

Number Theory Homework #2 Spring 2026

Instructor: *Chan Jeong Kuan*

Solutions by: *Haoyu Zhu*

EXERCISES

UFD(I missed to finish last time:)

1. 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 integers 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 $(-1) * (-1) = 1, i * (-i) = 1$. \square

3 Congruence

2. Exercise 3.17:

Proof. (\Rightarrow): If there exists $x_0 \in \mathbb{Z}_n$ solving $f(x) \equiv 0 \pmod{n}$, then it simultaneously solves $f(x) \equiv 0 \pmod{p_i^{a_i}}$ as an element in $\mathbb{Z}_{p_i^{a_i}}$ after applying the canonical projection

$\mathbb{Z}_n \rightarrow \mathbb{Z}_{p_i^{a_i}}$. This is well-defined because $f(x) \in \mathbb{Z}[x]$ and $n = \prod_{i=1}^t p_i^{a_i}$.

(\Leftarrow): Assume that $f(x_i) \equiv 0 \pmod{p_i^{a_i}}$ for each i . Equivalently speaking, $f(x_i) = 0 \in \mathbb{Z}_{p_i^{a_i}}$ with $x \in \mathbb{Z}_{p_i^{a_i}}$ and $f(x) \in \mathbb{Z}_{p_i^{a_i}}[x]$. In terms of **Chinese Remainder Theorem**, $p_i^{a_i}$ being pairwise relatively prime integers, we can find a unique $x_0 \in \mathbb{Z}_n$ such that $x_0 = x_i$ in $\mathbb{Z}_{p_i^{a_i}}$ as projecting $\mathbb{Z}_n \rightarrow \mathbb{Z}_{p_i^{a_i}}$ canonically. Now embedding $\mathbb{Z}_{p_i^{a_i}}$ and $\mathbb{Z}_{p_i^{a_i}}[x]$ into \mathbb{Z}_n and $\mathbb{Z}_n[x]$, respectively, we establish that $f(x_0) = 0 \in \mathbb{Z}_n$ since moreover,

$$\mathbb{Z}_n = \bigoplus_{i=1}^t \mathbb{Z}_{p_i^{a_i}}.$$

Remark that a ring-theoretic-free but equivalent argument is as below: since $f(x_0) \equiv 0$ modulo every $p_i^{a_i}$, $f(x_0) \equiv 0$ modulo their least common multiple, write

$$\text{lcm}_i(p_i^{a_i}) = \prod_{i=1}^t p_i^{a_i} = n.$$

□

3. Exercise 3.18:

Proof. As the canonical mappings show in 2 (Ex. 3.17), every $x_0 \in \mathbb{Z}_n$ one-to-one corresponds to the t-tuple $(x_i)_i$, and vice versa. According to the principle of multiplicity in combinatorics, $N = N_1 \cdots N_t$. □

4. Exercise 3.19:

Proof. Over the ring \mathbb{Z}_p , $x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0$. Consequently, assuming first $x \neq \pm 1$, $(x-1)$ and $(x+1)$ are zero divisors, which implies that p divides both of them and hence, their difference $(x+1) - (x-1) = 2$. However, p is an odd prime, which leads to contradiction. Thus, the solutions have to be only ± 1 . □

5. Exercise 3.20:

Proof. • $b = 1 : x = 1 \in \mathbb{Z}_2$.

• $b = 2 : x = \pm 1 \in \mathbb{Z}_4$.

• $b \geq 3 : (x+1)(x-1) = 0 \in \mathbb{Z}_{2^b}$. Since $(x+1)$ and $(x-1)$ share the same sign with a greatest common divisor less or equal than 2 over \mathbb{Z}_{2^b} , we need and only need one of them being divided by 2^{b-1} . Therefore, there are precisely four solution. □

