18.781 Theory of Numbers

Problem Set 9

Official Solutions

May 3, 2026

Contents

Disclaimer

This document contains the official solutions to Problem Set 9 of the Spring 2026 edition of 18.781 Theory of Numbers. While carefully proofread, all errors, typos, and omissions are mine alone. Please email allenees@mit.edu should you have any questions or concerns. All references made herein refer to Niven and Montgomery's *An Introduction to the Theory of Numbers*, 5th edition.

1 §4.1 #2

Problem (§4.1 #2)
If 100! were written out in the ordinary decimal notation without the factorial sign, how many zeros would there be in a row at the right end?

Solution. The number of zeroes in a row at the right end of 100! is

24.

This is equivalent to finding the largest exponent e such that $10^e \mid 100!$. However, in the prime factorization of 100!, each factor of 10 is obtained from a prime factor of 2 and a prime factor of 5. Thus we find the largest exponents e_2 and e_5 such that $2^{e_2} \mid 100!$ and $2^{e_5} \mid 100!$, respectively, and then obtain $e = \min(e_2, e_5)$. By de Polignac's formula,

$$e_2 = \sum_{i=1}^{\infty} \left[\frac{100}{2^i}\right] = \left[\frac{100}{2}\right] + \left[\frac{100}{4}\right] + \left[\frac{100}{8}\right] + \left[\frac{100}{16}\right] + \left[\frac{100}{32}\right] + \left[\frac{100}{64}\right] = 97,$$
$$e_5 = \sum_{i=1}^{\infty} \left[\frac{100}{5^i}\right] = \left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] = 24,$$

so $e = \min(e_2, e_5) = 24$. ■

Remark 1. *This is a direct application of de Polignac's formula. The limiting reagent here is the* 5*; one needs one* 2 *and one* 5 *to make a factor of* 10*, so the number of* 10*s that one can make is bounded by number of* 2*s and the number of* 5*s, whichever is less.*

Theorem (de Polignac's formula, Theorem 4.2)
Let p denote a prime. Then the largest exponent e such that $p^e \mid n!$ is

$$e = \sum_{i=1}^{n} \left[\frac{n}{p^i}\right].$$

2 §4.1 #8

Problem (§4.1 #8)

For any positive real numbers x and y prove that

$$[x-y] \leq [x] - [y] \leq [x-y] + 1.$$

Proof. We rewrite Theorem 4.1(4) by

$$[a] + [b] \leq [a+b] \leq [a] + [b] + 1.$$

Put $a = x - y$ and $b = y$. On the one hand we have $[x-y] + [y] \leq [x]$, or

$$[x-y] \leq [x] - [y];$$

on the other hand, we obtain $[x] \leq [x-y] + [y] + 1$, or

$$[x] - [y] \leq [x-y] + 1.$$

Together we get the result. ■

Theorem (Theorem 4.1(4))

Let x and y be real numbers. Then we have $[x] + [y] \leq [x+y] \leq [x] + [y] + 1$.

3 §4.2 #6

Problem (§4.2 #6)
Prove that $\sum_{d|n} d = \sum_{d|n} n/d$, and more generally that $\sum_{d|n} f(d) = \sum_{d|n} f(n/d)$.

Proof. Let S be the set of divisors of n. Then the map $\phi\colon S \to S$ given by $d \mapsto n/d$ is a bijection. Therefore,

$$\{f(d) \mid d \mid n\} = \{f(n/d) \mid d \mid n\},$$

so $\sum_{d|n} f(d) = \sum_{d|n} f(n/d)$. Setting $f(d) = d$ gives the first equality. ■

Remark 2. *When d runs through all divisors of n, so does n/d.*

4 §4.2 #20

Problem (§4.2 #20)
For any positive integer let $\lambda(n) = (-1)^{\Omega(n)}$. This is *Liouville's lambda function*. Prove that $\lambda(n)$ is totally multiplicative, and that

