Number Theory Homework #1 *Spring 2025*

Instructor: *Chan Ieong Kuan*

Solutions by: ***Haoyu Zhu***

Exercises

1 UFD

1. Exercise 1.1:

   Proof. $(a,b)|(b,r)$: $r = a - qb$, so $(a,b)|r$. Additionally, $(a,b)|b$.

   $(b,r)|(a,b)$: by virtue of $a = qb + r$, then proceeds similar asforehead. □

2. Exercise 1.3:
   - (187, 221) = (187, 34) = (34, 17) = 17.
   - (6188, 4709) = (4709, 1479) = (1479, 272) = (272, 119) = (119, 34) = (34, 17) = 17.
   - (314,159) = (159,155) = (155, 4) = 1

3. Exercise 1.16:

   Proof. Since $\mathbb{Z}$ is a unique factorization domain and $(u,v) = 1$, one can decompose u, v with $0 \leq n_1 \leq n_2, e_i > 0$, and p_i primes:

   $$u = \prod_{i=1}^{n_1} p_i^{e_i}; v = \prod_{i=n_1+1}^{n_2} p_i^{e_i}; uv = \prod_{i=1}^{n_2} p_i^{e_i}$$

   In light of $uv = a^2$, e_i must all be even. Consequently, u, v are squares.

   □

4. Exercise 1.21

Proof. Without loss of generality, assume $ord_p\, a \leq ord_p\, b$, and write $r = ord_p\,(a+b), s = ord_p\, a, t = ord_p\, b$ satisfying

$$a = p^s q_a,\ b = p^t q_b, (a+b) = p^s(q_a + p^{(t-s)} q_b),$$

where q_a, q_b are relatively prime to p. Because p^s divides $a+b$, the inequality holds.

Moreover, when $t > s$,

$$q_a + p^{t-s} q_b \equiv q_a \pmod{p}$$

, so s is the maximal power of p factorizing $a+b$, thereby the equlity. □

5. Exercise 1.23

Proof. Suppose that a, b are both odd, then c^2 is even. As a result, c is even and $4|c^2 = a^2+b^2$, but a^2, b^2 are equivalent to 1 modulo 4. This is impossible. Consequently, one of a, b should be even, say a. For a, b, c are pairly coprime, b, c are odd numbers. Now $a^2 = (c-b)(c+b)$, and 4 divides both sides. One obtains:

$$\left(\frac{a}{2}\right)^2 = \frac{(c-b)}{2}\frac{(c+b)}{2}$$

Again, by virtue of $(b, c) = 1$, there exist $x, y \in \mathbb{Z}$ such that $xb + yc = 1$, then

$$(x+y)(\frac{(c+b)}{2}) + (y-x)\frac{(c-b)}{2} = 1.$$

Hence $(\frac{(c-b)}{2}, \frac{(c+b)}{2}) = 1$. According to Exercise 1.16, both $\frac{(c+b)}{2}$ and $\frac{(c-b)}{2}$ are squares which are coprime. Thereby the existence of u, v as stated in the problem.

Conversely, when $a = 2uv, b = v^2 - u^2, c = v^2 + u^2$, then

$$a^2 + b^2 = 4u^2v^2 + u^4 - 2u^2v^2 + v^4 = c^2$$

.

□

2 Arithmetic Functions

1. Number of Divisors Function: $\nu(n)$

The function $\nu(n)$ counts the number of positive divisors of n:

$$\nu(n) = \sum_{d|n} 1$$

2. Sum of Divisors Function: $\sigma(n)$

The function $\sigma(n)$ calculates the sum of all positive divisors of n:

$$\sigma(n) = \sum_{d|n} d$$

3. Generalized Sum of Divisors Function: $\sigma_s(n)$

For a real or complex number s, the function $\sigma_s(n)$ is defined as:

$$\sigma_s(n) = \sum_{d|n} d^s$$

4. Euler's Totient Function: $\phi(n)$

Euler's totient function $\phi(n)$ counts the number of integers up to n that are coprime to n:

$$\phi(n) = |\{k \in \mathbb{N} \mid 1 \leq k \leq n, \gcd(k, n) = 1\}|$$

5. Mobius Function: $\mu(n)$

The Mbius function $\mu(n)$ is defined as:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes,} \\ 0 & \text{if } n \text{ has a squared prime factor.} \end{cases}$$

6. Riemann Zeta Function: $\zeta(s)$

The Riemann zeta function $\zeta(s)$ is defined for complex numbers s with $\Re(s) > 1$ as:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

6. Exercise 2.10

Proof. For every coprime pair m, n, once $d \mid mn$, d can be uniquely factored into $d = d_1 d_2$, where $d_1 \mid m, d_2 \mid n$. Provided $(m, n) = 1$, one has

$$g(mn) = \sum_{d \mid mn} f(d) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2) = \left(\sum_{d_1 \mid m} f(d_1) \right) \left(\sum_{d_2 \mid n} f(d_2) \right) = g(m) g(n)$$

□

7. Exercise 2.12

Proof. Since $\phi(n), \mu(n)$ are multiplicative, the combinations of their products or quotients remain multiplicative. In terms of Exercise 2.10, the three Arithmetic Functions are multiplicative, too. As a result, they are determined completely by its value on prime powers. For any $n = \prod_{i=1}^{k} {p_i}^{e_i}$, applying multiplicative f one obtains $f(n) = \prod_{i=1}^{k} f({p_i}^{e_i})$. Now we only need to set $n = p^e$.

