18.781 Theory of Numbers

Problem Set 7

Official Solutions

April 19, 2026

Contents

Disclaimer

This document contains the official solutions to Problem Set 7 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 §3.4 #3

Problem (§3.4 #3)

If $\mathscr{C}$ is any class of integers, finite or infinite, let $m\mathscr{C}$ denote the class obtained by multiplying each integer of $\mathscr{C}$ by the integer m. Prove that if $\mathscr{C}$ is the class of integers represented by any form f, then $m\mathscr{C}$ is the class represented by mf.

Proof. Suppose that $\mathscr{C}$ is the class of integers represented by a form $f \in \mathbb{Z}[X_1, \ldots, X_n]$.[1] To show the claim, we show

- every element of $m\mathscr{C}$ is represented by mf, and
- any element represented by mf is an element of $m\mathscr{C}$.

For the first item, let $c' \in m\mathscr{C}$. Then $c' = mc$ for some $c \in \mathscr{C}$. By assumption, there exist integers $x_1, \ldots, x_n$ such that $f(x_1, \ldots, x_n) = c$. Then $mf(x_1, \ldots, x_n) = mc = c'$, so c' is represented by mf. Conversely, for the second item, let c' be represented by mf. By definition, there exist integers $x_1, \ldots, x_n$ such that $c' = mf(x_1, \ldots, x_n)$. However, note that $f(x_1, \ldots, x_n) \in \mathscr{C}$ by definition, so $c' \in m\mathscr{C}$. ■

[1] This notation just means that f is a polynomial in variables $X_1, \ldots, X_n$ with integral coefficients.

2 §3.4 #6

Problem (§3.4 #6)
Let d be a perfect square, possibly 0. Show that there is a quadratic form $ax^2 + bxy + cy^2$ of discriminant d for which $a = 0$.

Proof. Since d is a perfect square, there exists some $b \in \mathbb{Z}$ such that $d = b^2$. Then any form $f(x, y) = bxy + cy^2$ has $a = 0$ and has discriminant $b^2 - 4ac = b^2 = d$. ■

3 §3.4 #7

Problem (§3.4 #7)
Let a, b, and c be integers with $a \neq 0$. Show that if one root of the equation $au^2 + bu + c = 0$ is rational then the other one is, and that $b^2 - 4ac$ is a perfect square, possibly 0. Show also that if $b^2 - 4ac$ is a perfect square, possibly 0, then the roots of the equation $au^2 + bu + c = 0$ are rational.

Proof. Since $a \neq 0$, the roots of $au^2 + bu + c = 0$ are precisely the roots of $u^2 + bu/a + c/u = 0$. Let r_1 and r_2 be the two roots of $u^2 + bu/a + c/a = 0$, so $u^2 + bu/a + c/a = (u - r_1)(u - r_2) = u^2 - (r_1 + r_2)u + r_1 r_2$. This implies

$$-\frac{b}{a} = r_1 + r_2 \quad \text{and} \quad \frac{c}{a} = r_1 r_2.$$

In particular, if r_1 is rational, then $r_2 = -b/a - r_1$ is rational as well. Moreover, $b = -(r_1 + r_2)a$ and $c = ar_1 r_2$, so

$$b^2 - 4ac = (-(r_1 + r_2)a)^2 - 4a^2 r_1 r_2 = a^2\left(r_1^2 - 2r_1 r_2 + r_2^2\right) = (a(r_1 - r_2))^2$$

is a rational perfect square since both r_1 and r_2 are rational. But $b^2 - 4ac$ is an integer since a, b, and c are integers, so $a(r_1 - r_2)$ must be an integer as well. This implies that $b^2 - 4ac$ is a perfect square.

Conversely, suppose $b^2 - 4ac$ is a perfect square, say k^2 for some $k \in \mathbb{Z}$. Then the above calculation shows that $(a(r_2 - r_1))^2 = (a(r_1 - r_2))^2 = b^2 - 4ac = k^2$, so

$$a(r_2 - r_1) = \pm k.$$

But recall that we also have

$$a(r_1 + r_2) = -b,$$

so adding the two equations give $2ar_2 = -b \pm k$, which implies that $r_2 = (-b \pm k)/2a$. Therefore, r_1 is rational. Then $r_2 = -b/a - r_1$ is rational as well. ∎

4 §3.4 #8

Problem (§3.4 #8)

Show that the discriminant of the quadratic form $(h_1x+k_1y)(h_2x+k_2y)$ is the square of the determinant $\begin{vmatrix} h_1 & h_2 \\ k_1 & k_2 \end{vmatrix}$. Deduce that if h_1, h_2, k_1, and k_2 are all integers, then the discriminant is a perfect square, possibly 0.

