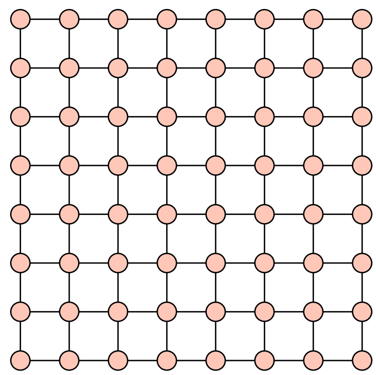
1. Ramanujan graphs

Suppose we are designing a computer network. We would like for there to be a short path from any computer to any other computer. In principle, we could just connect every pair of computers, but that would be expensive. So let's say that we can only afford to connect each computer to, say, four others.



We could try arranging the computers in a square grid, but that is not very effective. There are lots of short paths between two nearby computers, but none between far away computers. We will see that it is possible to do better.

There are various ways of measuring how well-connected a graph is. One of these is by looking at the eigenvalues of its adjacency matrix.

Definition 1.1. Let k be a positive integer. A graph is *k-regular* if there are k edges connected to each vertex.

Definition 1.2. Let G be a graph. The *adjacency matrix* A of G is the matrix with $A_{ij} = 1$ if vertices i and j are connected, and $A_{ij} = 0$ otherwise.

We will write $\lambda_i(G)$ for the ith largest eigenvalue of the adjacency matrix of G.

Here we have used the fact that the eigenvalues of a real symmetric matrix are always real.

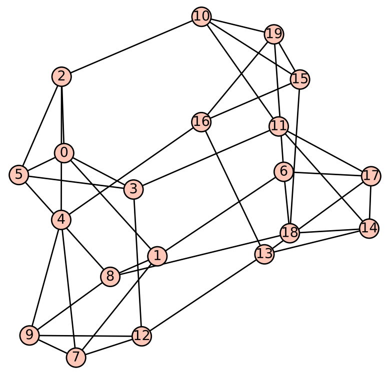
Proposition 1.3 ([Nil91])**.** *Let G be a connected k-regular graph. Suppose that G has two edges of distance at least $2m$ apart. Then*

$$\lambda_2(G) \geq 2\sqrt{k-1} - \frac{2\sqrt{k-1}-1}{m}.$$

In particular, this bound approaches $2\sqrt{k-1}$ as the number of vertices of G goes to infinity.

Definition 1.4. A connected k-regular graph is *Ramanujan* if $|\lambda_i(G)| \leq 2\sqrt{k-1}$ for $i > 1$.

Example 1.5. The following is a 4-regular Ramanujan graph with 20 vertices.



The graph was generated with the following SAGE code:

```
M = BrandtModule(2,175)
G = Graph(M.hecke_matrix(3),format='adjacency_matrix')
G.plot()
```

The following SAGE code computes eigenvalues of the adjacency matrix of G:

```
sorted(G.adjacency_matrix().eigenvalues())
```

We find that the largest nontrivial eigenvalues of the adjacency matrix are ± 3, while the Ramanujan bound is $2\sqrt{3} \approx 3.46$.

Non-example 1.6. A 4×5 wrapping square grid is not Ramanujan. The eigenvalues of its adjacency matrix are of the form $2\cos(2\pi n/4) + 2\cos(2\pi m/5)$. In particular, $2\cos\pi + 2\cos(4\pi/5) = -\frac{5+\sqrt{5}}{4} \approx -3.62$ is an eigenvalue.

Now I will explain the proof of Proposition 1.3. First, we need the following lemma.

Lemma 1.7. *Let A be a real symmetric $n \times n$ matrix. Then $\mathbb{R}^n$ has an orthogonal basis consisting of eigenvectors of A.*

Corollary 1.8 (Variational principle)**.** *Let A be a real symmetric $n \times n$ matrix, and let $e_1, \ldots, e_n$ be an orthogonal basis $\mathbb{R}^n$ consisting of eigenvectors of A, with eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$.*

Choose $m \in \{1, 2, \ldots, n\}$. Let $v \in \mathbb{R}^n$ be a nonzero vector satisfying $e_1^T v, e_2^T v, \ldots e_{m-1}^T v = 0$. Then

$$\lambda_m \geq \frac{v^T A v}{v^T v}\,.$$

Proof. Let $e_1, \ldots, e_n$ be eigenvectors of A that form an orthogonal basis of $\mathbb{R}^n$. Let $\lambda_1, \ldots, \lambda_n$ be the corresponding eigenvalues. WLOG we may assume $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Any $v \in \mathbb{R}^n$ can be written as $a_1 e_1 + \ldots a_n e_n$. Then

$$\frac{v^T A v}{v^T v} = \frac{\sum_{i=1}^n \lambda_i a_i^2}{\sum_{i=1}^n a_i^2} \leq \lambda_1\,.$$

□

Proof of Proposition 1.3. We will apply Corollary 1.8. First, we construct the vector v.