6. Exercise 3.21:

Proof. Say $n = 2^b \prod_{i=1}^t p_i^{a_i}$. In light of multiplicity formula as in 3,

$$N = N(2) \prod_{i=1}^t N(p_i^{a_i}) = N(2) * 2^t,$$

where $N(2)$ is the number of solutions to $x^2 = 1 \pmod{2^b}$ given by 5. □

4 Unit group

7. Exercise 4.6: Show that 3 is a primitive root modulo p , a Fermat prime of the form $2^n + 1$.

Proof. Otherwise, with $p = 2^n + 1$ a prime, we can define its primitive root, say g , and hence $3 \equiv g^k \pmod{p}$, where k satisfies $1 < k < p - 1 = 2^n$. Since $g^{2^n} \equiv 1 \pmod{p}$, we know that k divides 2^n and $3^{\frac{2^n}{k}} \equiv 1 \pmod{p}$. Therefore, k is even and 3 is a quadratic residue modulo p . However, for every $n \geq 4$, $2^n + 1 \equiv 2 \pmod{3}$, so by law of quadratic reciprocity,

$$\left(\frac{3}{2^n + 1}\right) \left(\frac{2^n + 1}{3}\right) = (-1)^{(2^n - 1)(1)} \Leftrightarrow \left(\frac{3}{2^n + 1}\right) (-1) = 1 \Leftrightarrow \left(\frac{3}{2^n + 1}\right) = -1,$$

which contradicts that 3 is a quadratic residue.

When $n \leq 3$, i.e. $p = 5$, it is easy to verify that 3 is a primitive root.

(Remark: I fail to find any solution not using the LAW OF QUADRATIC RESIDUES ...) \square

8. Exercise 4.11:

Proof. Denote by g some generator of $U(\mathbb{Z}_p) = \{1, 2, \dots, p-1\}$, i.e. one of the primitive roots modulo p . Then, $g^{p-1} = 1 \in \mathbb{Z}_p$. We do all our next computation over \mathbb{Z}_p .

When $p - 1 \nmid k \Leftrightarrow g^k \neq 1$ in \mathbb{Z}_p ,

$$\sum_{i=1}^{p-1} i^k = \sum_{i=0}^{p-2} (g^i)^k = \sum_{i=0}^{p-2} (g^k)^i = \frac{g^{(p-1)k} - 1}{g^k - 1} = 0.$$

When $p - 1 \mid k \Leftrightarrow g^k = 1 \in \mathbb{Z}_p$,

$$\sum_{i=1}^{p-1} i^k = \sum_{i=0}^{p-2} (g^k)^i = \sum_{i=0}^{p-2} 1 = p - 1 = -1.$$

\square

5 Quadratic Residues

9. Exercise 5.5:

Proof. Provided that $p \nmid a$, when x runs modulo p , so does $y = ax + b$. Therefore,

$$\sum_{x=0}^{p-1} ((ax + b)/p) = \sum_{x=0}^{p-1} (y/p) = 0.$$

The last equation holds because there are as many non-residues as residues. \square

10. Exercise 5.11:

Proof. Note that $2^p = 2^{(q-1)/2} = (2/q) = (-1)^{q^2-1/8} = (-1)^{p^2+p/2} = 1 \in \mathbb{Z}_q$. The last equation is obtained from the fact that $p \equiv 3 \pmod{4}$. Thus, prime q is a factor of $2^p - 1$, completing the proof. \square

11. Exercise 5.29:

Proof. Write the primitive root in \mathbb{Z}_p as g , hence write $i = g^{e_i}$, $i = 1, 2, \dots, p-1$. Besides, denote the numbers of residues and nonresidues by, respectively, $(R), (N)$. We have already known very clearly that $(R) = (N) = \frac{p-1}{2}$.

Now the set (with ascending order) $\{1, 2, \dots, p-1\}$ can be represented in the same order by $\{e_1, e_2, \dots, e_{p-1}\}$, and some i is a quadratic residue if and only if e_i is an even integer.

