

18.781 Theory of Numbers

Quiz 3

Official Solutions

May 7, 2026

Contents

1	Problem 1	2
2	Problem 2	3
3	Problem 3	4
4	Problem 4	5
5	Problem 5	7
6	Problem 6	8

Disclaimer

This document contains the official solutions to Quiz 3 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))

State each of the following clearly.

- (1) Möbius inversion formula

Solution. If $F(n) = \sum_{d|n} f(d)$ for every positive integer n , then $f(n) = \sum_{d|n} \mu(d)F(n/d)$. ■

Problem (Problem 1(2))

State each of the following clearly.

- (2) Hasse-Minkowski's principle for linear systems

Solution. Let A be a $m \times n$ matrix over $\mathbb{Z}$ and let $b \in \mathbb{Z}^m$. Then the system $Ax = b$ has a solution $x \in \mathbb{Z}^n$ if and only if it has a solution modulo m for every positive integer m . ■

2 Problem 2

Problem (Problem 2(1))

Let $f(x, y) = x^2 + xy + y^2$ be a binary quadratic form.

(1) Show that any positive definite binary quadratic form of discriminant -3 is equivalent to $f(x, y)$.

Proof. Note that $f(x, y)$ is reduced; if we put $a' = 1$, $b' = 1$, and $c' = 1$, then $0 \leq b' \leq |a'| = |c'|$. Moreover, $f(x, y)$ is positive definite since $a' > 0$ and its discriminant is negative. Hence we show that $f(x, y)$ is the only reduced binary quadratic form of discriminant -3 . Let $g(x, y) = ax^2 + bxy + cy^2$ be a positive definite reduced binary quadratic form of discriminant $d = b^2 - 4ac = -3$. Therefore, a is some integer such that

$$0 < a \leq \sqrt{-d/3} = 1,$$

so $a = 1$. Since g is reduced, we have $-|a| < b \leq |a| < c$ or $0 \leq b \leq |a| = |c|$. In either case $b = 0$ or $b = 1$.

- We cannot have $b = 0$ since no integer c satisfies $-3 = d = b^2 - 4ac = -4c$.
- Hence $b = 1$, which forces $-3 = d = b^2 - 4ac = 1 - 4c$, so $c = 1$.

Therefore, $g(x, y) = f(x, y)$, so any positive definite quadratic form of discriminant -3 is equivalent to $f(x, y)$. ■

Problem (Problem 2(2))

Let $f(x, y) = x^2 + xy + y^2$ be a binary quadratic form.

(2) Determine whether 2003 can be represented by $f(x, y)$ properly. Note that 2003 is a prime.

Proof. Note that $d = -3$ satisfies $d \equiv 1 \pmod{4}$, and $p = 2003$ is an odd prime. Moreover, recall that there exists a binary quadratic form of discriminant d that properly represents p if and only if $\left(\frac{d}{p}\right) = 1$. Since all positive definite binary quadratic forms of discriminant -3 are equivalent to $f(x, y)$, we compute by quadratic reciprocity that

$$\begin{aligned} \left(\frac{-3}{2003}\right) &= \left(\frac{-1}{2003}\right) \left(\frac{3}{2003}\right) \\ &= (-1)^{(2003-1)/2} \left(\frac{2003}{3}\right) (-1)^{(2003-1)(3-1)/4} \\ &= \left(\frac{2}{3}\right) \\ &= -1 \end{aligned}$$

since 2 is not a quadratic residue modulo 3. Thus, 2003 is not properly represented by $f(x, y)$. ■

3 Problem 3

Problem (Problem 3(1))

There are two problems in this set.

(1) Prove that

$$\frac{2+\sqrt{3}}{2\sqrt{3}}(1+\sqrt{3})^n + \frac{\sqrt{3}-2}{2\sqrt{3}}(1-\sqrt{3})^n$$

is an integer for any $n \geq 0$.

