18.781 Theory of Numbers

Problem Set 8

Official Solutions

April 26, 2026

Contents

Disclaimer

This document contains the official solutions to Problem Set 8 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 §3.5 #5

Problem (§3.5 #5)

Show that x^2+5y^2 and $2x^2+2xy+3y^2$ are the only reduced quadratic forms of discriminant -20. Show that the first of these forms do not represent 2, but that the second one does. Deduce that these forms are inequivalent, and hence that $H(-20)=2$. Show that a prime p is represented by at least one of these forms if and only if $p=2$, $p=5$, or $p \equiv 1$, 3, 7, or 9 $\pmod{20}$.

Proof. Let $f(x,y)=x^2+5y^2$ and $g(x,y)=2x^2+2xy+3y^2$ with discriminant $d=-20$. First note that both f and g are positive definite since $d<0$ and $a>0$, by Theorem 3.11. They are clearly both reduced as well, so we show that there are no other reduced quadratic forms. Let $h(x,y)=ax^2+bxy+cy^2$ be a reduced binary quadratic form with discriminant $d=b^2-4ac=-20$. By Theorem 3.19, a is some integer such that $0<a\le\sqrt{-d/3}=\sqrt{20/3}$, which means that $a=1$ or $a=2$.

- Let $a=1$. Since h is reduced, we have $-|a|<b\le|a|<|c|$ or $0\le b\le|a|=|c|$. In either condition, we must have $b=0$ or $b=1$. We cannot have $b=1$ since no integer c satisfies $-20=d=b^2-4ac=1-4c$. Hence $b=0$, which forces $-20=d=b^2-4ac=-4c$, or $c=5$. This means $h(x,y)=x^2+5y^2=f(x,y)$.

- Let $a=2$. Since h is reduced, we have $-|a|<b\le|a|<|c|$ or $0\le b\le|a|=|c|$. In the first condition, b can take the values $b=-1,0,1,2$. We cannot have $b=0$ since no integer c satisfies $-20=d=b^2-4ac=-8c$; similarly, we cannot have $b=\pm1$ since no integer c satisfies $-20=d=b^2-4ac=1-8c$. In the case when $b=2$, we have $-20=d=b^2-4ac=4-8c$, or $c=3$. This means $h(x,y)=2x^2+2xy+3y^2=g(x,y)$.

  In the second condition, b can take the values $b=0,1,2$. By our previous work, we showed $b\ne0$ and $b\ne1$. Thus, the only other possibility is when $b=2$ and $a=2=c$, but this violates $-20=d=b^2-4ac$.

Thus, f and g are the only reduced quadratic forms of discriminant -20. Now g represents 2 since $g(1,0)=2$, but f does not: If $f(x,y)=2$, then we cannot have $y\ge1$ (since otherwise we have $2=x^2+5y^2\ge x^2+5$, i.e., $-3\ge x^2$, which is impossible), so $y=0$, which is also impossible (since this forces $x^2=2$ but 2 is not a perfect square). Thus f and g are not equivalent since g represents 2 but f does not, by Theorem 3.17.

By Corollary 3.14, there exists a binary quadratic form of discriminant d that represents p if and only if $p\mid d$ or $\left(\frac{d}{p}\right)=1$. For the first case, $p=2$ and $p=5$ divides $d=-20$. For the second, by quadratic reciprocity we have

$$1=\left(\frac{-20}{p}\right)=\left(\frac{2^2}{p}\right)\left(\frac{5}{p}\right)\left(\frac{-1}{p}\right)=\left(\frac{p}{5}\right)\left(\frac{-1}{p}\right).$$

By §3.1 #10 and the well known identity for $(-1\mid p)$ we have

$$\left(\frac{p}{5}\right)=\begin{cases}1 & \text{if } p\equiv\pm1 \pmod 5,\\ -1 & \text{if } p\equiv\pm2 \pmod 5,\end{cases}\quad\text{and}\quad \left(\frac{-1}{p}\right)=\begin{cases}1 & \text{if } p\equiv1 \pmod 4,\\ -1 & \text{if } p\equiv3 \pmod 4.\end{cases}$$

- In the former case, we solve the system $p\equiv\pm1\pmod 5$ and $p\equiv1\pmod 4$. The Chinese remainder theorem gives $p\equiv1,9\pmod{20}$.

- In the latter case, we solve the system $p\equiv\pm2\pmod 5$ and $p\equiv-1\pmod 4$. The Chinese remainder theorem gives $p\equiv3,7\pmod{20}$.

