Hints / solution sketches to problems

5.4.

(a). We discussed this in class; it is a direct application of Dirichlet's Theorem 5.9 (in LN), taking $d = -4$ in that theorem. Indeed, for $d = -4$ we can take $S_d = \{x^2 + y^2\}$; and we have $w = 4$; hence Theorem 5.9 gives that for every odd positive integer n,

$$R(n; x^2 + y^2) = 4 \sum_{m \mid n} \Big(\frac{-4}{m}\Big).$$

Using now also the fact that

$$\Big(\frac{-4}{m}\Big) = \begin{cases} 0 & \text{if } 2 \mid m, \\ 1 & \text{if } m \equiv 1 \mod 4, \\ -1 & \text{if } m \equiv 3 \mod 4, \end{cases}$$

we obtain the desired formula,

$$R(n; x^2 + y^2) = 4(d_1(n) - d_3(n)).$$

□

(b). For any positive integer n, a simple discussion gives

$$R(4n; x^2 + y^2) = R(n; x^2 + y^2). \tag{1}$$

[Detailed proof: Note that for any even integer x we have $x^2 \equiv 0 \mod 4$, and for every odd integer x we have $x^2 \equiv 1 \mod 4$. Hence for any integers x, y, if $x^2 + y^2 \equiv 0 \mod 4$ then both x and y must be *even*. It follows that the map $\langle x, y\rangle \mapsto \langle x/2, y/2\rangle$ maps the set

$$(*) \qquad \{\langle x, y\rangle \in \mathbb{Z}^2 \ : \ x^2 + y^2 = 4n\}$$

to a subset of $\mathbb{Z}^2$. Using this fact, it is easy to verify that this map $\langle x, y\rangle \mapsto \langle x/2, y/2\rangle$ is a *bijection* from the set in $(*)$ onto the set

$$\{\langle x', y'\rangle \in \mathbb{Z}^2 \ : \ {x'}^2 + {y'}^2 = n\}.$$

Hence these two sets have the same cardinality, i.e. (1) holds.]

Next we note that for any *odd* positive integer u, we have

$$R(2u; x^2 + y^2) = R(u; x^2 + y^2). \tag{2}$$

Proof: Note that $2u \equiv 2 \mod 4$, hence if $x, y \in \mathbb{Z}$ satisfy $x^2 + y^2 = 2u$ then both x and y must be odd, and so both $a = \frac{x-y}{2}$ and $b = \frac{x+y}{2}$ are integers. Note also that these a, b satisfy $a^2 + b^2 = (x^2 + y^2)/2 = u$. Conversely, if a, b are any two integers satisfying $a^2 + b^2 = u$ then the integers $x = a + b$ and $y = b - a$ satisfy $x^2 + y^2 = 2(a^2 + b^2) = 2u$. Note also that the two maps $\langle x, y\rangle \mapsto \langle \frac{x-y}{2}, \frac{x+y}{2}\rangle$ and $\langle a, b\rangle \mapsto \langle a + b, b - a\rangle$ are each others' inverses. Hence we have exhibited a bijection between the two sets

$$\{\langle x, y\rangle \in \mathbb{Z}^2 \ : \ x^2 + y^2 = 2u\} \quad \text{and} \quad \{\langle a, b\rangle \in \mathbb{Z}^2 \ : \ a^2 + b^2 = u\},$$

and therefore (2) holds.

By using both (2) and (1) (repeatedly), one proves that

$$R(2^k u; x^2+y^2) = R(u; x^2+y^2) \tag{3}$$

for every odd positive integer u and every $k \in \mathbb{Z}_{\geq 0}$. Also, by part (a), we have $R(u; x^2+y^2) = 4(d_1(u) - d_3(u))$. But note also that the set of odd positive divisors of u is equal to the set of odd positive divisors of $2^k u$. Hence:

$$R(2^k u; x^2+y^2) = R(u; x^2+y^2) = 4(d_1(u) - d_3(u)) = 4(d_1(2^k u) - d_3(2^k u)).$$

Hence we have proved the desired formula for $n = 2^k u$. Since every positive integer n can be expressed as $2^k u$, the proof is complete. $\square$

5.5. I have taken this problem from MNZ, [1, p. 176, Problem 6].

It follows from LN Lemma 5.2 that every positive definite quadratic form $[a, b, c]$ of discriminant -23 is equivalent to some quadratic form $[a, b, c]$ which satisfies $|b| \leq |a| \leq |c|$, which must of course also be positive definite and have discriminant $b^2 - 4a = -23$ (since our equivalence relation preserves positive definiteness and preserves the discriminant). Thus let us start by determining all positive definite quadratic forms $[a, b, c]$ satisfying $|b| \leq |a| \leq |c|$ and $b^2 - 4ac = -23$.

