Ramanujan Graphs, Quaternions, and Number Theory homework - Day 3

Some of these exercises are rather time-consuming/difficult. You don't need to do all of them; just choose the ones that look the most interesting to you.

1. Prove Lemma 3.3 in the notes.

2. Let $\mathcal{O} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{Z}\}$.

   (a) Show that there is no left $\mathcal{O}$-ideal Λ such that $\Lambda \subseteq \mathcal{O}$ and $[\mathcal{O} : \Lambda] = 3$.

   (b) List the left $\mathcal{O}$-ideals Λ such that $\Lambda \subseteq \mathcal{O}$ and $[\mathcal{O} : \Lambda] = 9$. By Theorem 3.9 in the notes, there are four of them.

3. Let $\mathcal{O}$ be an order in $\mathbb{H}$. Problem 4d below shows that if $\mathcal{O}$ is unramified at a prime p, then for all n, $\mathcal{O}/p^n\mathcal{O}$ is isomorphic to $M_2(\mathbb{Z}/p^n\mathbb{Z})$, the set of 2×2 matrices with coefficients in $\mathbb{Z}/p^n\mathbb{Z}$. Show that, nonetheless, $\mathcal{O}$ is never isomorphic to $M_2(\mathbb{Z})$. (Hint: can the product of two nonzero elements of $\mathcal{O}$ be zero? What about the product of two nonzero elements of $M_2(\mathbb{Z})$?)

4. Let p be a prime number. In the second lecture, we constructed a graph according to the following procedure:

   - Draw a vertex for each lattice in the plane.
   - Draw an edge between the vertices Λ_1, Λ_2 if $\Lambda_2 \subset \Lambda_1$ and $[\Lambda_1 : \Lambda_2] = p$.
   - Identify vertices Λ_1, Λ_2 if there exists a real number z such that $\Lambda_1 = z\Lambda_2$.

   In the third lecture, we constructed a graph according to the following procedure:

   - Let $\mathcal{O}$ be an order in $\mathbb{H}$.
   - Draw a vertex for each left $\mathcal{O}$-ideal.
   - Draw an edge between the vertices Λ_1, Λ_2 if $\Lambda_2 \subset \Lambda_1$ and $[\Lambda_1 : \Lambda_2] = p^2$.
   - Identify vertices Λ_1, Λ_2 if there exists $z \in \mathbb{H}$ such that $\Lambda_1 = \Lambda_2 z$.

   In this exercise, you will show that these two procedures yield the same graph if $\mathcal{O}$ is unramified at p.

   This exercise is rather long, so feel free to do just parts of it. You can assume part (a) when doing part (b), etc. In particular, part (f) will help you understand why we want to prove parts (d)–(e), and part (d) will help you understand why we want to prove parts (a)–(c).

(a) The *Chevalley-Warning theorem* states the following. Let $n > d$ be positive integers, and let P be a homogeneous polynomial of degree d in n variables with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Then there exist $x_1, \ldots, x_n \in \mathbb{Z}/p\mathbb{Z}$, not all zero, such that $P(x_1, \ldots, x_n) = 0$.

Prove the Chevalley-Warning theorem, using the following steps.

i. By Fermat's little theorem, if $P(x_1, \ldots, x_n) \neq 0$, then $P(x_1, \ldots, x_n)^{p-1} = 1$. So the number of zeros of P is congruent mod p to

$$\sum_{x_1,\ldots,x_n \in \mathbb{Z}/p\mathbb{Z}} \left(1 - P(x_1, \ldots, x_n)^{p-1}\right) .$$

ii. Since P is homogeneous of degree d, P^{p-1} is homogeneous of degree $(p-1)d$. Consider a monomial $x_1^{d_1} \cdots x_n^{d_n}$ appearing in P^{p-1}. We have $\sum_i d_i = (p-1)d < (p-1)n$, so we must have $d_i < p-1$ for some i.

iii. For any nonzero $y \in \mathbb{Z}/p\mathbb{Z}$, we have

$$\sum_{x_i \in \mathbb{Z}/p\mathbb{Z}} x_i^{d_i} = \sum_{x_i \in \mathbb{Z}/p\mathbb{Z}} (yx_i)^{d_i} = y^{d_i} \sum_{x_i \in \mathbb{Z}/p\mathbb{Z}} x_i^{d_i} .$$

If $d_i < p-1$, then we can find y so that $y^{d_i} \neq 1$, which implies

$$\sum_{x_i \in \mathbb{Z}/p\mathbb{Z}} x_i^{d_i} = 0 .$$

iv. Conclude that the number of solutions to the equation $P(x_1, \ldots, x_n) = 0$ is divisible by p. In particular, $(0, \ldots, 0)$ cannot be the only solution.