Therefore, p is representable if and only if $p=2$, $p=5$, or $p\equiv1,3,7,9\pmod{20}$. ∎

Remark 1. *Theorem 3.11 gives a nice and efficient identification of positive definite binary quadratic forms.*

> **Theorem** (Theorem 3.11)
> Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form with integral coefficients and discriminant d. If $d > 0$ then $f(x, y)$ is indefinite. If $d = 0$ then $f(x, y)$ is semidefinite but not definite. If $d < 0$ then a and c have the same sign and $f(x, y)$ is either positive definite or negative definite according as $a > 0$ or $a < 0$.

Remark 2. *Corollary 3.14 is useful for identifying which primes is representable by a binary quadratic form of a given discriminant.*

> **Corollary** (Corollary 3.14)
> Suppose that $d \equiv 0$ or $1 \pmod 4$. If p is an odd prime, then there is a binary quadratic form of discriminant d that represents p, if and only if $p \mid d$ or $\left(\frac{d}{p}\right) = 1$.

Remark 3. *The key statement of Theorem 3.17 is that equivalent binary quadratic forms share the same representations and the same discriminant.*

> **Theorem** (Theorem 3.17)
> Let f and g be equivalent binary quadratic forms. For any given integer n, the representations of n by f are in one-to-one correspondence with the representations of n by g. Also, the proper representations of n by f are in one-to-one correspondence with the proper representations of n by g. Moreover, the discriminants of f and g are equal.

Remark 4. *Theorem 3.19 is useful in finding all the reduced binary quadratic forms with a discriminant that is not a perfect square.*

> **Theorem** (Theorem 3.19)
> Let f be a reduced binary quadratic form whose discriminant d is not a perfect square. If f is indefinite, then $0 < |a| \leq \frac{1}{2}\sqrt{d}$. If f is positive definite then $0 < a \leq \sqrt{-d/3}$. In either case, the number of reduced forms of a given nonsquare discriminant is finite.

2 §3.5 #11

Problem (§3.5 #11)

Suppose that $ax^2+bxy+cy^2 \sim Ax^2+Bxy+Cy^2$. Show that $(a,b,c)=(A,B,C)$.

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 $Mf(x,y)=f(m_{11}x+m_{12}y, m_{21}x+m_{22}y)$. Let $f(x,y)=ax^2+bxy+cy^2$ and $F(x,y)=Ax^2+Bxy+Cy^2$. By definition, there exists some $M\in\Gamma$ such that

$$\begin{aligned} F(x,y) &= Mf(x,y) \\ &= f(m_{11}x+m_{12}y, m_{21}x+m_{22}y) \\ &= \left(am_{11}^2+bm_{11}m_{22}+cm_{21}^2\right)x^2+ \\ &\quad + \left(2am_{11}m_{12}+bm_{12}m_{21}+bm_{11}m_{22}+2cm_{21}m_{22}\right)xy \\ &\quad + \left(am_{12}^2+bm_{12}m_{22}+cm_{22}^2\right)y^2. \end{aligned}$$

Relating the coefficients of F and Mf gives

$$\begin{aligned} A &= am_{11}^2+bm_{11}m_{21}+cm_{21}^2, \\ B &= 2am_{11}m_{12}+bm_{12}m_{21}+bm_{11}m_{22}+2cm_{21}m_{22}, \\ C &= am_{12}^2+bm_{12}m_{22}+cm_{22}^2. \end{aligned}$$

We assume that a, b, and c are integers that are not all zero, as are A, B, and C, since otherwise (a,b,c) and (A,B,C) are not defined. By definition, we have $(a,b,c)\mid a$ if $a\neq 0$, $(a,b,c)\mid b$ if $b\neq 0$, and $(a,b,c)\mid c$ if $c\neq 0$, and at least one of them is true, so $(a,b,c)\mid A$, $(a,b,c)\mid B$, and $(a,b,c)\mid C$ from above. Therefore, we have

$$(a,b,c)\mid(A,B,C). \tag{1}$$

Conversely, $M^{-1}=\begin{bmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{bmatrix}\in\Gamma$ is such that $f(x,y)=M^{-1}F(x,y)$. Relating the coefficients of f and $M^{-1}F$ gives

$$\begin{aligned} a &= Am_{22}^2-Bm_{21}m_{22}+Cm_{21}^2, \\ b &= -2Am_{12}m_{22}+Bm_{12}m_{21}+Bm_{11}m_{22}-2Cm_{11}m_{21}, \\ c &= Am_{12}^2-Bm_{11}m_{12}+Cm_{11}^2. \end{aligned}$$

By definition, we have $(A,B,C)\mid A$ if $A\neq 0$, $(A,B,C)\mid B$ if $B\neq 0$, and $(A,B,C)\mid C$ if $C\neq 0$, and at least one of them is true, so $(A,B,C)\mid a$, $(A,B,C)\mid b$, and $(A,B,C)\mid c$ from above. Therefore, we have

$$(A,B,C)\mid(a,b,c). \tag{2}$$

Combining (1) and (2) gives $(a,b,c)=(A,B,C)$. ∎

3 §3.5 #12

Problem (§3.5 #12)
Let $f(x,y) = ax^2 + bxy + cy^2$ be a positive semidefinite quadratic form of discriminant 0. Put $g = (a,b,c)$. Show that f is equivalent to the form gx^2.