Assume that $[a, b, c]$ is such a form. Then

$$4a^2 \leq 4|ac| = |b^2 + 23| \leq 23 + b^2 \leq 23 + a^2,$$

and this implies $3a^2 \leq 23$, viz., $|a| \leq 2$. We also have $a > 0$ since $[a, b, c]$ is positive definite. Hence $a = 1$ or $a = 2$.

Case 1: $a = 1$. Then $|b| \leq |a| = 1$, and also $b^2 = 4ac - 23 \equiv 1 \mod 4$; hence $b = \pm 1$. It follows that $4c - 23 = 4ac - 23 = b^2 = 1$, i.e. $c = 6$. Hence: $[a, b, c] = [1, 1, 6]$ or $[1, -1, 6]$.

Case 2: $a = 2$. The $|b| \leq |a| \leq 2$; also $b^2 = 4ac - 23 \equiv 1 \mod 4$; hence $b = \pm 1$. It follows that $8c - 23 = 4ac - 23 = b^2 = 1$, i.e. $c = 3$. Hence: $[a, b, c] = [2, 1, 3]$ or $[2, -1, 3]$.

Hence we have proved that every positive definite quadratic form of discriminant -23 must be equivalent to one of the forms $[1, 1, 6]$, $[1, -1, 6]$, $[2, 1, 3]$ or $[2, -1, 3]$. It remains to sort out which equivalences exist between these four forms.

Recall from LN (197) that if $[a, b, c]$ and $[a', b', c']$ are equivalent then there exists some $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ such that (among other things) $a\alpha^2 + b\alpha\gamma + c\gamma^2 = a'$, viz., a' can be properly[1] represented by $[a, b, c]$. Thus: If $[1, 1, 6]$ and $[2, 1, 3]$ are equivalent, then there exist $x, y \in \mathbb{Z}$ satisfying $\gcd(x, y) = 1$ and $x^2 + xy + 6y^2 = 2$. The last relation can be rewritten as $(x + \frac{1}{2}y)^2 + \frac{23}{4}y^2 = 2$, and this implies $\frac{23}{4}y^2 \leq 2$; thus $y = 0$; hence $x^2 = 2$, which is impossible. This proves that $[1, 1, 6]$ and $[2, 1, 3]$ are *not* equivalent. The same argument also shows that $[1, 1, 6]$ and $[2, -1, 3]$ are not equivalent. Next, if $[2, 1, 3]$ and

[1]Indeed, we have $\gcd(\alpha, \gamma) = 1$, since $\alpha\delta - \beta\gamma = 1$.

$[2,-1,3]$ are equivalent then by LN (197), there exists $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ satisfying

$$(4) \qquad \begin{pmatrix} 2 & -1/2 \\ -1/2 & 3 \end{pmatrix} = \begin{pmatrix} 2\alpha^2+\alpha\gamma+3\gamma^2 & (4\alpha\beta+\beta\gamma+\alpha\delta+6\gamma\delta)/2 \\ (4\alpha\beta+\beta\gamma+\alpha\delta+6\gamma\delta)/2 & 2\beta^2+\beta\delta+3\delta^2 \end{pmatrix}.$$

In particular we then have $2 = 2\alpha^2+\alpha\gamma+3\gamma^2 = 2(\alpha+\frac{1}{4}\gamma)^2+\frac{23}{8}\gamma^2$; hence $\frac{23}{8}\gamma^2 \le 2$, which forces $\gamma = 0$, and thus also (again using $2 = 2\alpha^2+\alpha\gamma+3\gamma^2$): $\alpha = \pm 1$. Now $\alpha\delta = \alpha\delta - \beta\gamma = 1$ implies that $\delta = \alpha = \pm 1$, and next using also $2\beta^2+\beta\delta+3\delta^2 = 3$, viz., $2\beta^2 \pm \beta = 0$, we conclude that $\beta = 0$. But then $(4\alpha\beta+\beta\gamma+\alpha\delta+6\gamma\delta)/2 = 1/2$, so that the relation (4) does *not* hold. Hence $[2,1,3]$ and $[2,-1,3]$ are not equivalent!

