

18.781 Theory of Numbers

Quiz 1

Official Solutions

March 5, 2026

Contents

1	Problem 1	2
2	Problem 2	4
3	Problem 3	5
4	Problem 4	6
5	Bonus	8

Disclaimer

This document contains the official solutions to Quiz 1 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 Problem 1

Problem (Problem 1(1))

There are 4 problems in this set. Do now just write down solutions. **Explain your reasoning carefully!**

(1) Find the last 2 digits of 27^{81} .

Solution. The last 2 digits of 27^{81} is

27.

This is equivalent to computing $27^{81} \pmod{100}$. Note $\phi(100) = \phi(2^2) \phi(5^2) = (4-2)(25-5) = 40$. Since $(27, 100) = 1$, Euler's theorem applies and we obtain

$$27^{40} = 27^{\phi(100)} \equiv 1 \pmod{100}.$$

Therefore,

$$27^{81} = 27^{40} \cdot 27^{40} \cdot 27 \equiv 1 \cdot 1 \cdot 27 \pmod{100} = 27 \pmod{100},$$

as required. ■

Problem (Problem 1(2))

There are 4 problems in this set. Do now just write down solutions. **Explain your reasoning carefully!**

(2) Find all possible pairs of positive integers m and n so that $(m, n) = 6$ and $[m, n] = 60$.

Solution. The only possible pairs are

$$(m, n) \in \{(6, 60), (12, 30), (30, 12), (60, 6)\}.$$

Note that

$$mn = |mn| = (m, n)[m, n] = 6 \cdot 60 = 360.$$

Write $m = 6x$ and $n = 6y$ for some $x, y \in \mathbb{Z}$. Now $(x, y) = 1$, so the above equation becomes

$$36xy = mn = 360,$$

or $xy = 10$. Therefore, $(x, y) \in \{(1, 10), (2, 5), (5, 2), (10, 1)\}$, which gives the result. ■

Problem (Problem 1(3))

There are 4 problems in this set. Do now just write down solutions. **Explain your reasoning carefully!**

(3) Find all integer solutions x, y, a, b satisfying

$$x^2 + 9y^2 = 23 \cdot (4a^2 + b^2).$$

Solution. The only solution is

$$(x, y, a, b) = (0, 0, 0, 0).$$

Besides this *trivial solution*, we show that there are no other *nontrivial solutions*. Suppose there is another solution $(x, y, a, b) \neq (0, 0, 0, 0)$. Rewrite

$$x^2 + (3y)^2 = 23 \cdot (4a^2 + b^2) = 23 \cdot ((2a)^2 + b^2).$$

The left hand $N := x^2 + (3y)^2$ is a sum of squares, so the primes $p \equiv 3 \pmod{4}$ appearing in the prime factorization of N have even exponents. By the same argument, the primes $p \equiv 3 \pmod{4}$ appearing in the prime factorization of $M = (2a)^2 + b^2$ have even exponents. But $23M$ has a prime factor $p \equiv 3 \pmod{4}$ that has an odd exponent (since $23 \equiv 3 \pmod{4}$), and since $N = 23M$, N does as well, a contradiction. ■

Problem (Problem 1(4))

There are 4 problems in this set. Do now just write down solutions. **Explain your reasoning carefully!**

(4) Determine whether the following system has a solution:

$$7X + 2Y \equiv 7 \pmod{9},$$

$$7X + 2Y \equiv 8 \pmod{10}.$$

Solution. Let $Z = 7X + 2Y$. Since $(9, 10) = 1$, the Chinese remainder theorem gives a solution $Z \equiv c \pmod{90}$, where $0 \leq c < 90$. Now $(7, 2) = 1$, so there exists integers $a, b \in \mathbb{Z}$ such that $7a + 2b = 1$. Then

$$7(ac) + 2(bc) = c,$$

so $X = ac$ and $Y = bc$ is a solution. ■

2 Problem 2

Problem (Problem 2(1))

Here is a set of 3 simple proof questions.

(1) Let $a, m, n \in \mathbb{Z}$. Suppose that $(m, a) = 1 = (n, a)$. Prove that $(mn, a) = 1$.