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 $Mf(x,y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$. We assume that a, b, and c are integers that are not all zero, as otherwise g is not defined. The discriminant of f is $d = b^2 - 4ac = 0$. Write $a' = a/g$, $b' = b/g$, and $c' = c/g$, so $(a', b', c') = 1$. Because $b^2 = 4ac$, dividing by g^2 gives $(b')^2 = 4a'c'$. Consider the following lemma.

Lemma 5
The integers a' and c' are coprime squares.

Proof of Lemma 5. If $(a', c') > 1$, then there exists some prime p such that $p \mid (a', c')$. Hence $p \mid a'$ and $p \mid c'$, so $p \mid 4a'c' = b'^2$ and hence $p \mid b'$. This implies that $(a', b', c') \geq p$, contrary to $(a', b', c') = 1$. To show that a' and c' are squares, consider the prime factorizations

$$a' = \prod_{p \text{ prime}} p^{\alpha(p)}, \qquad b' = \prod_{p \text{ prime}} p^{\beta(p)}, \qquad c = \prod_{p \text{ prime}} p^{\gamma(p)}.$$

Since $(a', c') = 1$ we must have $\alpha(p) = 0$ or $\gamma(p) = 0$ for every prime p. Since $(b')^2 = 4a'c'$, we have

$$2\beta(p) = \alpha(p) + \gamma(p) + 2\mathbb{I}[p = 2].$$

If $p = 2$, then $2\beta(p) = \alpha(p) + \gamma(p) + 2$. If $\alpha(p) = 0$, then $2\beta(p) = \gamma(p) + 2$, so $\gamma(p)$ is even. If $\gamma(p) = 0$, then $2\beta(p) = \alpha(p) + 2$, so $\alpha(p)$ is even. If $p > 2$, then $2\beta(p) = \alpha(p) + \gamma(p)$. Following a similar reasoning, if $\alpha(p) = 0$, then $2\beta(p) = \gamma(p)$, so $\gamma(p)$ is even. If $\gamma(p) = 0$, then $2\beta(p) = \alpha(p)$, so $\alpha(p)$ is even. Thus each exponent in the prime factorizations of a' and c' is even, so a' and c' are squares. ■

By Lemma 5, we write $a' = m^2$ and $c' = n^2$ for $m, n \in \mathbb{Z}$ such that $(m,n) = 1$. Therefore, there exist $u, v \in \mathbb{Z}$ such that $mu - nv = 1$. Write $f'(x,y) = gx^2$. Then consider the matrix $M = \begin{bmatrix} m & n \\ v & u \end{bmatrix} \in \Gamma$. We have

$$\begin{aligned}
Mf'(x,y) &= f'(mx + ny, vx + uy) \\
&= g(mx + ny)^2 \\
&= g\left(m^2x^2 + 2mnxy + n^2y^2\right) \\
&= g\left(a'x^2 + b'xy + c'y^2\right) \\
&= ax^2 + bxy + cy^2 \\
&= f(x,y),
\end{aligned}$$

where we choose m and n appropriately up to sign such that $b' = 2mn$ (as $(b')^2 = 4m^2n^2 = (2mn)^2$). ■

4 §3.5 #13

Problem (§3.5 #13)

A binary quadratic form $ax^2 + bxy + cy^2$ is called *primitive* if $(a, b, c) = 1$. Prove that if $ax^2 + bxy + cy^2$ is a form of discriminant d and $r = (a, b, c)$, then $(a/r)x^2 + (b/r)xy + (c/r)y^2$ is a primitive form of discriminant d/r^2. If d is a perfect square, let $h(d)$ denote the number of classes of primitive forms with discriminant d. Prove that $H(d) = \sum h\left(d/r^2\right)$ where the sum is over all positive integers r such that $r^2 \mid d$.