On the other hand, the quadratic forms $[1,1,6]$ and $[1,-1,6]$ *are* equivalent; indeed, the matrix $g := \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ (which one finds by similar computations as the one in the previous paragraph) gives

$$\begin{aligned} g^{\mathrm{tr}} \begin{pmatrix} 1 & 1/2 \\ 1/2 & 6 \end{pmatrix} g &= \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1/2 \\ 1/2 & 6 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1/2 \\ 1/2 & 11/2 \end{pmatrix} = \begin{pmatrix} 1 & -1/2 \\ -1/2 & 6 \end{pmatrix}. \end{aligned}$$

To sum up, we have proved that every positive definite quadratic form of discriminant -23 must be equivalent to one of the forms $[1,1,6]$, $[1,-1,6]$, $[2,1,3]$ or $[2,-1,3]$, and we have also proved that among these, $[1,1,6]$ and $[1,-1,6]$ are equivalent, while the three forms $[1,1,6]$, $[2,1,3]$ and $[2,-1,3]$ are pairwise inequivalent. These facts together imply the statement in the problem formulation. □

Alternative: Using LN Problem 5.2 (or more precisely: the solution of that problem), one immediately reaches the set of representatives $[1,1,6]$, $[2,1,3]$ and $[2,-1,3]$, without any need to discuss possible equivalences between these.

We now turn to the second half of the problem. Thus let p be a prime satisfying $\left(\frac{-23}{p}\right) = \pm 1$. Then we have $p \neq 23$, thus $\gcd(p,23) = 1$, and so by LN Theorem 5.9 applied with $d = -23$ and $n = p$,

$$R(p;-23) = 2\Big(\left(\frac{-23}{1}\right) + \left(\frac{-23}{p}\right)\Big) = 2\Big(1 + \left(\frac{-23}{p}\right)\Big).$$

Also, by definition of $R(p;-23)$ and using the first part of the present problem, we have

$$R(p;-23) = R(p;Q_1) + R(p;Q_2) + R(p;Q_3)$$

Combining these two relations, we conclude that if $\left(\frac{-23}{p}\right) = -1$ then $R(p;Q_1) = R(p;Q_2) = R(p;Q_3) = 0$, while if $\left(\frac{-23}{p}\right) = 1$ then

(5) $$R(p;Q_1) + R(p;Q_2) + R(p;Q_3) = 4.$$

Furthermore,

$$\forall j \in \{1,2,3\}: \quad R(p;Q_j) \text{ is } \textit{even},$$

since $Q_j(x,y) = Q_j(-x,-y)$ $(\forall x,y \in \mathbb{R})$ and $Q_j(0,0) = 0 \neq p$. We also have

$$R(p;Q_2) = R(p;Q_3),$$

since $Q_2(x,-y) = Q_3(x,y)$ $(\forall x,y \in \mathbb{R})$[2], and $Q_2(x,0) = 2x^2 \neq p$ $(\forall x \in \mathbb{Z})$. Hence there exist $a,b \in \mathbb{Z}_{\geq 0}$ (which depend on p) such that $R(p;Q_1) = 2a$ and $R(p;Q_2) = R(p;Q_3) = 2b$. Using this notation, (5) implies that $a + 2b = 2$; and the only pairs $\langle a,b\rangle \in (\mathbb{Z}_{\geq 0})^2$ which satisfy the last relation are $\langle 2,0\rangle$ and $\langle 0,1\rangle$. Hence we have proved that if $\left(\frac{-23}{p}\right) = 1$ then either $[R(p;Q_1) = 4$ and $R(p;Q_2) = R(p;Q_3) = 0]$ or else $[R(p;Q_1) = 0$ and $R(p;Q_2) = R(p;Q_3) = 2]$.

