 10$. The positive divisors of 10 are 1, 2, 5, 10 and the desired sum is

$$\begin{aligned} \sum_{d \mid 10} \mu(d) &= \mu(1) + \mu(2) + \mu(5) + \mu(10) \\ &= 1 + (-1) + (-1) + 1 = 0 \end{aligned}$$

The full significance of the Möbius μ-function should become apparent with the next theorem.

Theorem 6.7 Möbius inversion formula. Let F and f be two number-theoretic functions related by the formula

$$F(n) = \sum_{d \mid n} f(d)$$

Then

$$f(n) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d)$$

Proof. The two sums mentioned in the conclusion of the theorem are seen to be the same upon replacing the dummy index d by $d' = n/d$; as d ranges over all positive divisors of n, so does d'.

Carrying out the required computation, we get

$$\sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d \mid n}\left(\mu(d) \sum_{c \mid (n/d)} f(c)\right) = \sum_{d \mid n}\left(\sum_{c \mid (n/d)} \mu(d) f(c)\right) \tag{1}$$

It is easily verified that $d \mid n$ and $c \mid (n/d)$ if and only if $c \mid n$ and $d \mid (n/c)$. Because of this, the last expression in Eq. (1) becomes

$$\sum_{d \mid n}\left(\sum_{c \mid (n/d)} \mu(d) f(c)\right) = \sum_{c \mid n}\left(\sum_{d \mid (n/c)} f(c)\mu(d)\right) = \sum_{c \mid n}\left(f(c) \sum_{d \mid (n/c)} \mu(d)\right) \tag{2}$$

In compliance with Theorem 6.6, the sum $\sum_{d \mid (n/c)} \mu(d)$ must vanish except when $n/c = 1$ (that is, when $n = c$), in which case it is equal to 1; the upshot is that the right-hand side of Eq. (2) simplifies to

$$\sum_{c \mid n}\left(f(c) \sum_{d \mid (n/c)} \mu(d)\right) = \sum_{c=n} f(c) \cdot 1 = f(n)$$

giving us the stated result.

Let us use $n = 10$ again to illustrate how the double sum in Eq. (2) is turned around. In this instance, we find that

$$\begin{aligned}
\sum_{d \mid 10}\left(\sum_{c \mid (10/d)} \mu(d) f(c)\right) &= \mu(1)[f(1) + f(2) + f(5) + f(10)] \\
&\quad + \mu(2)[f(1) + f(5)] + \mu(5)[f(1) + f(2)] \\
&\quad + \mu(10) f(1) \\
&= f(1)[\mu(1) + \mu(2) + \mu(5) + \mu(10)] \\
&\quad + f(2)[\mu(1) + \mu(5)] + f(5)[\mu(1) + \mu(2)] \\
&\quad + f(10)\mu(1) \\
&= \sum_{c \mid 10}\left(\sum_{d \mid (10/c)} f(c)\mu(d)\right)
\end{aligned}$$

To see how the Möbius inversion formula works in a particular case, we remind the reader that the functions τ and σ may both be described as "sum functions":

$$\tau(n) = \sum_{d \mid n} 1 \qquad \text{and} \qquad \sigma(n) = \sum_{d \mid n} d$$

Theorem 6.7 tells us that these formulas may be inverted to give

$$1 = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \tau(d) \qquad \text{and} \qquad n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \sigma(d)$$

which are valid for all $n \geq 1$.

Theorem 6.4 ensures that if f is a multiplicative function, then so is $F(n) = \sum_{d \mid n} f(d)$. Turning the situation around, one might ask whether the multiplicative nature of F forces that of f. Surprisingly enough, this is exactly what happens.

Theorem 6.8. If F is a multiplicative function and

$$F(n) = \sum_{d \mid n} f(d)$$

then f is also multiplicative.

Proof. Let m and n be relatively prime positive integers. We recall that any divisor d of mn can be uniquely written as $d = d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1, d_2) = 1$. Thus, using the inversion formula,

$$\begin{aligned}
f(mn) &= \sum_{d \mid mn} \mu(d) F\left(\frac{mn}{d}\right) \\
&= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) \\
&= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\
&= \sum_{d_1 \mid m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2 \mid n} \mu(d_2) F\left(\frac{n}{d_2}\right) \\
&= f(m) f(n)
\end{aligned}$$

which is the assertion of the theorem. Needless to say, the multiplicative character of μ and of F is crucial to the previous calculation.

For $n \geq 1$, we define the sum

$$M(n) = \sum_{k=1}^{n} \mu(k)$$

Then $M(n)$ is the difference between the number of square-free positive integers $k \leq n$ with an even number of prime factors and those with an odd number of prime factors. For example, $M(9) = 2 - 4 = -2$. In 1897, Franz Mertens (1840–1927) published a paper with a 50-page table of values of $M(n)$ for $n = 1, 2, \ldots, 10000$. On the basis of the tabular evidence, Mertens concluded that the inequality

$$|M(n)| < \sqrt{n} \qquad n > 1$$

is "very probable." (In the previous example, $|M(9)| = 2 < \sqrt{9}$.) This conclusion later became known as the Mertens conjecture. A computer search carried out in

1963 verified the conjecture for all n up to 10 billion. But in 1984, Andrew Odlyzko and Herman te Riele showed that the Mertens conjecture is false. Their proof, which involved the use of a computer, was indirect and produced no specific value of n for which $|M(n)| \geq \sqrt{n}$; all it demonstrated was that such a number n must exist somewhere. Subsequently, it has been shown that there is a counterexample to the Mertens conjecture for at least one $n \leq (3.21)10^{64}$.

