18.781 Problem Set 8: Due Wednesday, April 26.

1. Recall that for any (nonsquare) discriminant d, there is a bijection $\theta : F(d) \to X(d)$ from the set of primitive forms of discriminant d to the set of quadratic irrationals of discrimant d. We have defined actions of $\mathrm{GL}_2(\mathbb{Z})$ on both sides: for a form f, $\gamma f = f \circ \gamma^{-1}$, and for $\alpha \in \mathbb{C} - \mathbb{Q}$ and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ by $\gamma\alpha = \dfrac{a\alpha + b}{c\alpha + d}$. Show that θ is equivariant for the subgroup $\mathrm{SL}_2(\mathbb{Z})$. You may use the fact that $\mathrm{SL}_2(\mathbb{Z})$ is generated as a group by the matrices

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad T = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

2. **(a)** Let α be in the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im} z > 0\}$. Show that there is at most one element of the domain D (defined as the set of $z = x + iy \in \mathbb{H}$ such that $-\frac{1}{2} \leq x < \frac{1}{2}$, $|z| \geq 1$ and $x \leq 0$ if $|z| = 1$) of the form $\gamma\alpha$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

(b) Now let $\alpha \in D$ and compute the isotropy group

$$I(\alpha) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma\alpha = \alpha\}.$$

Can you relate this to the computation of the group of units of imaginary quadratic orders?

3. Find the reduced form strictly equivalent to each of the following forms. In each case give the matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $f \circ \gamma$ is reduced.

$$10x^2 + 14xy + 5y^2 \qquad 10x^2 + 12xy + 5y^2$$

4. For the discriminants -163 and -164, enumerate the reduced positive-definite forms in $F(d)$, and compute the class number h, the strict class number h_s, and the form class number h_f.

5. Show that a prime number p is represented by the form $x^2 + 3xy + 4y^2$ if and only if p is odd and congruent to 1, 2, or 4 $\pmod 7$.

6. These representation theorems are not purely existential; one may use them to construct such representations. Here is an example. The number $p = 131101$ is prime. (This is the "hard" part.) It is congruent to 1 mod 4, so it can be expressed as a sum of two squares. You will find (x, y) such that $x^2 + y^2 = p$ in this exercise.

(a) Show that 3 is a quadratic non-residue mod p.

(b) Find the binary expansion of p, and use it to expedite the computation of the representative s of $3^{\frac{p-1}{4}} \bmod p$ such that $0 < s < p$.

(c) Euler's criterion tells us that $s^2 \equiv -1 \,(\mathrm{mod}\, p)$. Find k such that $s^2 = kp - 1$. Then the quadratic form $f(x, y) = px^2 + 2sxy + ky^2$ has discriminant -4, and $f(1, 0) = p$.

(d) Now reduce this form to a reduced form, which, since $h_f(-4) = 1$, must be $x^2 + y^2$. As you do this reduction, keep track of the matrices you use, and in the end apply the product to the vector $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ to get what you were looking for.

EYPHKA! num $= \Delta + \Delta + \Delta$

—C.-F. Gauss, entry 18, July 10, 1796, in his diary. (Gauss was born on April 30, 1777. The entry records his proof of a conjecture of Fermat, that any positive integer is a sum of three triangular numbers, i.e., numbers of the form $n(n + 1)/2$ for an integer n.)