567 Number Theory I, Fall Term 2008, Solutions 13

1. (i) Find all elements A of Γ which commute with S. (ii) Find all elements A of Γ which commute with T. (iii) Find the smallest $n > 0$ such that $(ST)^n = I$. (iv) Determine all A in Γ which leave i fixed. (v) Determine all A in Γ which leave $\rho = e(1/3)$ fixed.

(i) Consider $Az = \frac{az+b}{cz+d}$, $ad - bc = 1$. Then $SA = -\frac{cz+d}{az+b}$, $AS = \frac{bz-a}{dz-c}$. Cross multiplying and equating coefficients gives $ab = -cd$, $c^2 - d^2 = b^2 - a^2$. $bc = 0$ implies $ad = 1$, $a = d = \pm 1$, $A = I$. $ad = 0$ implies $bc = -1$, $b = \pm 1$, $c = \mp 1$, $A = S$. If $abcd \neq 0$, then $ad - bc = 1$ implies $(a, c) = (b, d) = 1$ and so $ab = -cd$ gives $a = \pm d$, $b = \mp c$, whence $\pm(a^2 + b^2) = 1$ and so $ab = 0$ which is impossible. (ii) $TAz = \frac{(a+1)z+b+d}{cz+d}$, $TAz = \frac{az+a+b}{cz+c+d}$. Equating coefficients gives $(a + c)c = ac$ so $c = 0$. Then $ad = 1$, $a = d = \pm 1$, $Az = z \pm b$ for arbitrary b, so T commutes with T^b ($b \in \mathbb{Z}$). (iii) $STz = -1/(z + 1)$, $(ST)^2 z = -(z + 1)/z$, $(ST)^3 z = z$. $n = 3$. (iv) $i = \frac{ai+b}{ci+d}$ and equating real and imaginary parts gives $a = d$, $b = -c$. Then $a^2 + b^2 = 1$, so $a = \pm 1$, $b = 0$, or $a = 0$, $b = \pm 1$. Thus $A = I$ or $A = S$. (v) $\rho = \frac{a\rho+b}{c\rho+d}$, cross multiplying, and using $\rho^2 + \rho + 1 = 0$ and fact that ρ is not real gives $c = -b$, $a = d + b$. Thus $a(a - b) + b^2 = 1$. There are three sets of solutions $a = d = \pm 1$, $b = c = 0$; $a = 0$, $d = c = -b = \pm 1$; $a = b = -c = \pm 1$, $d = 0$. Thus $A = I$, $A = ST$ or $A = T^{-1}S$.

2. Prove that if $A \in \Gamma$, and $(x, y)^T = A(x', y')^T$, then the quadratic form Q' defined by $Q'(x', y') = Q(x, y)$ satisfies $d_{Q'} = d_Q$.

In an obvious abuse of notation here and below we use A for both $A \in \Gamma$ and the associated matrix $\mathcal{A} \in SL_2(\mathbb{Z})$. Also we associate Q with the matrix $\mathcal{Q} = \begin{bmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{bmatrix}$. Now $\mathcal{Q}' = \mathcal{A}^T \mathcal{Q} \mathcal{A}$ and $d(Q') = -4\det(\mathcal{A}^T \mathcal{Q} \mathcal{A}) = -4\det(\mathcal{Q}) = d(\mathcal{Q})$.

3. (i) If d is fixed, prove that there is a bijection between the set of forms with discriminant d and the members of $\mathbb{H}$. (ii) Prove that two quadratic forms with discriminant d are equivalent iff their representatives are equivalent under Γ.

(i) For a given form Q we map Q to the root w of $Q(z, 1)$ in $\mathbb{H}$. If Q' is another form mapping to w, then it has the same roots as Q so is proportional to Q. As the discriminants are identical and the constant terms are positive the constant of proportionality must be 1. Now let $w = u + iv \in \mathbb{H}$. Choose $a = \sqrt{-d}/(2v)$, $c = aw\overline{w}$, $b = -2au$. Then $az^2 + bz + c = a(z - w)(z - \overline{w})$ and $d = b^2 - 4ac$. (ii) Suppose that Q maps to $z \in \mathbb{H}$ and Q' is equivalent to Q as in Q2. Let z' be the representative of Q'. Then $0 = Q'(z', 1) = Q(az' + b, cz' + d) = (cz' + d)^2 Q(Az', 1)$ and so $Az' = z$. Now suppose that Q and Q' have representatives z and z', and $z = Az'$ for some $A \in \Gamma$. Then $0 = Q(z, 1) = (cz' + d)^2 Q(Az', 1) = Q(az' + b, cz' + d) = (z', 1)\mathcal{A}^T \mathcal{Q} \mathcal{A}(z', 1)^T = Q''(z', 1)$ where Q'' is equivalent to Q under A. But z' is the representative of Q', so $Q'' = Q'$ and Q and Q' are equivalent.

4. Prove that $Q(x, y) = ax^2 + bxy + cy^2$ is reduced iff either $-a < b \le a < c$ or $0 \le b \le a = c$.

Write $Q = a(x - zy)(x - \overline{z}y)$. Then $z \in \mathbb{D}$ iff $-\frac{1}{2} \le \Re z < \frac{1}{2}$ and $|z| > 1$, or $-\frac{1}{2} \le \Re z \le 0$ and $|z| = 1$. Moreover, $b = -2a\Re z$ and $c = a|z|^2$.

5. Prove that the number of reduced forms with a given discriminant $d < 0$ is finite.

Let d be given. Then for any Q with discriminant d we have $4ac - b^2 = -d$. When Q is reduced, $|b| \le a$ and $c \ge a$. Hence $3a^2 \le -d$, so the number of possible a is at most $\sqrt{-d/3}$. For any such a there are at most $1 + 2a \le 1 + 2\sqrt{-d/3}$ choices for b. c is fixed by a and b.

6. When $d = -3, -4, -7, -8, -11, -15, -19, -20, -23$ determine all reduced forms with discriminant d, and the corresponding class number $h(d)$.

Let a, b, c denote the quadratic form Q. The reduced quadratic forms for each d are as follows.
-3:1,1,1; -4:1,0,1; -7:1,1,2; -8:1,0,2; -11:1,1,3; -15:1,1,4/2,1,2; -19:1,1,5; -20:1,0,5/2,2,3;
-23:1,1,6/2,1,3/2,-1,3. The class number is 1 for d = -3, -4, -7, -8, -11, is 2 for d = -15, -20 and is 3 for d = -23.