PROBLEMS 6.2

1. (a) For each positive integer n, show that

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$$

(b) For any integer $n \geq 3$, show that $\sum_{k=1}^{n} \mu(k!) = 1$.

2. The *Mangoldt function* Λ is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \text{ where } p \text{ is a prime and } k \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

Prove that $\Lambda(n) = \sum_{d \mid n} \mu(n/d) \log d = -\sum_{d \mid n} \mu(d) \log d$.
[*Hint:* First show that $\sum_{d \mid n} \Lambda(d) = \log n$ and then apply the Möbius inversion formula.]

3. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of the integer $n > 1$. If f is a multiplicative function that is not identically zero, prove that

$$\sum_{d \mid n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_r))$$

[*Hint:* By Theorem 6.4, the function F defined by $F(n) = \sum_{d \mid n} \mu(d) f(d)$ is multiplicative; hence, $F(n)$ is the product of the values $F(p_i^{k_i})$.]

4. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, use Problem 3 to establish the following:
(a) $\sum_{d \mid n} \mu(d)\tau(d) = (-1)^r$.
(b) $\sum_{d \mid n} \mu(d)\sigma(d) = (-1)^r p_1 p_2 \cdots p_r$.
(c) $\sum_{d \mid n} \mu(d)/d = (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r)$.
(d) $\sum_{d \mid n} d\mu(d) = (1 - p_1)(1 - p_2) \cdots (1 - p_r)$.

5. Let $S(n)$ denote the number of square-free divisors of n. Establish that

$$S(n) = \sum_{d \mid n} |\mu(d)| = 2^{\omega(n)}$$

where $\omega(n)$ is the number of distinct prime divisors of n.
[*Hint:* S is a multiplicative function.]

6. Find formulas for $\sum_{d \mid n} \mu^2(d)/\tau(d)$ and $\sum_{d \mid n} \mu^2(d)/\sigma(d)$ in terms of the prime factorization of n.

7. The *Liouville λ-function* is defined by $\lambda(1) = 1$ and $\lambda(n) = (-1)^{k_1+k_2+\cdots+k_r}$, if the prime factorization of $n > 1$ is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. For instance,

$$\lambda(360) = \lambda(2^3 \cdot 3^2 \cdot 5) = (-1)^{3+2+1} = (-1)^6 = 1$$

(a) Prove that λ is a multiplicative function.

(b) Given a positive integer n, verify that

$$\sum_{d \mid n} \lambda(d) = \begin{cases} 1 & \text{if } n = m^2 \text{ for some integer } m \\ 0 & \text{otherwise} \end{cases}$$

8. For an integer $n \geq 1$, verify the formulas below:
(a) $\sum_{d \mid n} \mu(d)\lambda(d) = 2^{\omega(n)}$.
(b) $\sum_{d \mid n} \lambda(n/d) 2^{\omega(d)} = 1$.

6.3 THE GREATEST INTEGER FUNCTION

The greatest integer or "bracket" function [ ] is especially suitable for treating divisibility problems. Although not strictly a number-theoretic function, its study has a natural place in this chapter.

Definition 6.4. For an arbitrary real number x, we denote by $[x]$ the largest integer less than or equal to x; that is, $[x]$ is the unique integer satisfying $x - 1 < [x] \leq x$.

By way of illustration, [ ] assumes the particular values

$$[-3/2] = -2 \quad [\sqrt{2}] = 1 \quad [1/3] = 0 \quad [\pi] = 3 \quad [-\pi] = -4$$

The important observation to be made here is that the equality $[x] = x$ holds if and only if x is an integer. Definition 6.4 also makes plain that any real number x can be written as

$$x = [x] + \theta$$

for a suitable choice of θ, with $0 \leq \theta < 1$.

We now plan to investigate the question of how many times a particular prime p appears in $n!$. For instance, if $p = 3$ and $n = 9$, then

$$\begin{aligned} 9! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \\ &= 2^7 \cdot 3^4 \cdot 5 \cdot 7 \end{aligned}$$

so that the exact power of 3 that divides $9!$ is 4. It is desirable to have a formula that will give this count, without the necessity of always writing $n!$ in canonical form. This is accomplished by Theorem 6.9.

Theorem 6.9. If n is a positive integer and p a prime, then the exponent of the highest power of p that divides $n!$ is

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

where the series is finite, because $[n/p^k] = 0$ for $p^k > n$.

Proof. Among the first n positive integers, those divisible by p are $p, 2p, \ldots, tp$, where t is the largest integer such that $tp \leq n$; in other words, t is the largest integer