It remains to discuss the prime $p = 139$. Note that this p satisfies $\left(\frac{-23}{139}\right) = -\left(\frac{23}{139}\right) = \left(\frac{139}{23}\right) = \left(\frac{1}{23}\right) = 1$;[3] Hence by what we have just proved, we have either $[R(p;Q_1) = 4$ and $R(p;Q_2) = R(p;Q_3) = 0]$ or else $[R(p;Q_1) = 0$ and $R(p;Q_2) = R(p;Q_3) = 2]$. However by completing the square we see that the equation $Q_1(x,y) = 139$ is equivalent with $(x + \frac{1}{2}y)^2 + \frac{23}{4}y^2 = 139$, and this implies $\frac{23}{4}y^2 \leq 139$, which forces $|y| \leq 4$, i.e. (using also the symmetry $Q_1(-x,-y) = Q_1(x,y)$) one only needs to test the five cases $y = 0,1,2,3,4$. One verifies that none of these cases gives rise to a solution $\langle x,y\rangle \in \mathbb{Z}^2$. Hence $R(139;Q_1) = 0$, and so by what we noted above, we must also have $R(139;Q_2) = R(139;Q_3) = 2$. [4] □

[2] This means that Q_2 and Q_3 are *"improperly equivalent"*, a concept which is not discussed in LN.

[3] The first equality holds since $139 \equiv 3 \mod 4$ implies $\left(\frac{-1}{139}\right) = -1$. The second equality holds by quadratic reciprocity, using $23 \equiv 139 \equiv 3 \mod 4$. The third equality holds since $139 \equiv 1 \mod 23$.

[4] The solutions to the equations $Q_2(x,y) = 139$ and $Q_3(x,y) = 139$ can similarly be found by completing the square. Indeed, $Q_2(x,y) = 139$ is equivalent with $2(x + \frac{1}{4}y)^2 + \frac{23}{8}y^2 = 139$, which implies $\frac{23}{8}y^2 \leq 139$, and so $|y| \leq 6$, i.e. we need only test the cases $y \in \{0,1,2,3,4,5,6\}$, and going through these, we find the single solution $\langle x,y\rangle = \langle 8,1\rangle$. Hence the set of solutions to $Q_2(x,y) = 139$ is $\{\langle 8,1\rangle, \langle -8,-1\rangle\}$, and the set of solutions to $Q_3(x,y) = 139$ is $\{\langle -8,1\rangle, \langle 8,-1\rangle\}$.

5.6. We will need the following strengthening of LN Lemma 8.13:

Lemma 1. *For all (real) $X \geq 1$,*

$$\sum_{1 \leq n \leq X} \frac{1}{n} = \log X + \gamma + O(X^{-1}).$$

Proof. Set $f(X) := \sum_{1 \leq n \leq X} \frac{1}{n} - \log X$; then our task is to prove that $f(X) = \gamma + O(X^{-1})$ for all $X \geq 1$. We know that $f(m) \to \gamma$ when m tends to $+\infty$ *through* $\mathbb{Z}$, by LN Lemma 8.13. Also for every $m \in \mathbb{Z}_{\geq 2}$ we have

$$f(m-1) - f(m) = -\log(m-1) + \log m - \frac{1}{m} = -\log\Big(1 - \frac{1}{m}\Big) + \frac{1}{m} = O(m^{-2}),$$

by the Taylor expansion of $\log(1+u)$ for $|u| < 1$. Hence for all $m, k \in \mathbb{Z}^+$, we have:

$$\begin{aligned} f(m) = f(m+k) + \sum_{j=m+1}^{m+k} \big(f(j-1) - f(j)\big) &= f(m+k) + \sum_{j=m+1}^{m+k} O(j^{-2}) \\ &= f(m+k) + O(m^{-1}), \end{aligned} \tag{6}$$

where the implied constant in both "big-Os" are absolute. (The last error bound is proved using a standard integral bound: $j^{-2} \leq \int_{j-1}^{j} x^{-2}\,dx$ for each $j \geq 2$; hence $\sum_{j=m+1}^{m+k} j^{-2} \leq \int_m^{m+k} x^{-2}\,dx \leq \int_m^\infty x^{-2}\,dx = m^{-1}$.) Letting $k \to \infty$ in (6), we conclude that

$$f(m) = \gamma + O(m^{-1}), \qquad \forall m \in \mathbb{Z}^+. \tag{7}$$

Finally, for an arbitrary real $X \geq 1$, set $m := \lfloor X \rfloor$. Then

$$f(X) = f(m) + \log m - \log X = f(m) + \log(m/X),$$

and using here (7) and $\max(\frac{1}{2}, 1 - X^{-1}) \leq m/X \leq 1$, which implies $\log(m/X) = O(X^{-1})$, we conclude that

$$f(X) = \gamma + O(m^{-1}) + O(X^{-1}) = \gamma + O(X^{-1}).$$

□

We can now solve Problem 5.6: We have, for all $X \geq 1$:

