Number Theory Homework #1 *Spring 2026*

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

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

.

□

6. Exercise 1.25

Proof. If $a^n - 1$ is prime, note that $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + 1)$. Since $a^n - 1$ is prime, one of these factors must be 1. Clearly $a^{n-1} + \cdots + 1 > 1$ for $a > 1$, so we must have $a - 1 = 1$, hence $a = 2$.

Now suppose n is composite, say $n = pq$ with $p, q > 1$. Then $2^n - 1 = 2^{pq} - 1 = (2^p)^q - 1$. Since $x^q - 1 = (x-1)(x^{q-1} + \cdots + 1)$, we have $2^p - 1 \mid 2^{pq} - 1$. Similarly, $2^q - 1 \mid 2^{pq} - 1$. Since $2^{pq} - 1$ is prime, one of these divisors must be 1 or the number itself. But $2^p - 1 > 1$ and $2^q - 1 > 1$ for $p, q > 1$, contradicting that $2^n - 1$ is a prime. Therefore n cannot be composite, so n is prime. □

7. Exercise 1.33

Proof. Necessity: if $\alpha = a + bi$ is a unit, then $\exists c + di$ such that $(a + bi)(c + di) = 1$. Take modulus, and we have $\lambda(a + bi)\lambda(c + di) = 1$, where a, b, c, d are integers and thus $(a^2 + b^2), (c^2 + d^2)$ are non-negative inegers and have to be both 1. Hence $\lambda(\alpha) = 1$.

Sufficiency: when $\lambda(\alpha) = 1, \alpha = 1, -1, i, -i$ which can be verified to be units because $(-1) * (-1) = 1, i * (-i) = 1$. □

2 Arithmetic Functions

8. Exercise 2.6

Proof. For each integer $k \geq 1$, the numbers among $1, 2, \ldots, n$ that are divisible by p^k are $p^k, 2p^k, 3p^k, \ldots, \lfloor n/p^k \rfloor p^k$. Thus there are exactly $\lfloor n/p^k \rfloor$ multiples of p^k in $\{1, 2, \ldots, n\}$.

Now consider the prime factorization of $n!$. The exponent of p in $n!$ counts how many factors of p appear in the product $1 \cdot 2 \cdots n$. Each multiple of p contributes at least one factor of p. Among these, the multiples of p^2 contribute another more p, and so on.

Therefore, the total exponent of p in $n!$ is:

$$\begin{aligned} \operatorname{ord}_p n! &= (\text{number of multiples of } p) \\ &\quad + (\text{number of multiples of } p^2) \\ &\quad + (\text{number of multiples of } p^3) + \cdots \\ &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \end{aligned}$$

This sum is finite since $\lfloor n/p^k \rfloor = 0$ when $p^k > n$. □

9. Exercise 2.7

Proof. For the first inequality, note that $\left\lfloor \frac{n}{p^i} \right\rfloor \leq \frac{n}{p^i}$. Therefore,

$$\operatorname{ord}_p n! \leq \sum_{i=1}^{\infty} \frac{n}{p^i} = n \sum_{i=1}^{\infty} \frac{1}{p^i} = n \cdot \frac{1/p}{1 - 1/p} = \frac{n}{p-1}.$$

For the second inequality, we write $n!$ as a product over all primes:

$$n! = \prod_{p \leq n} p^{\operatorname{ord}_p n!}.$$

Using the inequality just proved,

$$n! = \prod_{p \leq n} p^{\operatorname{ord}_p n!} \leq \prod_{p \leq n} p^{n/(p-1)}.$$

Taking the nth root of both sides yields

$$(n!)^{1/n} \leq \prod_{p \leq n} p^{1/(p-1)},$$

where the product is taken over all primes p dividing $n!$ (i.e., all primes $p \leq n$). □

10. Exercise 2.8

Proof. Assume, for contradiction, that there are only finitely many primes. Then the product $\prod_p p^{1/(p-1)}$ over all primes would be some finite constant C, independent of n. Consequently, for all n we would have

$$(n!)^{1/n} \leq C.$$

However, we know that $n! \geq (n/2)^{n/2}$ for $n \geq 2$ (since at least the last $n/2$ factors are $\geq n/2$). Taking nth roots gives

$$(n!)^{1/n} \geq \left(\frac{n}{2}\right)^{1/2}.$$

The right-hand side grows without bound as $n \to \infty$. This is a contradiction for sufficiently large n, and hence there are infinitely many primes. □

11. 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.

□