Proof. Put $a = (1+\sqrt{3}) + (1-\sqrt{3}) = 2$ and $b = -(1+\sqrt{3})(1-\sqrt{3}) = 2$ and note that $1+\sqrt{3}$ and $1-\sqrt{3}$ are roots of $Q(z) = z^2 - az - b = z^2 - 2z - 2$. Then the sequence f_n (for any integer $n \geq 0$) given by

$$f_n := \frac{2+\sqrt{3}}{2\sqrt{3}}(1+\sqrt{3})^n + \frac{\sqrt{3}-2}{2\sqrt{3}}(1-\sqrt{3})^n$$

satisfies the recurrence $f_{n+2} = af_{n+1} + bf_n = 2f_{n+1} + 2f_n$ (for any integer $n \geq 0$). Thus, we need only show that f_0 and f_1 are integers, since then the recurrence relation implies that f_n is an integer for all integers $n \geq 2$. Hence

$$\begin{aligned} f_0 &= \frac{2+\sqrt{3}}{2\sqrt{3}}(1+\sqrt{3})^0 + \frac{\sqrt{3}-2}{2\sqrt{3}}(1-\sqrt{3})^0 = 1, \\ f_1 &= \frac{2+\sqrt{3}}{2\sqrt{3}}(1+\sqrt{3})^1 + \frac{\sqrt{3}-2}{2\sqrt{3}}(1-\sqrt{3})^1 = 3, \end{aligned}$$

and we conclude the proof. ■

Problem (Problem 3(2))

There are two problems in this set.

(2) Find the solution of the recurrence function with $f_0 = 3$, $f_1 = -4$, and

$$f_{n+2} = 4f_{n+1} - 4f_n.$$

Solution. The solution (for integers $n \geq 0$) is

$$f_n = 3 \cdot 2^n - 5n \cdot 2^n.$$

Put $a = 4$ and $b = -4$. Note $\lambda = 2$ is a root of the polynomial $Q(z) = z^2 - az - b = z^2 - 4z + 4$. Take $\alpha = f_0 = 3$ and $\beta = f_1/2 - f_0 = -5$ such that $\lambda\alpha + \lambda\beta = f_1$. Then $f_{n+2} = 4f_{n+1} - 4f_n = af_{n+1} - bf_n$, $f_0 = 3$, and $f_1 = -4$ satisfies

$$f_n = \alpha\lambda^n + \beta n\lambda^n = 3 \cdot 2^n - 5n \cdot 2^n$$

for integers $n \geq 0$. ■

4 Problem 4

Problem (Problem 4(1))

Solve the following:

$$(1) \ 9x^2 - 6x \equiv 16 \pmod{77}.$$

Solution. There are

no solutions.

By the Chinese remainder theorem we solve the simultaneous congruences

$$9x^2 - 6x \equiv 16 \pmod{7},$$

$$9x^2 - 6x \equiv 16 \pmod{11}.$$

But the former congruence is $2x^2 + x \equiv 2 \pmod{7}$, which becomes $(x+2)^2 \equiv x^2 + 4x + 4 \pmod{7} \equiv 5 \pmod{7}$ after multiplying by 4 and adding 4. Making the change of variables $y = x + 2$, we solve $y^2 \equiv 5 \pmod{7}$. But

$$\left(\frac{5}{7}\right) \equiv 5^{(7-1)/2} \pmod{7} \equiv 125 \pmod{7} \equiv -1 \pmod{7},$$

so 5 is not a quadratic residue modulo 7. Hence, $y^2 \equiv 5 \pmod{7}$ has no solution y , hence no solution x to the former congruence and thus no solution x to the original congruence. ■

Problem (Problem 4(2))

Solve the following:

$$(2) \ x^5 + y^5 + z^5 = w^{10} + 37.$$

Solution. There are

no solutions.