Proof. Since $(m, a) = 1 = (n, a)$, there exists $x, y, w, z \in \mathbb{Z}$ such that

$$1 = mx + ay,$$

$$1 = nw + az.$$

Then

$$1 = (mx + ay)(nw + az) = mn(xy) + (nwy + mxz + ayz)a$$

is an integer linear combination of mn and a , so $(mn, a) = 1$. ■

Problem (Problem 2(2))

Here is a set of 3 simple proof questions.

(2) Let p be an odd prime and $a \in \mathbb{N}$ with $p \nmid a$. Prove that if $x^2 \equiv a \pmod{p}$ has a solution, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Proof. Suppose $x \in \mathbb{Z}$ solves $x^2 \equiv a \pmod{p}$. Since $p \nmid a$, then $p \nmid x^2$, which implies $p \nmid x$ (i.e., $(x, p) = 1$). Then

$$\begin{aligned} a^{(p-1)/2} &\equiv (x^2)^{(p-1)/2} \pmod{p} \\ &\equiv x^{p-1} \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

by Fermat's little theorem. ■

Problem (Problem 2(3))

Here is a set of 3 simple proof questions.

(3) Let $n \in \mathbb{Z}$ with $n > 4$. Prove that if $(n-1)! + 1 \equiv 0 \pmod{n}$, then n is prime.

Proof. We prove by contrapositive. Suppose n is composite, and say $n = ab$ for some integers $1 < a \leq b < n$.

- If $a < b$, then a and b both appear individually in the expansion $(n-1)!$. Thus $n = ab \mid (n-1)!$, so $(n-1)! \equiv n \equiv 0 \pmod{n}$.
- If $a = b$, i.e., $a^2 = n > 4$, then $a > 2$ and $n = a^2 > 2a$. Thus a and $2a$ both appear individually in the expansion $(n-1)!$, so $2n^2 = 2a^2 = a \cdot 2a \mid (n-1)!$. Hence $(n-1)! \equiv 2n^2 \equiv 0 \pmod{n}$.

The proof is complete. ■

3 Problem 3

Problem (Problem 3(1))

Determine whether there are solutions for the following congruence equations. If so, find the number of solutions (in complete residue system). There are 3 subproblems in this set.

$$(1) 14X \equiv 35 \pmod{91}$$

Solution. Since $(14, 91) = 7 \mid 35$, the congruence has a solution. Precisely, it has $(14, 91) = 7$ solutions. ■

Problem (Problem 3(2))

Determine whether there are solutions for the following congruence equations. If so, find the number of solutions (in complete residue system). There are 3 subproblems in this set.

$$(2) X^{13} - X \equiv 0 \pmod{105}$$

Solution. We have $105 = 3 \cdot 5 \cdot 7$, so we apply Chinese remainder theorem to obtain the system

$$X^{13} - X \equiv 0 \pmod{3},$$

$$X^{13} - X \equiv 0 \pmod{5},$$

$$X^{13} - X \equiv 0 \pmod{7}.$$

But any $x \in \{0, \dots, 104\}$ satisfies this system by Fermat's little theorem: for such a x ,

$$x^3 \equiv x \pmod{3}, \quad x^5 \equiv x \pmod{5}, \quad x^7 \equiv x \pmod{7},$$

which implies

$$x^{13} - x \equiv (x^3)^4 x - x \pmod{3} \equiv x - x \pmod{3} \equiv 0 \pmod{3},$$

$$x^{13} - x \equiv (x^5)^2 x^3 - x \pmod{5} \equiv x^5 - x \pmod{5} \equiv 0 \pmod{5},$$

$$x^{13} - x \equiv x^7 x^6 - x \pmod{7} \equiv x^7 - x \pmod{7} \equiv 0 \pmod{7},$$

so there are 105 solutions. ■

Problem (Problem 3(3))

Determine whether there are solutions for the following congruence equations. If so, find the number of solutions (in complete residue system). There are 3 subproblems in this set.