We can first without any effort conduct the total counting:

$$p - 2 = (RR) + (NR) + (RN) + (NN). \quad (1)$$

Then, since 1 is always a quadratic residue and $(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p}$, the numbers of each pair depend on the residue of p modulo 4. From another perspective, if we add $(p-1, 1)$ into these $(p-2)$ pairs and complete the cycle in $U(\mathbb{Z}_p)$, then we obtain exactly from $(R) = (N) = \frac{p-1}{2}$:

$$(RR) + (RN) = (NR) + (NN) = (RR) + (NR) = (RN) + (NN) = \frac{p-1}{2}.$$

Thus, we only need to exam which type $(p-1, 1)$ falls into and then cancel it out.

- When $p \equiv 3 \pmod{4}$, we compute $(-1/p) \equiv (-1)^{(p-1)/2} \equiv -1 \pmod{p}$. Therefore, the $(p-1, 1) = (NR)$.

$$\begin{aligned}(RR) + (RN) &= \frac{p-1}{2}, \\(NR) + (NN) &= \frac{p-1}{2} - 1, \\(RR) + (NR) &= \frac{p-1}{2} - 1, \\(RN) + (NN) &= \frac{p-1}{2}.\end{aligned}$$

- When $p \equiv 1 \pmod{4}$, we compute $(-1/p) \equiv 1 \pmod{p}$. In this case, the $(p-1, 1) = (RR)$.

$$\begin{aligned}(RR) + (RN) &= \frac{p-1}{2} - 1, \\(NR) + (NN) &= \frac{p-1}{2}, \\(RR) + (NR) &= \frac{p-1}{2} - 1, \\(RN) + (NN) &= \frac{p-1}{2}.\end{aligned}$$

□

Prepare for 5.30 Exercise 5.6 to 5.8:

Proof. On one hand, for y satisfying $(\frac{y^2+a}{p}) = 1$ we have 2 solutions: (x, y) and $(-x, y)$, while for y satisfying $(\frac{y^2+a}{p}) = -1$ we have no solutions. We now add up all cases with y running from 0 to $p-1$ and obtain the number of solutions is $\sum_{y=0}^{p-1} (1 + (\frac{y^2+a}{p}))$.

On the other hand, write $u = x + y, v = x - y, uv \equiv a(p)$. $p \nmid a$ infers p does not divide u, v , hence the existence of u^{-1}, v^{-1} . Once we fix $u(p)$, $v \equiv u^{-1}a(p)$ is determined, hence $p-1$ solutions. When $p \mid a$, solutions are $\{(0, v) \mid v(p)\} \cup \{(u, 0) \mid u(p)\}$, i.e. $2p-1$ solutions.

With the double counting of number of solutions to $x^2 - y^2 \equiv a(p)$, we prove Ex. 8 that $\sum_{y=0}^{p-1} (\frac{y^2+a}{p})$ is either -1 (when $p \nmid a$) or $p-1$ (when $p \mid a$). □

12. Exercise 5.30:

Proof. Since $n, n+1, p$ are pairwise relatively prime integers, $(n(n+1)/p) = (n/p)(n+1/p)$. It equals to 1 for $(RR), (NN)$ pairs and -1 for the others, hence the first equation. It remains to show that the sum is -1. Using Ex. 8 and properties of Jacobi symbols,

$$\begin{aligned}
 \sum_{n=1}^{p-1} \left(\frac{n(n+1)}{p} \right) &= \sum_{n=1}^{p-1} \left(\frac{(n + \frac{p+1}{2})^2 - (\frac{p+1}{2})^2}{p} \right) \\
 &= \sum_{n=0}^{p-1} \left(\frac{(n + \frac{p+1}{2})^2 - (\frac{p+1}{2})^2}{p} \right) - \left(\frac{(\frac{p+1}{2})^2 - (\frac{p+1}{2})^2}{p} \right) \\
 &= -1 - 0 \\
 &= -1.
 \end{aligned}$$

□

13. Exercise 5.31:

Proof.

$$\begin{array}{cccc}
 (RR) & +(NN) & -(RN) & -(NR) \\
 & -(NN) & -(RN) & \\
 + & 2(RR) & & +2(RN) \\
 + & (RR) & & +(NR) \\
 \hline
 & 4(RR) & &
 \end{array}$$

Then plug-in the previous results and complete the verification.

□