

# 18.781 Theory of Numbers

## Quiz 2

### Official Solutions

April 9, 2026

## Contents

|   |           |   |
|---|-----------|---|
| 1 | Problem 1 | 2 |
| 2 | Problem 2 | 3 |
| 3 | Problem 3 | 4 |
| 4 | Problem 4 | 5 |
| 5 | Problem 5 | 6 |
| 6 | Problem 6 | 8 |
| 7 | Bonus     | 9 |

## Disclaimer

This document contains the official solutions to Quiz 2 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](mailto: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 Problem 1

## Problem (Problem 1(1))

State each of the following clearly.

(1) Hensel's lemma

*Solution.* Suppose that  $f(X)$  is a polynomial with integral coefficients. If  $f(a) \equiv 0 \pmod{p^j}$  and  $f'(a) \not\equiv 0 \pmod{p}$ , then there exists a unique  $t \pmod{p}$  such that  $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$ . ■

**Remark 1.** Here are some common mistakes.

- Some students stated the lemma only for the case when  $j = 1$ , not for general  $j \in \mathbb{N}$ .
- Some students did not say that the  $t \pmod{p}$  is **unique**.
- Some students just stated "lifting lemma" without giving details.
- Some students incorrectly stated Hensel's lemma as an if and only if statement.

## Problem (Problem 1(2))

State each of the following clearly.

(2) Quadratic Reciprocity Law for Jacobi Symbols

*Solution.* If  $P$  and  $Q$  are odd and positive and if  $(P, Q) = 1$ , then  $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$ . ■

**Remark 2.** Here are some common mistakes.

- Some students left out the condition that  $P$  and  $Q$  are **odd**.
- Some students left out the **coprime** condition  $(P, Q) = 1$ .

## 2 Problem 2

### Problem (Problem 2(1))

Determine how many solutions there are for each of the following equations:

$$(1) X^6 \equiv -1 \pmod{65}$$

*Solution.* There are

12 solutions.

By the Chinese remainder theorem, the number of solutions is simply the product of the number of solutions of the congruences  $X^6 \equiv -1 \pmod{5}$  and  $X^6 \equiv -1 \pmod{13}$ . Recall that the congruence  $X^n \equiv a \pmod{p}$  (where  $(a, p) = 1$ ) has  $(n, p-1)$  solutions if and only if  $a^{(p-1)/(n, p-1)} \equiv 1 \pmod{p}$ . For the former, set  $n = 6$ ,  $p = 5$ , and  $a = 4$  to obtain  $(6, 4) = 2$  solutions; for the latter, set  $n = 6$ ,  $p = 13$ , and  $a = 12 \equiv -1 \pmod{p}$  to obtain  $(6, 12) = 6$  solutions. ■

### Problem (Problem 2(2))

Determine how many solutions there are for each of the following equations:

$$(2) X^7 - X \equiv 0 \pmod{7^2}$$

*Solution.* There are

7 solutions.

Let  $f(X) = X^7 - X$ . We have  $f(X) \equiv 0 \pmod{7}$  by Fermat's little theorem, so the congruence  $X^7 - X \equiv 0 \pmod{7}$  has 7 solutions modulo 7. Because the derivative  $f'(X) = 7X^6 - 1$  does not vanish modulo 7 (i.e.,  $f'(0) = -1 \not\equiv 0 \pmod{7}$  and  $f'(X) \equiv 7X^6 - 1 \pmod{p} \equiv 6 \pmod{p}$  for nonzero  $X$  by Fermat's little theorem), each of the seven solutions lift to a unique solution modulo  $7^2$ , by Hensel's lemma. ■

### Problem (Problem 2(3))

Determine how many solutions there are for each of the following equations:

$$(3) f(X) \equiv 0 \pmod{7^n} \text{ where } f(X) = X^3 - 2X^2 + X - 2 \text{ for each } n \in \mathbb{N}.$$

*Solution.* There is

1 solution for all  $n \in \mathbb{N}$ .