Proof. We obtain that

$$(h_1x + k_1y)(h_2x + k_2y) = h_1h_2x^2 + (h_1k_2 + h_2k_1)xy + k_1k_2y^2,$$

so using the identity $(X+Y)^2 - 4XY = (X-Y)^2$ with $X = h_1k_2$ and $Y = h_2k_1$, its discriminant is

$$(h_1k_2 + h_2k_1)^2 - 4(h_1h_2)(k_1k_2) = (h_1k_2 - h_2k_1)^2,$$

which is clearly the square of the determinant $h_1k_2 - h_2k_1$ of the matrix. Now if $h_1, h_2, k_1, k_2 \in \mathbb{Z}$, then $h_1k_2 - h_2k_1 \in \mathbb{Z}$ and thus the discriminant $(h_1k_2 - h_2k_1)^2$ is clearly a perfect square. ■

5 §3.4 #9

Problem (§3.4 #9)
Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form with integral coefficients whose discriminant d is a perfect square, possibly 0. Show that there are integers h_1, h_2, k_1, and k_2 such that $f(x, y) = (h_1x + k_1y)(h_2x + k_2y)$.

Proof. Let the discriminant $d = b^2 - 4ac$ of f be a perfect square. First, suppose that $a \neq 0$. Then

$$f(x, 1) = ax^2 + bx + c$$

is a quadratic, so by §3.4 #7 (Problem 3) $f(x, 1)$ has rational roots r_1 and r_2. We have $f(r_1, 1) = 0$ and $f(r_2, 1) = 0$. But also note

$$f(x, y) = y^2 f\left(\frac{x}{y}, 1\right),$$

so taking $x = r_1y$ (resp. $x = r_2y$) implies that $(x - r_1y)$ (resp. $(x - r_2y)$) divides $f(x, y)$ since $f(r_1y, y) = y^2 f(r_1, 1) = 0$ (resp. $f(r_2y, y) = y^2 f(r_2, 1) = 0$). Thus

$$f(x, y) = a(x - r_1y)(x - r_2y) = ax^2 - a(r_1 + r_2)xy + ar_1r_2y^2,$$

which implies that $ar_1r_2 = c \in \mathbb{Z}$. In particular, this implies that there exist $h_1, h_2 \in \mathbb{Z}$ such that $h_1h_2 = a$, $h_1r_1 \in \mathbb{Z}$, and $h_2r_2 \in \mathbb{Z}$. Set $k_1 = h_1r_1$ and $k_2 = h_2r_2$. Then we obtain

$$f(x, y) = a(x - r_1y)(x - r_2y) = h_1h_2(x - r_1y)(x - r_2y) = (h_1x - h_1r_1y)(h_2x - h_2r_2y) = (h_1x - k_1y)(h_2x - k_2y).$$

In the case when $a = 0$, we have $f(x, y) = bxy + cy^2$. Take $h_1 = 0$, $h_2 = b$, $k_1 = 1$, and $k_2 = c$; then

$$(h_1x + k_1y)(h_2x + k_2y) = y(bx + cy) = bxy + cy^2 = f(x, y),$$

as required. ∎

6 §3.4 #10

Problem (§3.4 #10)

Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form with integral coefficients. Show that there exist integers x_0, y_0, not both 0, such that $f(x_0, y_0) = 0$, if and only if the discriminant d of $f(x, y)$ is a perfect square, possibly 0.

Proof. ($\Longrightarrow$) Suppose there exist integers x_0 and y_0, not both 0, such that $f(x_0, y_0) = 0$. Note that if $a = 0$, then $d = b^2 - 4ac = b^2$ is already a perfect square. Thus assume $a \neq 0$. In particular, this implies that $y_0 \neq 0$; otherwise, if $y_0 = 0$, then $x_0 \neq 0$ (since they cannot be both 0) and $0 = f(x_0, y_0) = ax_0^2$, which implies $a = 0$.

- If $x_0 = 0$, then $0 = f(x_0, y_0) = cy_0^2$. Since $y_0 \neq 0$, this implies $c = 0$, so $d = b^2 - 4ac = b^2$, a perfect square.
- If $x_0 \neq 0$, then using $f(x, y) = y^2 f(x/y, 1)$ implies that $f(x_0/y_0, 1) = 0$. In other words, taking $u = x/y$, x_0/y_0 is a solution to the quadratic $f(x/y, 1) = f(u, 1) = au^2 + bu + c$. But note $x_0/y_0 \in \mathbb{Q}$, so §3.4 #7 (Problem 3) implies that the discriminant $d = b^2 - 4ac$ is a perfect square.

($\Longleftarrow$) Suppose that the discriminant d of $f(x, y)$ is a perfect square that is possibly 0. Then by §3.4 #9 (Problem 5), there exist $h_1, h_2, k_1, k_2 \in \mathbb{Z}$ such that $f(x, y) = (h_1 x + k_1 y)(h_2 x + k_2 y)$.