If there is some solution $(x, y, z, w) \in \mathbb{Z}^4$, then it also satisfies the relation $x^5 + y^5 + z^5 \equiv w^{10} + 37 \pmod{11}$. Hence $w^{10} \pmod{11}$ is either 0 or 1 by Fermat's little theorem, so $w^{10} + 37 \pmod{11}$ is thus either 4 or 5. On the other hand, the terms x^5 , y^5 and z^5 are either 0 mod 11, 1 mod 11, or $-1 \pmod{11}$, so $x^5 + y^5 + z^5 \pmod{11}$ belongs in the set $\{0, \pm 1, \pm 2, \pm 3\} \neq \{4, 5\}$, a contradiction. ■

Problem (Problem 4(Bonus))

Solve the following:

$$(3) \quad X^{11} + 3 \equiv Y^6 \pmod{13}.$$

Solution. The solutions are

$$\begin{aligned} (X, Y) &= (4, 0), \\ (X, Y) &= (3, 2), (3, 5), (3, 6), (3, 7), (3, 8), (3, 11), \\ (X, Y) &= (6, 1), (6, 3), (6, 4), (6, 9), (6, 10), (6, 12). \end{aligned}$$

By Fermat's little theorem, $Y^{12} \pmod{13}$ is either 0 or 1, so $Y^6 \pmod{13}$ is either 0, 1, or -1 . Hence $X \not\equiv 0 \pmod{13}$ as otherwise the congruence $X^{11} + 3 \equiv Y^6 \pmod{13}$ implies that $3 \equiv 0, \pm 1 \pmod{13}$, a contradiction. Since $X \not\equiv 0 \pmod{13}$, Fermat's little theorem implies $X^{12} \equiv 1 \pmod{13}$, so $X^{11} \equiv X^{-1} \pmod{13}$ and we solve for

$$\begin{aligned} X^{-1} + 3 &\equiv 0 \pmod{13}, \\ X^{-1} + 3 &\equiv 1 \pmod{13}, \\ X^{-1} + 3 &\equiv -1 \pmod{13}. \end{aligned}$$

For convenience, we first show that 2 is a primitive root modulo 13. The order of 2 modulo 13 divides $\phi(13) = 12$ by Fermat's little theorem, so the possible orders are 1, 2, 3, 4, 6, and 12; all but the last hold since

$$\begin{aligned} 2^1 &\equiv 2 \pmod{13}, & 2^2 &\equiv 4 \pmod{13}, \\ 2^3 &\equiv 8 \pmod{13}, & 2^4 &\equiv 16 \pmod{13} \\ 2^6 &\equiv 12 \pmod{13}, & 2^{12} &\equiv 1 \pmod{13}. \end{aligned}$$

- The first congruence (when $Y^6 \equiv 0 \pmod{13}$) is $X^{-1} \equiv -3 \pmod{13} \equiv 10 \pmod{13}$, i.e., $10X \equiv 1 \pmod{13}$. The Euclidean algorithm gives $X = 4$. Now $Y^6 \equiv 0 \pmod{13}$ only when $Y \equiv 0 \pmod{13}$, so $(X, Y) = (4, 0)$.
- The second (when $Y^6 \equiv 1 \pmod{13}$) is that $X^{-1} \equiv -2 \pmod{13} \equiv 11 \pmod{13}$, i.e., $11X \equiv 1 \pmod{13}$. The Euclidean algorithm gives $X = 6$. We write $Y = 2^k$ for some $k \in \mathbb{Z}$ (since 2 is a primitive root modulo 13), and this gives $2^{6k} \equiv 1 \pmod{13}$. Thus $6k \equiv 0 \pmod{\phi(13)} \equiv 0 \pmod{12}$, which holds only for k even. Thus

$$Y \in \{2^0 \pmod{13}, 2^2 \pmod{13}, 2^4 \pmod{13}, 2^6 \pmod{13}, 2^8 \pmod{13}, 2^{10} \pmod{13}\} = \{1, 3, 4, 9, 10, 12\}.$$