Write  $f(X) = (X^2 + 1)(X - 2)$ . We first work with  $n = 1$ . We have  $f(2) = 0$  (i.e.,  $X = 2$  is a solution). This is the only solution since 7 is a prime  $7 \equiv 3 \pmod{4}$ , so  $-1$  is not a quadratic residue modulo 7 since

$$\left(\frac{-1}{7}\right) = -1.$$

In particular,  $X^2 + 1 \equiv 0 \pmod{7}$  has no solutions. Now note  $f'(X) = 3X^2 - 4X + 1$  and  $f'(2) \not\equiv 0 \pmod{7}$ , so by Hensel's lemma, 2 lifts to a solution modulo  $7^2$  that is also  $\equiv 2 \pmod{7}$ . This is an invariant (i.e., repeated lifts are always  $\equiv 2 \pmod{p}$  by construction), so we apply Hensel's lemma repeatedly to obtain a unique solution modulo  $7^n$  for all  $n \in \mathbb{N}$ . ■

### 3 Problem 3

**Problem (Problem 3)**

Solve  $X^5 \equiv -125 \pmod{64}$ . (Hint: Recall  $\{\pm 5, \pm 5^2, \dots, \pm 5^{16}\}$  is a complete reduced residue system modulo 64.)

*Solution.* The solution is

$$X = -5^7.$$

The hint immediately implies that  $\phi(64) = 32$  (since the set  $\{\pm 5, \pm 5^2, \dots, \pm 5^{16}\}$  has 32 elements). Since  $-125 = -5^3$  is in the complete reduced residue system modulo 64 and multiplication in any complete reduced residue system modulo  $m$  is closed (i.e., the product of any two integers that are coprime to  $m$  is also coprime to  $m$ ), any integer  $x$  such that  $x^5 \equiv -125 \pmod{64}$  must be in the complete reduced residue system modulo 64. Thus,  $x = -5^k$  for some  $k \in \{1, \dots, 16\}$  (since it clearly can't be the positive version  $5^k$ ). As such, if  $x^5 \equiv -125 \pmod{64}$ , then  $-5^{5k} \equiv -5^3 \pmod{64}$ , which implies  $5k \equiv 3 \pmod{\phi(64)}$ , or equivalently  $5k \equiv 3 \pmod{32}$ . Now note  $(5, 32) = 1$ , and  $5 \cdot 45 \equiv 1 \pmod{32}$ , so  $k \equiv 3 \cdot 45 \pmod{32} \equiv 7 \pmod{32}$ . Thus  $x = -5^7$  is a solution. ■

## 4 Problem 4

### Problem (Problem 4(1))

In the following,  $p$  denotes an odd prime number. Explain your reasoning clearly.

Suppose that  $p$  is a prime with  $p = 2^{2^n} + 1$  for some positive integer  $n$ .

(1) Show that

$$3^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

*Proof.* By Euler's criterion,

$$3^{(p-1)/2} \equiv \left(\frac{3}{p}\right) \pmod{p},$$

so it suffices to show that 3 is *not* a quadratic residue modulo  $p$ . Since  $n \geq 1$  is an integer, we have  $p \equiv 1 \pmod{4}$  since  $p = 2^{2^n} + 1 = 2^{2 \cdot 2^{n-1}} + 1 = 4^{2^{n-1}} + 1$ . Therefore, quadratic reciprocity implies

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

since 2 is not a quadratic residue modulo 3. This finishes the proof. ■

### Problem (Problem 4(2))

In the following,  $p$  denotes an odd prime number. Explain your reasoning clearly.

Suppose that  $p$  is a prime with  $p = 2^{2^n} + 1$  for some positive integer  $n$ .

(2) Compute the order of 3 mod  $p$ .