$$(3) X^{p-1} + \dots + X + 1 \equiv 0 \pmod{p}$$

Solution. Let $f(X) = X^{p-1} + \dots + X + 1$. Then $(X - 1)f(X) = X^p - 1$. Thus, any solution to $f(X) \equiv 0 \pmod{p}$ also satisfy $X^p - 1 \equiv 0 \pmod{p}$, i.e., $X^p \equiv 1 \pmod{p}$. Let x be a solution to $f(X) \equiv 0 \pmod{p}$. Then

$$x^p \equiv 1 \pmod{p}.$$

Fermat's little theorem implies $x^p \equiv x \pmod{p}$, which forces $x = 1$. Thus, there is only 1 solution. ■

4 Problem 4

Problem (Problem 4(1))

There are 3 problems in this set. In the following let p be an odd prime number.

(1) Prove that

$$(X + Y)^p \equiv X^p + Y^p \pmod{p}.$$

Proof. Recall that

$$\binom{p}{k} \equiv 0 \pmod{p}$$

for any integer $1 \leq k \leq p - 1$. The binomial theorem implies

$$\begin{aligned} (X + Y)^p &= \sum_{k=0}^p \binom{p}{k} X^k Y^{p-k} \\ &= X^p + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} X^k Y^{p-k}}_{\equiv 0 \pmod{p}} + Y^p \\ &\equiv X^p + Y^p \pmod{p}, \end{aligned}$$

as required. ■

Problem (Problem 4(2))

There are 3 problems in this set. In the following let p be an odd prime number.

(2) Let $k > 0$ and $m \in \mathbb{Z}$ such that $m \equiv 1 \pmod{p^k}$. Prove that

$$m^p \equiv 1 \pmod{p^{k+1}}.$$

Proof. By definition, there exists some integer n such that $np^k = m - 1$, i.e., $m = np^k + 1$. Then

$$\begin{aligned} m^p &= (np^k + 1)^p \\ &= \sum_{\ell=0}^p \binom{p}{\ell} (np^k)^\ell \\ &= 1 + \underbrace{p(np^k)}_{\equiv 0 \pmod{p^{k+1}}} + \underbrace{\sum_{\ell=2}^p \binom{p}{\ell} (np^k)^\ell}_{\equiv 0 \pmod{p^{k+1}}} \\ &\equiv 1 \pmod{p^{k+1}}, \end{aligned}$$

as required. ■

Problem (Problem 4(3))

There are 3 problems in this set. In the following let p be an odd prime number.

(3) Prove that

$$\binom{p(p-1)}{p} \equiv \binom{p-1}{1} \equiv -1 \pmod{p}.$$

(Hint: Expand $(X+1)^{p(p-1)} \pmod{p}$ in two ways and compare the coefficients of X^p .)

Proof. We follow the hint. On the one hand,

$$(X+1)^{p(p-1)} = \sum_{k=0}^{p(p-1)} \binom{p(p-1)}{k} X^k,$$

so the coefficient of X^p is $\binom{p(p-1)}{p}$. On the other hand, we use Problem 4(1) to write $(X+1)^p \equiv X^p + 1 \pmod{p}$. Then

$$\begin{aligned} ((X+1)^p)^{p-1} &\equiv (X^p + 1)^{p-1} \pmod{p} \\ &\equiv \sum_{k=0}^{p-1} \binom{p-1}{k} X^{pk} \pmod{p}, \end{aligned}$$

so the residue modulo p of the coefficient of X^p is $\binom{p-1}{1}$. Thus

$$\binom{p(p-1)}{p} \equiv \binom{p-1}{1} \equiv -1 \pmod{p},$$

as desired. ■

5 Bonus

Problem (Bonus-1)

Let $a \in \mathbb{N}$ and p be an odd prime. Prove the converse of Problem 2(2), that is, prove that if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, then $x^2 \equiv a \pmod{p}$ has exactly two solutions.