- $\sum_{d \mid p^e} \mu(d)\phi(d) = \mu(1)\phi(1) + \mu(p)\phi(p) = 1 - (p-1) = 2 - p$.
- $\sum_{d \mid p^e} \mu(d)^2 \phi(d)^2 = \mu(1)^2 \phi(1)^2 + \mu(p)^2 \phi(p)^2 = 1 + (p-1)^2 = p^2 - 2p + 2$.
- $\sum_{d \mid p^e} \mu(d)/\phi(d) = \mu(1)/\phi(1) + \mu(p)/\phi(p) = 1 - (p-1)^{-1}$.

The formulas for arbitrary positive integrers follow trivially. □

8. Exercise 2.22

Proof. For convenience, we define

$$f(n) = \sum_{(t,n)=1} t.$$

We start with the sum of all elements in $\{1, 2, \ldots, n\}$:

$$\sum_{i=1}^{n} i = \frac{(1+n)n}{2}.$$

Next, we partition the elements based on their greatest common divisor with n, rewriting the sum as:

$$\sum_{i=1}^{n} i = \sum_{d|n} \sum_{(t,n)=d} t.$$

Using the substitution $t = dt'$ where $(t', n/d) = 1$, we obtain:

$$\sum_{(t,n)=d} t = d \sum_{(t',n/d)=1} t' = df(n/d).$$

Thus, we conclude:

$$\begin{aligned}
&\frac{(1+n)n}{2} = \sum_{d|n} df(n/d), \\
\Leftrightarrow\quad &\frac{(1+n)n}{2} = \sum_{d|n} (n/d) f(d), \\
\Leftrightarrow\quad &(1+n) = \sum_{d|n} \frac{2f(d)}{d}.
\end{aligned}$$

Define $g(n) = \frac{2f(n)}{n}$. We want to show that $g(n) = \phi(n)$. Writing n in its prime factorization as $n = \prod_{i=1}^{k} p_i^{e_i}$, we obtain:

$$\begin{aligned}
&(1+n) = g * I(n), \\
\Leftrightarrow\quad &g(n) = (\mu * I) * g(n) = \mu * (I * g)(n) = \sum_{d|n} \mu(d) \left(1 + \frac{n}{d}\right), \\
\Leftrightarrow\quad &g(n) = (1+n) - \sum_{i=1}^{k} \left(1 + \frac{n}{p_i}\right) + \cdots + (-1)^k \left(1 + \frac{n}{\prod_{i=1}^{k} p_i}\right).
\end{aligned}$$

Note that $1 + \frac{n}{p}$ is the number of elements in $\{0, 1, 2, \ldots, n\}$ divided by p for $p \mid n$. By the principle of inclusion-exclusion, $g(n)$ equals to the number of elements in $\{0, 1, 2, \ldots, n\}$ that are coprime to n. We conclude that $g(n) = \phi(n)$.

$\square$

9. Exercise 2.25

Proof. We start with the Euler product formula for the Riemann zeta function:

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \sum_{i=1}^{\infty} \left(\frac{1}{p^s}\right)^i.$$

Taking the product over all primes and expanding the infinite series, we obtain:

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \sum_{i=1}^{\infty} \frac{1}{p^{is}} = \sum \prod_{i=1}^{N_n} \frac{1}{(p_i^s)^{e_i}}. \tag{1}$$

Next, we recover the Dirichlet series definition of the Riemann zeta function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{2}$$

Now, consider the alternative product expansion since each n can be uniquely factored as $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{1}{\prod_{i=1}^{N_n} (p_i^s)^{e_i}}. \tag{3}$$

We see that this expansion matches the right-hand side of the Euler product in equation (1), establishing the connection between the two representations of $\zeta(s)$.

□

10. Exercise 2.26

Proof. • Verification of $\zeta(s)^{-1} = \sum \frac{\mu(n)}{n^s}$

Starting from the Euler product representation of $\zeta(s)$:

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Taking the reciprocal:

$$\zeta(s)^{-1} = \prod_p \left(1 - \frac{1}{p^s}\right).$$

Expanding each term as an infinite product:

$$\prod_p \left(1 - \frac{1}{p^s}\right) = \sum \frac{(-1)^k}{(\prod_{i=1}^k p_i^s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

- Verification of $\zeta(s)^2 = \sum \frac{\nu(n)}{n^s}$

  Squaring the Euler product results in a double sum:

$$\zeta(s)^2 = \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{1}{(mn)^s}.$$

  We introduce the function $\nu(n)$, which counts the number of ways to write n as a product of two factors m and n:

$$\nu(n) = \sum_{d|n} 1.$$

  Thus, we can partition the sum above in terms of the value of mn, write M, and obtain:

$$\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{1}{(mn)^s} = \sum_{M=1}^{\infty} \sum_{n|M} \frac{1}{(M)^s} = \sum_{M=1}^{\infty} \frac{\nu(M)}{M^s}.$$

- Verification of $\zeta(s)\zeta(s-1) = \sum \frac{\sigma(n)}{n^s}$

  Starting from the product representation:

$$\zeta(s)\zeta(s-1) = \left(\sum_{m=1}^{\infty} \frac{1}{m^s}\right)\left(\sum_{n=1}^{\infty} \frac{1}{n^{s-1}}\right).$$

  Expanding the double sum:

$$\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{1}{m^s n^{s-1}} \overset{(M=mn)}{=} \sum_{M=1}^{\infty} \sum_{n|M} \frac{n}{M^s} = \sum_{M=1}^{\infty} \frac{\sum_{n|M} n}{M^s} = \sum_{M=1}^{\infty} \frac{\sigma(M)}{M^s}.$$

  where $\sigma(M) = \sum_{d|M} d$ is the sum of divisors function.

$\square$