(b) Apply the Chevalley-Warning theorem to show that there is a nonzero $z \in \mathcal{O}/p\mathcal{O}$ satisfying $\operatorname{tr} z = 0$ and $N(z) = 0$. (This part does not use the assumption that $\mathcal{O}$ is unramified at p.)

(c) Use induction to show that for any positive integer n, $\mathcal{O}/p^n\mathcal{O}$ has an element z such that z is not a multiple of p, $\operatorname{tr} z = 0$, and $N(z) = 0$. (Hint: suppose we have an element $z \in \mathcal{O}/p^{2n}\mathcal{O}$ such that z is not a multiple of p, and $\operatorname{tr} z$ and $N(z)$ are divisible by p^n. Since $\mathcal{O}$ is unramified at p, we can find $w \in \mathcal{O}/p^{2n}\mathcal{O}$ such that $\operatorname{tr} zw^*$ is not divisible by p. Let $z' = z - \frac{N(z)}{\operatorname{tr} zw^*} w$, and let $z'' = z' - \frac{\operatorname{tr} z'}{\operatorname{tr} zw^*} zw^*$. Verify that z'' is not a multiple of p, $N(z'') = N(z') = 0$, and $\operatorname{tr}(z'') = 0$.)

(d) Show that for any positive integer n, $\mathcal{O}/p^n\mathcal{O}$ is isomorphic to $M_2(\mathbb{Z}/p^n\mathbb{Z})$, the ring of 2×2 matrices with coefficients in $\mathbb{Z}/p^n\mathbb{Z}$. (Hint: in part (c), you found an element $z \in \mathcal{O}/p^n\mathcal{O}$; send z to $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Since $\mathcal{O}$ is unramified at p, there is an element $w \in \mathcal{O}/p^n\mathcal{O}$ such that $\operatorname{tr} zw = 1$. Send w to $\begin{pmatrix} \operatorname{tr} w & -N(w) \\ 1 & 0 \end{pmatrix}$).

(e) Let $\Lambda \subset \mathcal{O}$ be a lattice such that $[\mathcal{O} : \Lambda]$ is a power of p and $\mathcal{O} \cdot \Lambda \subseteq \Lambda$. Show that Λ is a left $\mathcal{O}$-ideal (i.e. show that if $z\Lambda \subseteq \Lambda$, then $z \in \mathcal{O}$).

(f) Show that for any positive integer n, there are natural bijections between the following sets:

i. Left $\mathcal{O}$-ideals Λ such that $p^n\mathcal{O} \subseteq \Lambda \subseteq \mathcal{O}$.

ii. Left $\mathcal{O}/p^n\mathcal{O}$-submodules of $\overline{\Lambda}$ of $\mathcal{O}/p^n\mathcal{O}$. (A left $\mathcal{O}/p^n\mathcal{O}$-submodule of $\mathcal{O}/p^n\mathcal{O}$ is an additive subgroup $\overline{\Lambda} \subset \mathcal{O}/p^n\mathcal{O}$ such that for all $z_1 \in \mathcal{O}/p^n\mathcal{O}$, $z_2 \in \overline{\Lambda}$, $z_1z_2 \in \overline{\Lambda}$).

iii. Left $M_2(\mathbb{Z}/p^n\mathbb{Z})$-submodules $\overline{E}$ of $M_2(\mathbb{Z}/p^n\mathbb{Z})$.

iv. Subgroups $\overline{V}$ of $(\mathbb{Z}/p^n\mathbb{Z})^2$.

v. Subgroups V of $\mathbb{Z}^2$ containing $p^n\mathbb{Z}^2$.

(g) Explain why the previous part implies that the two constructions yield the same graph.

5. In this exercise, we will see that Theorem 3.9 in the notes isn't quite true; there is an assumption missing that I did not want to tell you in class. This exercise will use Sage; go to `https://sagecell.sagemath.org/` if you haven't installed Sage or set up a CoCalc account.

(a) Evaluate

```
[BrandtModule(3,5).hecke_matrix(p) for p in [2,3,5,7,11,13]]
```

Verify that these are the same matrices that we saw in class today.

(b) Evaluate

```
[BrandtModule(3,7).hecke_matrix(p) for p in [2,3,5,7,11,13]]
```

Is there anything suspicious about the answer?

(c) In our construction of $G_p(\mathcal{O})$, we constructed a tree and then identified vertices that are related by right multiplication by elements of $\mathbb{H}$. Consider a vertex of the tree, corresponding to a left $\mathcal{O}$-ideal Λ. The set

$$\{z \in \mathbb{H} | \Lambda z = \Lambda\}$$

always contains ± 1. Does anything unusual happen if the set contains elements other than ± 1? Can you use this observation to explain what happens in part (b)?