For any vertices x, x' of G, let $d(x, x')$ denote the length of the shortest path from x to x'. Similarly, for any edge e and vertex x of G, let $d(e, x)$ be the length of the shortest path from an endpoint of e to x.

Let e_1, e_2 be edges of G of distance at least $2m$ apart.

Let v_1, v_2 be the vectors defined by

$$v_i(z) = \begin{cases} (k-1)^{-d(e_i,x)/2}, & d(e_i,x) < m \\ 0, & \text{otherwise} \end{cases} .$$

Here $v_i(z)$ denotes the entry of v_i corresponding to the vertex z. Note that, by the triangle inequality, there are no vertices that have distance $< m$ from e_1 and $\leq m$ from e_2. So there are no nonzero entries in common between v_1 and v_2, or between v_1 and Av_2. Then

$$v_1^T v_2 = v_1^T A v_2 = 0 .$$

The eigenvector of A with the largest eigenvalue is $e_1 = (1, 1, \ldots, 1)$. We have $e_1^T v_1, e_1^T v_2 > 0$, so we can find positive reals a_1, a_2 such that $e_1^T(a_1 v_1 - a_2 v_2) = 0$. We will apply Corollary 1.8 to $a_1 v_1 - a_2 v_2$. We have

$$\frac{(a_1v_1 - a_2v_2)^T A (a_1v_1 - a_2v_2)}{(a_1v_1 - a_2v_2)^T (a_1v_1 - a_2v_2)} = \frac{a_1^2 v_1^T A v_1 + a_2^2 v_2^T A v_2}{a_1^2 v_1^T v_1 + a_2^2 v_2^T v_2} \geq \min\left(\frac{v_1^T A v_1}{v_1^T v_1}, \frac{v_2^T A v_2}{v_2^T v_2}\right) .$$

Now observe that

$$k v_i^T v_i - v_i^T A v_i = \sum_{x,x' \in G | d(x,x')=1} (v_i(x) - v_i(x'))^2 .$$

Now, for any nonnegative integer g, $V_{i,s}$ denote the set of vertices having distance s from e_i. Each $x \in V_{i,s}$ has at most $k-1$ neighbors in $V_{i,s+1}$ (one neighbor must be the same distance or closer to e_i). So

$$\begin{aligned} &\sum_{x,x' \in G | d(x,x')=1} (v_i(x) - v_i(x'))^2 \\ \leq &\sum_{s=0}^{m-2} |V_{i,s}|(k-1)\left((k-1)^{-s/2} - (k-1)^{-(s+1)/2}\right)^2 + |V_{i,m-1}|(k-1)(k-1)^{1-m} \\ = &\sum_{s=0}^{m-2} \frac{|V_{i,s}|}{(k-1)^s}(k - 2\sqrt{k-1}) + \frac{|V_{i,m-1}|}{(k-1)^{m-1}}(k-1) \\ = &\sum_{s=0}^{m-1} \frac{|V_{i,s}|}{(k-1)^s}(k - 2\sqrt{k-1}) + \frac{|V_{i,m-1}|}{(k-1)^{m-1}}(2\sqrt{k-1} - 1) . \end{aligned}$$

Since an element of $V_{i,s}$ has at most $k-1$ neighbors in $V_{i+1,s}$, $(k-1)^{-s}|V_{i,s}|$ is a nonincreasing function of s. So in particular,

$$|V_{i,m-1}| \leq \frac{1}{m} \sum_{s=0}^{m-1} |V_{i,s}| .$$

Thus,

$$\begin{aligned} &\sum_{x,x' \in G | d(x,x')=1} (v_i(x) - v_i(x'))^2 \\ \leq &\sum_{s=0}^{m-1} \frac{|V_{i,s}|}{(k-1)^s} \left(k - 2\sqrt{k-1} + \frac{2\sqrt{k-1} - 1}{m}\right) \\ = &v_i^T v_i \left(k - 2\sqrt{k-1} + \frac{2\sqrt{k-1} - 1}{m}\right) . \end{aligned}$$