- The third (when $Y^6 \equiv -1 \pmod{13}$) is that $X^{-1} \equiv -4 \pmod{13} \equiv 9 \pmod{13}$, i.e., $9X \equiv 1 \pmod{13}$. The Euclidean algorithm gives $X = 3$. We write $Y = 2^k$ for some $k \in \mathbb{Z}$ (since 2 is a primitive root modulo 13), and this gives $2^{6k} \equiv -1 \pmod{13}$. Thus $6k \equiv 0 \pmod{\phi(13)} \equiv 6 \pmod{12}$, which holds only for k odd. Thus

$$Y \in \{2^1 \pmod{13}, 2^3 \pmod{13}, 2^5 \pmod{13}, 2^7 \pmod{13}, 2^9 \pmod{13}, 2^{11} \pmod{13}\} = \{2, 5, 6, 7, 8, 11\}.$$

The solution is complete. ■

5 Problem 5

Problem (Problem 5(1))

There are two problems in this set.

- (1) Find all the integral solutions of the following linear system:

$$x + 2y + 3z = 5,$$

$$2x + 3y + z = 0,$$

$$x + y - 2z = -5.$$

Solution. The solutions are given by

$$(x, y, z) = (7t - 15, 10 - 5t, t) \text{ for } t \in \mathbb{Z}.$$

To see this, note that

$$y + 5z = \text{first equation} - \text{third equation} = 5 - (-5) = 10,$$

so $y = 10 - 5z$. The second equation gives $0 = 2x + 3y + z = 2x + 3(10 - 5z) + z = 2x - 14z + 30$, or equivalently $x = 7z - 15$. Substituting this in the third equation shows consistency, so the system has one free parameter. If we parametrize $z = t$ over $t \in \mathbb{Z}$, then $(x, y, z) = (7t - 15, 10 - 5t, t)$ are solutions. ■

Problem (Problem 5(2))

There are two problems in this set.

- (2) Determine for what integers a , b , and c , the following system of equations has a solution in integers:

$$x + 2y + 3z = a,$$

$$2x + 3y + z = b,$$

$$x + y - 2z = c.$$

Solution. The system has a solution if and only if

$$a - b + c = 0 \text{ for } a, b, c \in \mathbb{Z}.$$

We show that this condition is necessary and sufficient. For necessity, note that

$$0 = \text{first equation} - \text{second equation} + \text{third equation} = a - b + c.$$

For sufficiency, suppose $a - b + c = 0$ for integers a , b , and c . Then

$$y + 5z = \text{first equation} - \text{third equation} = a - c,$$

so $y = a - c - 5z$. The second equation gives $b = 2x + 3y + z = 2x + 3(a - c - 5z) + z = 2x - 14z + 3a - 3c$, or equivalently $x = 2a - c + 7z$ after simplification (using the fact that $b = a + c$). If we parametrize $z = t$ over $t \in \mathbb{Z}$, then $(x, y, z) = (2a - c + 7t, a - c - 5t, t)$ over $t \in \mathbb{Z}$ are solutions. ■

6 Problem 6

Problem (Problem 6(1))

There are two problems in this set.

(1) Prove that if f and g are multiplicative, then

$$F(n) := \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

is multiplicative.

Proof. Let n and m be relatively prime integers. Every divisor d of mn is expressible as $d = ab$, where $a | m$ and $b | n$. Since n and m are relatively prime, $(a, b) = 1$ and $(m/a, n/b) = 1$, and this correspondence is one-to-one. Hence

$$F(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{\substack{a|m \\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) = \sum_{\substack{a|m \\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) = F(m)F(n),$$

as required. Since f and g are multiplicative, we have $f(ab) = f(a)f(b)$ and $g(mn/ab) = g(m/a)g(n/b)$ above. ■

Problem (Problem 6(2))

There are two problems in this set.