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a perfect square,} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Recall that $\Omega(n)$ is the number of primes dividing n, counting multiplicity. In other words, if n has factorization

$$n = \prod_{p \text{ prime}} p^{\alpha(p)},$$

then $\Omega(n) = \sum_{p \text{ prime}} \alpha(p)$. If we write

$$m = \prod_{p \text{ prime}} p^{\beta(p)},$$

then $\lambda(mn) = (-1)^{\Omega(mn)} = (-1)^{\sum_p (\alpha(p)+\beta(p))} = (-1)^{\sum_p \alpha(p)}(-1)^{\sum_p \beta(p)} = (-1)^{\Omega(n)}(-1)^{\Omega(m)} = \lambda(m)\lambda(n)$, so λ is completely multiplicative. Now Theorem 4.4 implies that $\sum_{d|n} \lambda(d)$ is multiplicative, so it suffices to compute $\lambda(p^\alpha)$ for prime powers $p^\alpha \mid n$. Now

$$\sum_{d|p^\alpha} \lambda(d) = 1 + \lambda(p) + \cdots + \lambda(p^\alpha) = 1 - 1 + \cdots + (-1)^\alpha = \begin{cases} 1 & \text{if } \alpha \text{ is even,} \\ 0 & \text{if } \alpha \text{ is odd.} \end{cases}$$

Since $\sum_{d|n} \lambda(d)$ is multiplicative if $n = \prod_{p|n} p^{\alpha(p)}$ we then have

$$\begin{aligned} \sum_{d|n} \lambda(d) &= \prod_{p|n} \sum_{d|p^{\alpha(p)}} \lambda(d) \\ &= \prod_{p|n} \begin{cases} 1 & \text{if } \alpha(p) \text{ is even,} \\ 0 & \text{if } \alpha(p) \text{ is odd,} \end{cases} \\ &= \begin{cases} 1 & \text{if } \alpha(p) \text{ is even for all } p \mid n, \\ 0 & \text{otherwise,} \end{cases} \\ &= \begin{cases} 1 & \text{if } n \text{ is a perfect square,} \\ 0 & \text{otherwise,} \end{cases} \end{aligned}$$

as required. ∎

Remark 3. *Being multiplicative is a strong property for a function to have; it allows for straightforward computation of a function input by reducing it to computation at prime powers.*

Theorem (Theorem 4.4)
Let $f(n)$ be a multiplicative function and let $F(n) = \sum_{d|n} f(d)$. Then $F(n)$ is multiplicative.

5 §4.3 #7

Problem (§4.3 #7)
Prove that for every positive integer n, $\sum_{d|n}\mu(d)d(d) = (-1)^{\omega(n)}$. Similarly, evaluate $\sum_{d|n}\mu(d)\sigma(d)$.

Proof. Note that $\mu(n)$ is multiplicative, by Theorem 4.7. Then $\mu(n)d(n)$ is multiplicative as well since for $(m,n)=1$

$$\mu(mn)d(mn) = \mu(m)\mu(n)d(m)d(n) = \big(\mu(m)d(m)\big)\big(\mu(n)d(n)\big)$$

and d is multiplicative. Then $\sum_{d|n}\mu(d)d(d)$ is multiplicative by Theorem 4.4, so it suffices to compute $\mu\left(p^\alpha\right)d\left(p^\alpha\right)$ for prime powers $p^\alpha \mid n$. Now $\mu(p^a)=0$ for $a\geq 2$, so

$$\sum_{d|p^\alpha}\mu\left(d\right)d\left(d\right) = 1+\mu(p)d(p)+\cdots+\mu\left(p^\alpha\right)d\left(p^\alpha\right) = 1+\mu(p)d(p) = -1.$$

Since $\sum_{d|n}\mu(d)d(d)$ is multiplicative if $n=\prod_{p|n}p^{\alpha(p)}$ we then have

$$\sum_{d|n}\mu(d)d(d) = \prod_{p|n}\sum_{d|p^{\alpha(p)}}\mu(d)\lambda(p) = \prod_{p|n}(-1) = (-1)^{\omega(n)},$$

where $\omega(n)$ refers to the number of distinct primes dividing n.