*Solution.* Let  $h$  denote the order of 3 mod  $p$ . The previous part implies that  $h \nmid (p-1)/2$ ; otherwise, if  $h \mid (p-1)/2$ , say  $hg = (p-1)/2$  for some  $g \in \mathbb{Z}$ , then

$$3^{(p-1)/2} \equiv 3^{hg} \pmod{p} \equiv (3^h)^g \pmod{p} \equiv 1^g \pmod{p} \equiv 1 \pmod{p},$$

contrary to the previous part. On the other hand,  $h \mid \phi(p) = p-1$ . Thus

- $h \nmid (p-1)/2 = 2^{2^n-1}$  and
- $h \mid p-1 = 2^{2^n}$ .

In particular,  $h$  is a power of 2, and the only power of 2 that divides  $2^{2^n}$  and does not divide  $2^{2^n-1}$  is  $2^{2^n} = p-1$  itself. Thus,  $h = p-1$ , which means that 3 is a primitive root modulo  $p$ . ■

## 5 Problem 5

### Problem (Problem 5(1))

In the following,  $p$  denotes an odd prime number. Explain your reasoning clearly.

Let  $k \in \mathbb{N}$ . Consider  $f_k: (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$  defined by

$$f_k(n) \equiv n^k \pmod{p} \quad \text{for } n \in (\mathbb{Z}/p\mathbb{Z})^\times.$$

(1) Prove that  $f_k$  is a group homomorphism.

*Proof.* Let  $n, m \in (\mathbb{Z}/p\mathbb{Z})^\times$ . Then

$$f_k(nm) \equiv (nm)^k \pmod{p} \equiv n^k m^k \pmod{p} = f_k(n) + f_k(m),$$

as desired. ■

### Problem (Problem 5(2))

In the following,  $p$  denotes an odd prime number. Explain your reasoning clearly.

Let  $k \in \mathbb{N}$ . Consider  $f_k: (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$  defined by

$$f_k(n) \equiv n^k \pmod{p} \quad \text{for } n \in (\mathbb{Z}/p\mathbb{Z})^\times.$$

(2) Prove that  $f_k$  is a group isomorphism if and only if  $(k, p-1) = 1$ .

*Proof.* Since  $p$  is an odd prime, it has a primitive root  $g \pmod{p}$ . Therefore, any  $n \in (\mathbb{Z}/p\mathbb{Z})^\times$  can be expressed uniquely as  $n = g^\ell$  for some  $\ell \in \{1, \dots, p-1\}$ . Let  $e(n) = \ell$  denote this exponent for any  $n \in (\mathbb{Z}/p\mathbb{Z})^\times$ . Then we write

$$f_k(n) \equiv n^k \pmod{p} = g^{e(n)k} \pmod{p}.$$

In the previous part we showed that  $f_k$  is a homomorphism, so we just need to show that it is bijective iff  $(k, p-1) = 1$ . Let  $m \in (\mathbb{Z}/p\mathbb{Z})^\times$ , so  $(m, p) = 1$ . Recall that the congruence  $n^k \equiv m \pmod{p}$  (i.e.,  $f_k(n) = m$ ) has  $(k, p-1)$  solutions or no solutions according as  $m^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$  or not.

( $\Leftarrow$ ) Suppose  $(k, p-1) = 1$ . Then there exists a unique  $n \in (\mathbb{Z}/p\mathbb{Z})^\times$  such that  $f_k(n) = m$  has  $(k, p-1) = 1$  solution since  $m^{(p-1)/(k, p-1)} \equiv m^{p-1} \pmod{p} \equiv 1 \pmod{p}$  by Fermat's little theorem. Since each  $m \in (\mathbb{Z}/p\mathbb{Z})^\times$  has an unique preimage  $n \in (\mathbb{Z}/p\mathbb{Z})^\times$ ,  $f_k$  is a bijection.