- If $h_1 = 0$ and $k_1 = 0$, then any $(x_0, y_0) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ satisfies $f(x_0, y_0) = 0$.
- If $h_1 \neq 0$ or $k_1 \neq 0$, then $(x_0, y_0) = (k_1, -h_1) \neq (0, 0)$ satisfies $f(x_0, y_0) = f(k_1, -h_1) = 0$.

Thus, there exist integers x_0, y_0, not both 0, such that $f(x_0, y_0) = 0$. ■

7 §3.5 #1

Problem (§3.5 #1)

Find a reduced form that is equivalent to the form $7x^2 + 25xy + 23y^2$.

Solution. An equivalent reduced form is

$$\boxed{x^2 + xy + 5y^2.}$$

For a 2×2 matrix $M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$ and any form $f(x, y)$, define $Mf(x, y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$. Write $f(x, y) = 7x^2 + 25xy + 23y^2$. Consider the matrix

$$M = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}.$$

Note that $M \in \Gamma$ (where Γ is the modular group[2]) since $\det M = 1$. Then $Mf \sim f$, where

$$Mf(x, y) = f(2x - y, -x + y) = x^2 + xy + 5y^2,$$

which is reduced since taking $a = 1$, $b = 1$, and $c = 5$ we have $-|a| < b \leq |a| < c$. ■

Remark 1. *To obtain the matrix M, consider the matrices*

$$M_1 = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}, \qquad M_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad M_3 = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}.$$

Since $M_1, M_2, M_3 \in \Gamma$, applying these matrices to $f_0 := f$ iteratively yields an equivalent form. In particular,

$$\begin{aligned} f_1(x, y) &:= M_1 f_0(x, y) = f_0(x - 2y, y) = 7x^2 - 3xy + y^2, \\ f_2(x, y) &:= M_2 f_1(x, y) = f_1(y, -x) = x^2 + 3xy + 7y^2, \\ f_3(x, y) &:= M_3 f_2(x, y) = f_2(x - y, y) = x^2 + xy + 5y^2, \end{aligned}$$

and f_3 is reduced. In particular, $M = M_1 M_2 M_3$.

[2] This group is also $\mathrm{SL}_2(\mathbb{Z})$.

8 §3.5 #6

Problem (§3.5 #6)
Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = f(-x, y) = ax^2 - bxy + cy^2$. These forms represent precisely the same numbers, but they are not necessarily equivalent (because the determinant of the transformation has determinant -1). Show that $x^2+xy+2y^2$ is equivalent to $x^2-xy+2y^2$, but that $3x^2+xy+4y^2$ and $3x^2-xy+4y^2$ are not equivalent.

Proof. For a 2×2 matrix $M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$ and any form $f(x, y)$, define $Mf(x, y) = f(m_{11}x + m_{12}y, m_{22}x + m_{22}y)$. Consider the matrix $M = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \in \Gamma$. Then writing $F(x, y) = x^2 + xy + 2y^2$ we obtain

$$MF(x, y) = F(x - y, y) = (x - y)^2 + (x - y)y + 2y^2 = x^2 - xy + 2y^2,$$

so $x^2 + xy + 2y^2$ is equivalent to $x^2 - xy + 2y^2$.

On the other hand, suppose for the sake of contradiction that $3x^2 + xy + 4y^2$ and $3x^2 - xy + 4y^2$ are equivalent. Write $G(x, y) = 3x^2 + xy + 4y^2$. By definition, there exists a matrix $N = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ such that

$$3x^2 - xy + 4y^2 = NG(x, y) = G(ax + by, cx + dy).$$

In particular, $3 = NG(1, 0) = G(a, c) = 3a^2 + ac + 4c^2$ and $4 = NG(0, 1) = G(b, d) = 3b^2 + bd + 4d^2$. This means

$$36 = 36a^2 + 12ac + 48c^2 = (6a + c)^2 + 47c^2,$$
$$48 = 36b^2 + 12bd + 48d^2 = (6b + d)^2 + 47d^2,$$

which forces $c = 0$, $a = \pm 1$ by the first equation and $d = \pm 1$, $b = 0$ by the second equation. Since $1 = ad - bc = ad$, a and d must have the same sign. Thus, either $a = d = 1$ or $a = d = -1$, which correspond to the matrices

$$N = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{or} \quad N = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

respectively, which both yield $NG(x, y) = 3x^2 + xy + 4y^2$. This is not $3x^2 - xy + 4y^2$, a contradiction. ■

Remark 2. *An alternative way of seeing that $3x^2 + xy + 4y^2$ and $3x^2 - xy + 4y^2$ are not equivalent binary quadratic forms is using the fact that if $d < 0$, then the reduced form in a given equivalence class is unique. Both $3x^2 + xy + 4y^2$ and $3x^2 - xy + 4y^2$ have discriminant $-47 < 0$ and both are reduced, so they cannot be equivalent.*