Along similar lines, $\mu(d)\sigma(d)$ is multiplicative since for $(m,n)=1$

$$\mu(mn)\sigma(mn) = \mu(m)\mu(n)\sigma(m)\sigma(n) = \big(\mu(m)\sigma(m)\big)\big(\mu(n)\sigma(n)\big)$$

and σ is multiplicative. Then $\sum_{d|n}\mu(d)\sigma(d)$ is multiplicative by Theorem 4.4, so it suffices to compute $\mu\left(p^\alpha\right)\sigma\left(p^\alpha\right)$ for prime powers $p^\alpha \mid n$. Again, $\mu(p^a)=0$ for $a\geq 2$, so

$$\sum_{d|p^\alpha}\mu(d)\sigma(d) = 1+\mu(p)\sigma(p)+\cdots+\mu\left(p^\alpha\right)\sigma\left(p^\alpha\right) = 1+\mu(p)\sigma(p) = -p.$$

Since $\sum_{d|n}\mu(d)\sigma(d)$ is multiplicative if $n=\prod_{p|n}p^{\alpha(p)}$ we then have

$$\sum_{d|n}\mu(d)\sigma(d) = \prod_{p|n}\sum_{d|p^{\alpha(p)}}\mu(d)\sigma(d) = \prod_{p|n}(-p) = (-1)^{\omega(n)}\prod_{p|n}p,$$

as required. ∎

Theorem (Theorem 4.7)
The function $\mu(n)$ is multiplicative and

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & \text{if } n=1, \\ 0 & \text{otherwise.} \end{cases}$$

6 §4.3 #12

Problem (§4.3 #12)

Combine the results of the two preceding problems to get

$$\sum_{d|n} \frac{S(d)}{d^2} = \frac{1}{6}\left(2n+3+\frac{1}{n}\right).$$

Then apply the Möbius inversion formula to get

$$\frac{S(n)}{n^2} = \sum_{d|n} \frac{1}{6}\mu(d)\left(\frac{2n}{d}+3+\frac{d}{n}\right).$$

Proof. Let $S(n)$ denote the sum of squares of the positive integers $\leq n$ and prime to n. For context, the identities

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6},$$
$$\sum_{j=1}^{n} j^2 = \sum_{d|n} d^2 S\left(\frac{n}{d}\right) = \sum_{d|n} \frac{n^2}{d^2} S(d).$$

are given by the two preceding problems. Therefore

$$\sum_{d|n} \frac{S(d)}{d^2} = \frac{1}{n^2} \cdot \frac{n(n+1)(2n+1)}{6} = \frac{1}{6}\left(2n+3+\frac{1}{n}\right).$$

The Möbius inversion formula with $f(d) = S(d)/d^2$ gives

$$\frac{S(n)}{n^2} = f(n) = \sum_{d|n} \mu(d) \cdot \frac{1}{6}\left(2(n/d)+3+\frac{1}{n/d}\right) = \sum_{d|n} \frac{1}{6}\mu(d)\left(\frac{2n}{d}+3+\frac{d}{n}\right),$$

as required. ∎

Theorem (Möbius inversion formula, Theorem 4.8)

If $F(n) = \sum_{d|n} f(d)$ for every positive integer n, then $f(n) = \sum_{d|n} \mu(d)F(n/d)$.

7 §4.4 #3

Problem (§4.4 #3)

Prove that the Fibonacci numbers satisfy the inequalities

$$\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} < F_{n+1} < \left(\frac{1+\sqrt{5}}{2}\right)^{n}$$

if $n > 1$.