Proof. Suppose that $ax^2 + bxy + cy^2$ is a form of discriminant $d = b^2 - 4ac$. Put $r = (a, b, c)$. Then we must have $(a/r, b/r, c/r) = (a, b, c)/r = 1$, so $(a/r)x^2 + (b/r)xy + (c/r)y^2$ is primitive. Its discriminant is

$$(b/r)^2 - 4(a/r)(c/r) = \left(b^2 - 4ac\right)/r^2 = d/r^2.$$

For the second claim, let $X(d)$ denote the set of equivalence classes of binary quadratic forms of discriminant d, and let $P(d)$ denote the set of equivalent classes of primitive binary quadratic forms of discriminant d. Consider the map

$$\begin{gathered}\Phi\colon X(d) \to \bigcup_{r \in R} P\left(d/r^2\right), \\ \left[ax^2 + bxy + cy^2\right] \mapsto \left[(a/r)x^2 + (b/r)xy + (c/r)y^2\right],\end{gathered}$$

where $R = \left\{r \in \mathbb{N} \;\middle|\; r^2 \mid d\right\}$ is the set of positive integers r such that $r^2 \mid d$. We show that Φ is a bijection. First, we need to show that Φ is well-defined. Our above discussion shows that any binary quadratic form of discriminant d is mapped to a primitive binary quadratic form of discriminant d/r^2, but now we need to show that any two binary quadratic forms of discriminant d in the same equivalence class are mapped to the same equivalence class of primitive quadratic forms of discriminant d/r^2. To this end, suppose f and g are two quadratic forms of discriminant d such that $f \sim g$. Then there exists some $M \in \Gamma$ such that $Mf = g$.[1] If $f(x, y) = ax^2 + bxy + cy^2$, put $r = (a, b, c)$, and

$$M\left(\frac{f(x, y)}{r}\right) = \frac{Mf(x, y)}{r} = \frac{g(x, y)}{r},$$

so $f/r \sim g/r$. This same argument justifies that Φ is bijective: suppose $f', g' \in P\left(d/r^2\right)$ for some $r \in R$ such that $f' \sim g'$, so $Mf' = g'$; then taking $f = rf'$ (hence surjective) nd $g = rg'$ implies that $Mf = M(rf') = rMf' = rg' = g$, so $f \sim g$ (hence injective).

Since Φ is a bijection, the cardinalities of the domain and codomain of Φ are the same. The cardinality of $X(d)$ is $H(d)$; the cardinality of $P\left(d/r^2\right)$ is $h\left(d/r^2\right)$, and since the $P\left(d/r^2\right)$ are all disjoint for distinct $r \in R$, the cardinality of the union is $\sum_{r \in R} h\left(d/r^2\right)$. Therefore, $H(d) = \sum_{r \in R} h\left(d/r^2\right)$. ■

Remark 6. *The first part of the problem suggests constructing a map Φ, and the second part of the problem essentially suggests proving that Φ is a bijection.*

[1] As always, 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 $Mf(x, y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$.

5 §3.6 #5

Problem (§3.6 #5)
Suppose that n is not a perfect square. Show that the number of ordered pairs (x, y) of positive integers for which $x^2 + y^2 = n$ is $R(n)/4$. Show that if n is a perfect square then the number of such representations of n is $R(n)/4 - 1$.

Proof. Let $\mathbb{Z}^{2*} = \mathbb{Z}^2 \setminus \big((\mathbb{Z} \times \{0\}) \cup \{0\} \times \mathbb{Z})\big)$, i.e., all integer lattice points that are neither on the x- nor y-axis, and let $X(n) = \big\{(x, y) \in \mathbb{Z}^{2*} \bigm| x^2 + y^2 = n\big\}$ and $X_+(n) = \big\{(x, y) \in \mathbb{N}^2 \bigm| x^2 + y^2 = n\big\}$. Consider

$$\begin{aligned} \Phi\colon X(n) &\to X_+(n), \\ (x, y) &\mapsto (|x|, |y|). \end{aligned}$$

Clearly, for every $(x, y) \in X_+(n)$, there are four preimages of (x, y) under Φ, namely $\Phi^{-1}(x, y) = \{(\pm x, \pm y)\}$, so

$$|X_+(n)| = \frac{|X(n)|}{4}.$$

- Suppose n is not a perfect square. Then there are no solutions where $x = 0$ or $y = 0$ since such a solution would imply that n is a perfect square. Thus $x \neq 0$ and $y \neq 0$, so $|X(n)| = R(n)$ and $|X_+(n)| = |X(n)|/4 = R(n)/4$.
- Suppose n is a perfect square. This means that there are the four additional solutions $\big(\pm\sqrt{n}, 0\big)$, $\big(0, \pm\sqrt{n}\big) \in \mathbb{Z}^2$ that do not belong in $X(n)$. Thus $|X(n)| = R(n) - 4$, and $|X_+(n)| = |X(n)|/4 = R(n)/4 - 1$.