( $\Rightarrow$ ) Suppose  $(k, p-1) > 1$ . If  $m^{(p-1)/(k, p-1)} \not\equiv 1 \pmod{p}$ , then  $n^k \equiv m$  has no solutions. Therefore,  $f_k$  is not surjective since  $f_k(n) \neq m$  for any  $n \in (\mathbb{Z}/p\mathbb{Z})^\times$ . On the other hand, if  $m^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$ , then  $n^k = m$  has  $(k, p-1) > 1$  solutions. Therefore,  $f_k$  is not injective since  $m \in (\mathbb{Z}/p\mathbb{Z})^\times$  has more than one preimage under  $f_k$ . ■

**Remark 3.** If one doesn't recall the above property about congruences  $n^k \equiv m \pmod{p}$ , then we give another proof that uses primitive roots (and essentially reproves this property).

*Alternate proof.* We again use  $g$  to denote a primitive root modulo  $p$  and  $e(n) = \ell$  to mean that  $n = g^\ell$ .

( $\Leftarrow$ ) Suppose  $(k, p-1) = 1$ . Let  $k^{-1}$  be the modular inverse of  $k$  modulo  $p-1$ , i.e.,  $kk^{-1} \equiv 1 \pmod{p-1}$ .

- For injectivity, consider  $n, m \in (\mathbb{Z}/p\mathbb{Z})^\times$  and suppose that  $f_k(n) = f_k(m)$ . Then

$$f_k(n) \equiv g^{e(n)k} \pmod{p} \equiv g^{e(m)k} \pmod{p} = f_k(m),$$

which implies that  $e(n)k \equiv e(m)k \pmod{p-1}$ . We multiply by  $k^{-1}$  to obtain  $e(n) \equiv e(m) \pmod{p-1}$ . Thus,  $e(n) = (p-1)r + e(m)$  for some  $r \in \mathbb{Z}$ . Then

$$n \equiv g^{e(n)} \pmod{p} \equiv g^{(p-1)r + e(m)} \pmod{p} \equiv g^{e(m)} \pmod{p} \equiv m \pmod{p}.$$

Then  $n = m$ .

- For surjectivity, let  $m \in (\mathbb{Z}/p\mathbb{Z})$ . Note  $m = g^{e(m)}$ . Then consider  $n = g^{k^{-1}e(m)}$ . We compute

$$f_k(n) \equiv n^k \pmod{p} \equiv g^{k^{-1}e(m)k} \pmod{p} \equiv g^{e(m)} \pmod{p} \equiv m \pmod{p},$$

where in the exponent  $k^{-1}e(m)k \equiv e(m) \pmod{p-1}$ .

Alternatively, one can prove a more general statement that an injective function  $F \rightarrow F$ , where  $F$  is finite, is also automatically surjective.

( $\Rightarrow$ ) Suppose that  $(k, p-1) = d > 1$ . Then note  $g$  is not in the image of  $f_k$ ; if it were, say  $g = f_k(g^{e(n)}) \equiv g^{e(n)k} \pmod{p}$ , then  $1 \equiv e(n)k \pmod{p-1}$ , which implies that  $(k, p-1) = 1$ , a contradiction. Thus,  $f_k$  is not surjective. ■

## 6 Problem 6

### Problem (Problem 6(1))

In the following,  $p$  denotes an odd prime number. Explain your reasoning clearly.

(1) Prove that the congruence

$$(x^2 + 1)(x^2 - 5)(x^2 + 5) \equiv 0 \pmod{p}$$

has a solution for every prime  $p$ .

*Proof.* Let  $p$  be an odd prime. If  $\left(\frac{-1}{p}\right) = 1$  or  $\left(\frac{-5}{p}\right) = 1$ , then we are done since that implies that  $-1$  or  $-5$  is a quadratic residue modulo  $p$ , or equivalently  $x^2 + 1 \equiv 0 \pmod{p}$  or  $x^2 + 5 \equiv 0 \pmod{p}$  has solutions. Otherwise,

$$\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-5}{p}\right) = (-1) \cdot (-1) = 1,$$

so 5 is a quadratic residue modulo  $p$ , or equivalently  $x^2 - 5 \equiv 0 \pmod{p}$  has a solution. ■

### Problem (Problem 6(2))

In the following,  $p$  denotes an odd prime number. Explain your reasoning clearly.