(2) Find an explicit formula for $f(n)$ so that

$$(-1)^{\omega(n)} = \sum_{d|n} f(d).$$

Proof. Write $F(n) = (-1)^{\omega(n)}$, where $\omega(n)$ denotes the number of distinct primes dividing n . We have

$$f(n) = \sum_{d|n} \mu(d)F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)(-1)^{\omega(n/d)}$$

by the Möbius inversion formula. Note that $F(n)$ is multiplicative, as is $\mu(n)$, so $f(n)$ is multiplicative by the previous part. Thus we need only compute $f(n)$ at prime powers p^k , which is

$$\begin{aligned} f(p^k) &= \sum_{d|p^k} \mu(d)(-1)^{\omega(p^k/d)} = \sum_{i=0}^k \mu(p^i)(-1)^{\omega(p^{k-i})} = \mu(0)(-1)^{\omega(p^k)} + \mu(p)(-1)^{\omega(p^{k-1})} = 0 \quad \text{for } k \geq 2, \\ f(p) &= \sum_{d|p} \mu(d)(-1)^{\omega(p/d)} = \sum_{i=0}^1 \mu(p^i)(-1)^{\omega(p^{1-i})} = \mu(0)(-1)^{\omega(p)} + \mu(p)(-1)^{\omega(1)} = -2, \end{aligned}$$

using the fact that $\mu(p^i) = 0$ for integers $i \geq 2$ and $\omega(p^i) = p$ for any integer $i \geq 1$. Thus if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k}) = \begin{cases} f(p_1) \cdots f(p_k) & \text{if } \alpha_1 = \cdots = \alpha_k = 1, \\ 0 & \text{otherwise,} \end{cases} = \begin{cases} (-2)^{\omega(n)} & \text{if } n \text{ is squarefree,} \\ 0 & \text{otherwise,} \end{cases}$$

where $\omega(n) = k$. Hence, $f(n) = |\mu(n)|(-2)^{\omega(n)} = \mu(n)(-1)^{\omega(n)}(-2)^{\omega(n)} = \mu(n)2^{\omega(n)}$, where $|\mu(n)| = (-1)^{\omega(n)}\mu(n)$ is the indicator function for n squarefree. But since $d(n) = 2^{\omega(n)}$, so $f(n) = \mu(n)2^{\omega(n)} = \mu(n)d(n)$. ■

Problem (Problem 6(Bonus))

This is a bonus problem.

(3) Define

$$F(n) := \begin{cases} 1 & \text{if } n \text{ is a square number,} \\ 0 & \text{otherwise.} \end{cases}$$

Find an explicit formula for $f(n)$ so that $F(n) = \sum_{d|n} f(d)$.

Proof. First we show $F(n)$ is multiplicative. Let n and m be relatively prime integers. If at least one of m or n is not a square, then mn is not as well, and hence $F(mn) = 0 = F(m)F(n)$. Conversely, if m and n are squares, then mn is a square as well, and hence $F(mn) = 1 = F(m)F(n)$.

By the Möbius inversion formula, we have

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right),$$

and $f(n)$ is multiplicative since both $\mu(n)$ and $F(n)$ are. Thus we need only compute $f(n)$ at prime powers p^k , so

$$f(p^k) = \sum_{d|p^k} \mu(d) F\left(\frac{p^k}{d}\right) = \sum_{i=0}^k \mu(p^i) F(p^{k-i}) = \mu(0)F(p^k) + \mu(p)F(p^{k-1}) = \begin{cases} 1 & \text{if } k \text{ is even,} \\ -1 & \text{otherwise,} \end{cases} = (-1)^k.$$

Here we use the fact that $\mu(p^i) = 0$ for integers $i \geq 2$. Thus if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k}) = (-1)^{\alpha_1 + \cdots + \alpha_k} = (-1)^{\Omega(n)},$$

where $\Omega(n)$ denotes the number of primes dividing n , counting multiplicity. ■