Proof. Suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Consider the set

$$R = \left\{ 1^2 a \pmod{p}, 2^2 a \pmod{p}, \dots, \left(\frac{p-1}{2} \right)^2 a \pmod{p} \right\}.$$

Their product is

$$\prod_{k=1}^{(p-1)/2} k^2 a \equiv a^{(p-1)/2} \prod_{k=1}^{(p-1)/2} k^2 \pmod{p} \equiv \prod_{k=1}^{(p-1)/2} k^2 \pmod{p}. \quad (1)$$

We show that that if $ai^2 \equiv aj^2 \pmod{p}$ for any $1 \leq i, j \leq (p-1)/2$, then $i = j$. If this holds, then $(a, p) = 1$, so $i^2 \equiv j^2 \pmod{p}$. In other words, $p \mid (i-j)(i+j)$, so $p \mid (i-j)$ or $p \mid (i+j)$. But

$$2 \leq i+j \leq p-1,$$

so we cannot have $p \mid (i+j)$; hence $p \mid (i-j)$, and since

$$1 - (p-1)/2 \leq i-j \leq (p-1)/2 - 1$$

we must have $i-j = 0$, so $i = j$. This implies that the elements of R are all distinct. Moreover,

$$\ell^2 \equiv (p-\ell)^2 \pmod{p}, \quad (2)$$

for all $\ell \in \{1, 2, \dots, (p-1)/2\}$, so

$$S = \{1^2, 2^2, \dots, ((p-1)/2)^2\}$$

is the set of all squares modulo p . The product of all $(p-1)/2$ distinct elements in R and S are the same modulo p , so the elements of R are also squares modulo p ; otherwise, the product (1) would not be a square modulo p , a contradiction. Therefore, R is just a permutation of S , so there exists some $i \in \{1, \dots, (p-1)/2\}$ such that

$$i^2 \equiv 1^2 a \pmod{p} \equiv a \pmod{p}.$$

Then (2) implies that $p-i$ is also such a solution, so $x = i$ and $x = p-i$ solve $x^2 \equiv a \pmod{p}$. There are no other solutions as they are all distinct, so there are exactly 2 solutions. ■

Problem (Bonus-2)

Let m and n be non-negative integers with $m > n$. Write

$$\begin{aligned} m &= m_r p^r + m_{r-1} p^{r-1} + \cdots + m_0, \\ n &= n_r p^r + n_{r-1} p^{r-1} + \cdots + n_0, \end{aligned}$$

where $0 \leq m_i, n_i \leq p-1$. Prove that

$$\binom{m}{n} \equiv \prod_{i=0}^r \binom{m_i}{n_i} \pmod{p}.$$

Proof. This result is known as *Lucas's theorem*. Here we use the convention that $\binom{m}{n} = 0$ if $m < n$.

We first make the following claim.

Lemma 1

For every integer $i \geq 1$,

$$(X+1)^{p^i} \equiv X^{p^i} + 1 \pmod{p}.$$

Proof of Lemma 1. We proceed by induction. The base case $i = 1$ follows from Problem 4(1). Now assume that the proposition holds for some integer $i = \ell$, i.e., $(X+1)^{p^\ell} \equiv X^{p^\ell} + 1 \pmod{p}$. Then

$$(X+1)^{p^{\ell+1}} = \left((X+1)^{p^\ell}\right)^p \equiv \left(X^{p^\ell} + 1\right)^p \pmod{p} \equiv X^{p^{\ell+1}} + 1 \pmod{p},$$

which completes the induction step. ■

Then the binomial theorem gives

$$\begin{aligned} \sum_{n=0}^m \binom{m}{n} X^n &= (X+1)^m \\ &= \prod_{i=0}^r \left((X+1)^{p^i}\right)^{m_i} \\ &\equiv \prod_{i=0}^r \left(X^{p^i} + 1\right)^{m_i} \pmod{p} \\ &\equiv \prod_{i=0}^r \sum_{k=0}^{m_i} \binom{m_i}{k} X^{kp^i} \pmod{p} \\ &\equiv \sum_{n=0}^m \prod_{i=0}^r \binom{m_i}{n_i} X^n \pmod{p}. \end{aligned}$$

Comparing the coefficients modulo p gives

$$\binom{m}{n} \equiv \prod_{i=0}^r \binom{m_i}{n_i} \pmod{p},$$

as required. ■