(2) For which primes  $p$  is  $-5$  a square modulo  $p$ ?

*Solution.* The primes are of the form

$$p \equiv 1, 3, 7, 9 \pmod{20}.$$

Since  $5 \equiv 1 \pmod{4}$  is a prime, we obtain by quadratic reciprocity that

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right).$$

We have

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}, \end{cases} \quad \text{and} \quad \left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{5}, \\ -1 & \text{if } p \equiv \pm 2 \pmod{5}. \end{cases}$$

- In the first case, we use the Chinese remainder theorem on

$$p \equiv 1 \pmod{4} \quad \text{and} \quad p \equiv b \pmod{5},$$

for  $b = \pm 1$ , giving  $p \equiv 1, 9 \pmod{20}$ .

- In the second case, we use the Chinese remainder theorem on

$$p \equiv -1 \pmod{4} \quad \text{and} \quad p \equiv b \pmod{5},$$

for  $b = \pm 2$ , giving  $p \equiv 3, 7 \pmod{20}$ .

This finishes the classification. ■

## 7 Bonus

### Problem (Bonus)

Let  $p$  be an odd prime. If  $0 < h < p$ ,  $n = hp + 1$ , and

$$\begin{aligned} 2^h &\not\equiv 1 \pmod{n}, \\ 2^{n-1} &\equiv 1 \pmod{n}, \end{aligned}$$

then  $n$  is prime.

*Proof.* Let  $Q$  be the set of primes that divide  $n$ . Suppose that  $n$  has prime factorization

$$n = \prod_{q \in Q} q^{\alpha(q)}.$$

Let  $d$  denote the order of  $2 \pmod{n}$ . Since  $2^{n-1} \equiv 1 \pmod{n}$ , we have  $d \mid (n-1)$ . On the other hand,  $d \nmid h$ ; otherwise, if  $d \mid h$ , say  $dg = h$  for some  $g \in \mathbb{Z}$ , then

$$2^h \equiv 2^{dg} \pmod{n} \equiv (2^d)^g \pmod{n} \equiv 1^g \pmod{n} \equiv 1 \pmod{n},$$

contrary to  $2^h \not\equiv 1 \pmod{n}$ . Thus

- $d \nmid h$  and
- $d \mid (n-1) = hp$ ,

which implies  $d \mid p$ . In particular,  $d \neq 1$  since  $2 \not\equiv 1 \pmod{n}$  for  $n$  composite, so  $d = p$ . Furthermore,  $d \mid \phi(n)$  (since the order always divides  $\phi(n)$ ), so  $p \mid \phi(n)$ . Recall that

$$\phi(n) = \prod_{q \in Q} q^{\alpha(q)-1}(q-1).$$

Now  $p \notin Q$  because  $p \nmid n$  (since  $n \equiv 1 \pmod{p}$ ). But also  $p \mid \phi(n)$ , so  $p \mid (q-1)$  for some prime  $q \in Q$ . In particular,  $q = pk + 1$  for some  $k \in \mathbb{N}$ . Moreover, write  $qt = n$  for some  $t \in \mathbb{N}$ . Then  $hp + 1 = n = qt = (pk + 1)t$ , or

$$(h - kt)p = t - 1. \tag{1}$$

- Since  $h < p$  (i.e.,  $h \leq p - 1$ ) by assumption, we have  $n = hp + 1 \leq (p - 1)p + 1 = p^2 - p + 1 < p^2$ .
- Then we must have  $t < p$ ; otherwise, if  $t \geq p$ , then  $n = (pk + 1)t \geq (pk + 1)p \geq p^2$ , contrary to  $n < p^2$ .

Since  $t \in \{1, \dots, p - 1\}$ , we have  $t - 1 \in \{0, \dots, p - 2\}$ . But (1) implies that  $p \mid (t - 1)$ , so  $t - 1 = 0$ . Thus  $t = 1$ , and we obtain  $n = qt = q$ , so  $n$  is prime. ■