$$\begin{aligned}
\sum_{n \leq X} d(n) &= \sum_{\substack{m_1, m_2 \geq 1 \\ m_1 m_2 \leq X}} 1 = \sum_{1 \leq m_1 \leq \sqrt{X}} \sum_{1 \leq m_2 \leq X/m_1} 1 + \sum_{1 \leq m_2 \leq \sqrt{X}} \sum_{\sqrt{X} < m_1 \leq X/m_2} 1 \\
&= \sum_{1 \leq m_1 \leq \sqrt{X}} \left\lfloor \frac{X}{m_1} \right\rfloor + \sum_{1 \leq m_2 \leq \sqrt{X}} \left(\left\lfloor \frac{X}{m_2} \right\rfloor - \left\lfloor \sqrt{X} \right\rfloor \right) \\
&= \left(2 \sum_{1 \leq m \leq \sqrt{X}} \left\lfloor \frac{X}{m} \right\rfloor \right) - \left\lfloor \sqrt{X} \right\rfloor^2 \\
&= 2 \sum_{1 \leq m \leq \sqrt{X}} \left(\frac{X}{m} + O(1) \right) - \big(\sqrt{X} + O(1) \big)^2 \\
&= \left(2 \sum_{1 \leq m \leq \sqrt{X}} \frac{X}{m} \right) - X + O\big(\sqrt{X}\big)
\end{aligned}$$

Using Lemma 1, the above is:

$$\begin{aligned}
&= 2X\big(\log\big(\sqrt{X}\big) + \gamma\big) + O\big(\sqrt{X}\big) - X + O\big(\sqrt{X}\big) \\
&= X \log X + (2\gamma - 1)X + O\big(\sqrt{X}\big).
\end{aligned}$$

$\square$

8.9. (a). The formula (313) says that for all $z \in \mathbb{C} \setminus \mathbb{Z}$:

$$\frac{1}{z} + \sum_{m \in \mathbb{Z} \setminus \{0\}} \Big(\frac{1}{z-m} + \frac{1}{m} \Big) = \pi \cot(\pi z),$$

where the sum in the left hand side is uniformly absolutely convergent (in the sense that $\sum \big| \frac{1}{z-m} + \frac{1}{m} \big| < \infty$) for z in any compact subset of $\mathbb{C} \setminus \mathbb{Z}$. Hence for any $k \geq 2$, by repeated differentiation $k-1$ times we have, for all $z \in \mathbb{C} \setminus \mathbb{Z}$,

$$(8) \qquad (-1)^{k-1}(k-1)! \sum_{m \in \mathbb{Z}} \frac{1}{(z-m)^k} = \Big(\frac{d}{dz} \Big)^{k-1} \Big(\pi \cot(\pi z) \Big),$$

where the sum in the left hand side is again uniformly absolutely convergent in any compact subset of $\mathbb{C} \setminus \mathbb{Z}$. In order to rewrite the derivative in the right hand side, let us note that *when* $z \in \mathbf{H}$, we have:

$$\pi \cot(\pi z) = \pi \frac{(e^{\pi i z} + e^{-\pi i z})/2}{(e^{\pi i z} - e^{-\pi i z})/(2i)} = -\pi i \frac{1 + e^{2\pi i z}}{1 - e^{2\pi i z}} = -\pi i \Big(1 + 2 \sum_{a=1}^{\infty} e^{2\pi i a z} \Big),$$

where the last equality holds (with the sum being absolutely convergent) since $|e^{2\pi i z}| < 1$ when $z \in \mathbf{H}$. In fact the last sum is uniformly absolutely convergent for z in compact subsets of $\mathbf{H}$; hence we may differentiate term by term, to obtain, for all $k \geq 2$:

$$(9) \qquad \Big(\frac{d}{dz} \Big)^{k-1} \Big(\pi \cot(\pi z) \Big) = -(2\pi i)^k \sum_{a=1}^{\infty} a^{k-1} e^{2\pi i a z} \qquad (\forall z \in \mathbf{H}).$$

Combining (8) and (9) we obtain the desired formula. □

(b). For any fixed $n \geq 1$, replacing k by $2k$ and z by nz in the formula in (a), we obtain:

$$\sum_{m \in \mathbb{Z}} \frac{1}{(nz+m)^{2k}} = \sum_{m \in \mathbb{Z}} \frac{1}{(nz-m)^{2k}} = \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{a=1}^{\infty} a^{2k-1} e^{2\pi i a n z} \qquad (\forall z \in \mathbf{H}).$$