Proof. Write $\varphi = \left(1+\sqrt{5}\right)/2$ and $\psi = \left(1-\sqrt{5}\right)/2$. Note that φ and ψ are the solutions to $x^2 - x - 1 = 0$, so $\varphi + \psi = 1$ and $\varphi\psi = -1$. Moreover, $\varphi - \psi = \sqrt{5}$. Then we have

$$F_{n+1} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1} = \frac{\varphi^{n+1} - \psi^{n+1}}{\varphi - \psi}.$$

First we note that $-1 < \psi < 0$ and $\varphi > 1$. Then we have $\psi F_n < 0$ since $n > 1$. In other words,

$$\psi \cdot \frac{\varphi^n - \psi^n}{\varphi - \psi} < 0,$$

or equivalently $\psi(\varphi^n - \psi^n) < 0$. This implies that $\psi\varphi^n < \psi^{n+1}$, or equivalently that $\varphi^{n+1} + \psi\varphi^n < \varphi^{n+1} + \psi^{n+1}$, so

$$\varphi^{n+1} - \psi^{n+1} < \varphi^{n+1} - \psi\varphi^n = (\varphi - \psi)\varphi^n.$$

Dividing by $\varphi - \psi$ gives

$$F_{n+1} = \frac{\varphi^{n+1} - \psi^{n+1}}{\varphi - \psi} < \varphi^n = \left(\frac{1+\sqrt{5}}{2}\right)^{n},$$

as required. For the lower bound, recall that $\varphi^2 - \varphi = 1 = \psi^2 - \psi$, or equivalently $\psi^2 = \psi - \varphi + \varphi^2$. Note $\psi < \varphi$, so $\psi/\varphi < 1$ and $(\psi/\varphi)^{n-1} < 1$. This implies that $\psi^{n-1} < \varphi^{n-1}$, or $\psi^{n+1} < \varphi^{n-1}\psi^2 = \varphi^{n-1}\left(\psi - \varphi + \varphi^2\right)$. Thus,

$$(\varphi - \psi)\varphi^{n-1} = \varphi^n - \varphi^{n-1}\psi < \varphi^{n+1} - \psi^{n+1}.$$

Dividing by $\varphi - \psi$ gives

$$\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} = \varphi^{n-1} < \frac{\varphi^{n+1} - \psi^{n+1}}{\varphi - \psi} = F_{n+1},$$

as required. ∎

8 §4.4 #6

Problem (§4.4 #6)
Prove that $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

Proof. Write $\varphi = \left(1+\sqrt{5}\right)/2$ and $\psi = \left(1-\sqrt{5}\right)/2$. Note that φ and ψ are the solutions to $x^2 - x - 1 = 0$, so $\varphi + \psi = 1$ and $\varphi\psi = -1$. Moreover, $\varphi - \psi = \sqrt{5}$. Then we have

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n = \frac{\varphi^n - \psi^n}{\varphi - \psi}.$$

Using this expansion we obtain

$$\begin{aligned}
F_{n+1}F_{n-1} - F_n^2 &= \frac{\varphi^{n+1} - \psi^{n+1}}{\varphi - \psi} \cdot \frac{\varphi^{n-1} - \psi^{n-1}}{\varphi - \psi} - \left(\frac{\varphi^n - \psi^n}{\varphi - \psi}\right)^2 \\
&= \frac{1}{(\varphi - \psi)^2}\left(\left(\varphi^{n+1} - \psi^{n+1}\right)\left(\varphi^{n-1} - \psi^{n-1}\right) - \left(\varphi^n - \psi^n\right)^2\right) \\
&= \frac{1}{(\varphi - \psi)^2}\left(\left(\varphi^{2n} - \varphi^{n-1}\psi^{n+1} - \varphi^{n+1}\psi^{n-1} + \psi^{2n}\right) - \left(\varphi^{2n} - 2\varphi^n\psi^n + \psi^{2n}\right)\right) \\
&= \frac{1}{(\varphi - \psi)^2}\left(2\varphi^n\psi^n - \varphi^{n-1}\psi^{n+1} - \varphi^{n+1}\psi^{n-1}\right) \\
&= \frac{\varphi^{n-1}\psi^{n-1}}{(\varphi - \psi)^2}\left(2\varphi\psi - \psi^2 - \varphi^2\right) \\
&= -\frac{(\varphi\psi)^{n-1}}{(\varphi - \psi)^2}(\varphi - \psi)^2 \\
&= -(\varphi\psi)^{n-1} \\
&= -(-1)^{n-1} \\
&= (-1)^n,
\end{aligned}$$

as required. ∎