The proof is complete. ■

6 §3.6 #8

Problem (§3.6 #8)
Prove that if a positive integer n can be expressed as a sum of the squares of two rational numbers then it can be expressed as a sum of the squares of two integers.

Proof. Let n be a positive integer, and suppose that $n = r^2 + s^2$ for $r, s \in \mathbb{Q}$. Write $r = a/q$ and $s = b/q$ for $a, b \in \mathbb{Z}$ and $q \in \mathbb{Z} \setminus \{0\}$. Then $nq^2 = a^2 + b^2$, so nq^2 is a sum of two squares. By Theorem 2.15, all primes appearing in the prime factorization of nq^2 that are $\equiv 3 \pmod 4$ have even exponents. The exponents of such primes in q^2 are already even, so the exponents of such primes in n are even as well. Therefore, n is expressible as a sum of the squares of two integers. ■

Theorem (Theorem 2.15)
Write the canonical factorization of n in the form

$$n = 2^{\alpha} \prod_{p \equiv 1(4)} p^{\beta} \prod_{p \equiv 3(4)} p^{\gamma}.$$

Then n can be expressed as a sum of two squares of integers if and only if all the exponents γ are even.

7 §3.6 #9

Problem (§3.6 #9)
Suppose that n is a positive integer that can be expressed as a sum of two relatively prime squares. Show that every positive divisor of n must also have this property.

Proof. Let n be a positive integer, and suppose that $n = a^2 + b^2$ for $a, b \in \mathbb{Z}$ such that $(a, b) = 1$. Then (a, b) is a proper representation of n. Recall that $P(n)$ is the number of proper representations of n of the form $x^2 + y^2$ for which $x > 0$ and $y \geq 0$, so $P(n) > 0$. We show that $P(d) > 0$ for every positive $d \mid n$. Recall that $r(n)$ is the number of proper representations of n. Moreover, $r(n) = 4P(n)$, so $r(n) > 0$. In particular, $r(n) = 2^{t+2}$, where t is the number of primes p that divide n and are also $\equiv 1 \pmod 4$, and

$$n = 2^\alpha \prod_{p \equiv 1(4)} p^\beta$$

for $\alpha \in \{0, 1\}$ by Theorem 3.22. If $d \mid n$, then d has prime factorization

$$d = 2^{\alpha'} \prod_{p \equiv 1(4)} p^{\beta'}$$

for $\alpha' \in \{0, 1\}$ and $\beta' \in \{0, \ldots, \beta\}$. By Theorem 3.22, $r(d) > 0$, so $P(d) > 0$ as well. ■

Remark 7. *One of the key facts used in this proof is that $r(n) = 4P(n)$, which we used to convert this problem to an equivalent problem in terms of $r(n)$.*

Theorem (Theorem 3.22)
Let n be a positive integer, and write $n = 2^\alpha \prod_p p^\beta \prod_q q^\gamma$ where p runs over prime divisors of n of the form $4k+1$ in the first product, and q runs over prime divisors of n of the form $4k+3$ in the second. If $\alpha = 0$ or 1 and all the γ are 0, then $r(n) = 2^{t+2}$ where t is the number of prime p of the form $4k+1$ that divide n. Otherwise $r(n) = 0$. If all the γ are even then $R(n) = \prod_p (\beta + 1)$. Otherwise $R(n) = 0$.

8 §3.6 #10

Problem (§3.6 #10)
Suppose that a matrix M with integral elements and determinant -1 takes a form $f(x,y) = ax^2 + bxy + cy^2$ to $x^2 + y^2$. Prove that f and $x^2 + y^2$ are equivalent by showing that there is another matrix M_1, with integral elements and determinant $+1$, that also takes f to $x^2 + y^2$.

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 $Mf(x,y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$. Let $g(x,y) = x^2 + y^2$, and suppose that $\det M = -1$ such that $Mf(x,y) = g(x,y)$. Then consider the matrices

$$N = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad M_1 = NM = \begin{bmatrix} m_{21} & m_{22} \\ m_{11} & m_{12} \end{bmatrix}.$$

Then clearly $\det M_1 = \det N \det M = -1 \cdot -1 = 1$. Moreover,

$$M_1 f(x,y) = NMf(x,y) = Ng(x,y) = g(y,x) = x^2 + y^2,$$

so f and $x^2 + y^2$ are equivalent. ∎