Also for any fixed $n \geq 1$, using $(-nz-m)^{2k} = (nz+m)^{2k}$, we have

$$\sum_{m \in \mathbb{Z}} \frac{1}{(-nz+m)^{2k}} = \sum_{m \in \mathbb{Z}} \frac{1}{(-nz-m)^{2k}} = \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{a=1}^{\infty} a^{2k-1} e^{2\pi i a n z} \qquad (\forall z \in \mathbf{H}).$$

Adding the two formulas above, and then adding over all $n \in \mathbb{Z}^+$, we obtain:

$$\sum_{n \neq 0} \sum_{m \in \mathbb{Z}} \frac{1}{(nz+m)^{2k}} = \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sum_{a=1}^{\infty} a^{2k-1} e^{2\pi i a n z}.$$

(We know that the double sum in the left hand side is absolutely convergent, by Problem 3.13(a); also the double sum in the right hand side is absolutely convergent for all $z \in \mathbf{H}$.)

Here in the right hand side we write $m := an$; then for each fixed $m \in \mathbb{Z}^+$, a runs over all (positive) divisors of m, and we obtain that the above sum equals

$$\frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{m=1}^{\infty} \left(\sum_{a|m} a^{2k-1} \right) e^{2\pi imz} = \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{m=1}^{\infty} \sigma_{2k-1}(m) e^{2\pi imz}.$$

Finally, we have

$$\sum_{m \in \mathbb{Z} \setminus \{0\}} \frac{1}{m^{2k}} = 2\zeta(2k),$$

and adding this equality to the equality proved above, we obtain:

$$\sum_{(m,n) \neq (0,0)} \frac{1}{(nz+m)^{2k}} = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{m=1}^{\infty} \sigma_{2k-1}(m) e^{2\pi imz},$$

i.e. the formula that we wanted to prove. □

9.1. (b).

(I may not write out the solution to this problem. However note that the fact that Λ is generated by $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is proved in the remark below following the solution to part (c).

9.1. (c). (i). Follows from [2, Lemma 3.5]. (ii). Assume that $T_1, T_2 \in \Lambda$ are such that $T_1(\mathcal{F}^\circ) \cap T_2(\mathcal{F}^\circ) \neq \emptyset$, i.e. there is a point τ' belonging to both $T_1(\mathcal{F}^\circ)$ and $T_2(\mathcal{F}^\circ)$. Set $\tau := T_1^{-1}(\tau')$ and $T := T_2^{-1}T_1 \in \Lambda$; then $\tau \in \mathcal{F}^\circ$ and $T(\tau) = T_2^{-1}(\tau') \in \mathcal{F}^\circ$. We will prove that

$$\forall T \in \Lambda : \ \forall \tau \in \mathcal{F}^\circ : \ T(\tau) \in \mathcal{F}^\circ \Rightarrow T = \pm I_2 \tag{10}$$

Note that when applying (10) to our situation, we obtain $T_2^{-1}T_1 = T = \pm I_2$, viz., $T_2 = \pm T_1$, and this completes the proof of (ii) (namely, we obtain the contrapositive form of (ii)).

Hence it now only remains to prove (10). Thus assume that $T \in \Lambda$, $\tau \in \mathcal{F}^\circ$ and $T(\tau) \in \mathcal{F}^\circ$. If $\operatorname{Im}\tau > \operatorname{Im} T(\tau)$ then after replacing $\langle \tau, T\rangle$ by $\langle T(\tau), T^{-1}\rangle$ we have $T \in \Lambda$, $\tau \in \mathcal{F}^\circ$ and $T(\tau) \in \mathcal{F}^\circ$ *and* $\operatorname{Im}\tau \leq \operatorname{Im} T(\tau)$ [5]; hence from now on we may assume that $\operatorname{Im}\tau \leq \operatorname{Im} T(\tau)$, with the earlier assumptions $T \in \Lambda$, $\tau \in \mathcal{F}^\circ$ and $T(\tau) \in \mathcal{F}^\circ$ still holding.

Write $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; then $\operatorname{Im} T(\tau) = \frac{\operatorname{Im}\tau}{|c\tau+d|^2}$, and hence $\operatorname{Im}\tau \leq \operatorname{Im} T(\tau)$ implies that $|c\tau + d|^2 \leq 1$. But we have

$$|c\tau + d|^2 = c^2|\tau|^2 + 2cd\operatorname{Re}(\tau) + d^2 \geq c^2 - 2|cd| + d^2 = (|c| - |d|)^2 \geq 1, \tag{11}$$

where the first inequality holds since $\tau \in \mathcal{F}^\circ$ implies that $|\tau| > 1$ and $|\operatorname{Re}\tau| < 1$, and the last inequality holds since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Lambda$ implies that $c \not\equiv d \mod 2$; hence $|c| \neq |d|$. Now (11) together with $|c\tau + d|^2 \leq 1$ implies that *equality* holds in both "$\geq$" in (11). Since $|\tau| > 1$ and $|\operatorname{Re}\tau| < 1$, this forces $c = 0$, and then $|d| = 1$. It then follows that $1 = ad - bc = ad$, so that $a = d = \pm 1$. Hence $T(\tau) = \tau + ab$, $\forall \tau \in \mathcal{H}$; and ab is an *even* integer, because of $T \in \Lambda$. Now $|\operatorname{Re}(\tau)| < 1$ and $|\operatorname{Re} T(\tau)| < 1$, i.e. $|\operatorname{Re}(\tau) + ab| < 1$, together force $ab = 0$, i.e. $b = 0$. Hence $T = \pm I_2$, and (10) is proved. □

[5] And it suffices to prove that the *new* T is $\pm I_2$, since this implies that T^{-1}, viz. the *old* T, is also $\pm I_2$.

Remark: By elaborating slightly on the above discussion we also obtain a proof of the claim that the group Λ is generated by $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Indeed, let us first note that (10) can be sharpened by replacing "$T(\tau) \in \mathcal{F}^\circ$" by "$T(\tau) \in \mathcal{F}$":

$$\forall T \in \Lambda : \ \forall \tau \in \mathcal{F}^\circ : \ T(\tau) \in \mathcal{F} \Rightarrow T = \pm I_2. \tag{12}$$

[Proof: Assume that $T \in \Lambda$, $\tau \in \mathcal{F}^\circ$ and $T(\tau) \in \mathcal{F}$. Note that $\mathcal{F}$ equals the closure of $\mathcal{F}^\circ$; hence there exists a sequence of points $\tau_1, \tau_2, \ldots$ in $\mathcal{F}^\circ$ tending to $T(\tau)$. Then $T^{-1}(\tau_j)$ tends to τ as $j \to \infty$, and we have $\tau \in \mathcal{F}^\circ$; hence for j sufficiently large we have $T^{-1}(\tau_j) \in \mathcal{F}^\circ$. For any such j, we have both $\tau_j \in \mathcal{F}^\circ$ and $T^{-1}(\tau_j) \in \mathcal{F}^\circ$; hence by (10), $T^{-1} = \pm I_2$; and hence $T = \pm I_2$.]

Now we can argue as follows: Let Λ' be the subgroup of $\mathrm{SL}(2, \mathbb{Z})$ generated by $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. It is obvious that $\Lambda' \subset \Lambda$; hence our task is to prove that $\Lambda \subset \Lambda'$. Let U be an arbitrary element in Λ, and consider the point $U(2i)$ in $\mathbf{H}$. Next, note that [2, Lemma 3.5] actually says that $\mathbf{H} = \cup_{T \in \Lambda'} T(\mathcal{F})$! Hence there exists some $T \in \Lambda'$ such that $U(2i) \in T(\mathcal{F})$. Then $T^{-1}U(2i) \in \mathcal{F}$, and $T^{-1}U \in \Lambda$; and also $2i \in \mathcal{F}^\circ$. Hence by (12), $T^{-1}U = \pm I_2$, i.e. $T = \pm U$, i.e. we have proved that either $U \in \Lambda'$ or $-U \in \Lambda'$. But note that

$$-I_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 \in \Lambda'.$$

Hence $-U \in \Lambda'$ implies $U = (-I_2)(-U) \in \Lambda'$, i.e. we definitely have $U \in \Lambda'$. This completes the proof that $\Lambda \subset \Lambda'$, viz., $\Lambda = \Lambda'$. □

References

1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An introduction to the theory of numbers*, fifth ed., John Wiley & Sons Inc., New York, 1991.
2. Elias M. Stein and Rami Shakarchi, *Complex analysis*, Princeton Lectures in Analysis, II, Princeton University Press, Princeton, NJ, 2003. MR 1976398 (2004d:30002)