So, putting everything together, we get

$$kv_i^T v_i - v_i^T A v_i \leq v_i^T v_i \left(k - 2\sqrt{k-1} + \frac{2\sqrt{k-1} - 1}{m} \right)$$

$$v_i^T A v_i \geq v_i^T v_i \left(2\sqrt{k-1} - \frac{2\sqrt{k-1} - 1}{m} \right)$$

$$\lambda_2 \geq 2\sqrt{k-1} - \frac{2\sqrt{k-1} - 1}{m} \, .$$

□

2. Quaternion algebras

Definition 2.1. Let r, s be nonzero rational numbers. The *quaternion algebra* $D_{r,s}$ is the set

$$\{a + bi + cj + dk | a, b, c, d \in \mathbb{Q}\} \ .$$

We give $D_{r,s}$ the structure of a noncommutative ring by defining

$$ij = -ji = k, \quad jk = -kj = si, \quad ki = -ik = rj,$$
$$i^2 = -r, \quad j^2 = -s, \quad k^2 = -rs\,.$$

Definition 2.2. Let D be a quaternion algebra. An *lattice* in D is a subset $\Lambda \subset D$ such that:

(1) Λ is an additive subgroup of D.
(2) Λ both contains and is contained in a set of the form

$$\{a + bi + cj + dk | a, b, c, d \in \lambda\mathbb{Z}\}$$

for $\lambda \in \mathbb{Q}$.

An *order* in D is a lattice of D that is also a subring of D (i.e. it contains 1 and is closed under multiplication).

An order in D is *maximal* if it is not contained in a larger order.

Let $\mathcal{O}$ be a order in D. A *left $\mathcal{O}$-lattice* is an lattice $\Lambda \subset D$ that is closed under left multiplication by $\mathcal{O}$ (for all $x \in \mathcal{O}$, $y \in \Lambda$, $xy \in \Lambda$).

Two left $\mathcal{O}$-lattices Λ_1, Λ_2 are said to be *equivalent* if there is a nonzero $\lambda \in D$ such that $\Lambda_1 = \Lambda_2 \cdot \lambda$. We will write $\Lambda_1 \sim \Lambda_2$ to indicate that Λ_1 and Λ_2 are equivalent.

Definition 2.3. Let Λ be a lattice in a quaternion algebra D. Define

$$\mathcal{O}_\ell(\Lambda) := \{x \in D | x\Lambda \subseteq \Lambda\}$$
$$\mathcal{O}_r(\Lambda) := \{x \in D | \Lambda x \subseteq \Lambda\} \ .$$

We say that Λ is a *left $\mathcal{O}_\ell(\Lambda)$-ideal* and a *right $\mathcal{O}_r(\Lambda)$-ideal*.

A left $\mathcal{O}$-ideal is also a left $\mathcal{O}$-lattice, but the converse is not true. (A left $\mathcal{O}$-ideal is not allowed to be a left $\mathcal{O}'$ lattice for any $\mathcal{O}' \supsetneq \mathcal{O}$.)

Example 2.4. Consider the quaternion algebra $D_{1,3}$. The additive subgroup generated by

$$\frac{1+j}{2}, \quad \frac{i+k}{2}, \quad j, \quad k$$

is a maximal order.

We will consider the (non-maximal) order $\mathcal{O}$ generated by

$$\frac{1+j+4k}{2}, \quad \frac{i+9k}{2}, \quad j+4k, \quad 5k\,.$$

Clearly, $\mathcal{O}$ is a left $\mathcal{O}$-ideal. Let us try to find some more left $\mathcal{O}$-ideals. We will list all of the left $\mathcal{O}$-lattices Λ satisfying $2\mathcal{O} \subset \Lambda \subset \mathcal{O}$. Note that these are in bijection with left ideals of $\mathcal{O}/2\mathcal{O}$ (i.e. additive subgroups of $\mathcal{O}/2\mathcal{O}$ that are stable under left multiplication by $\mathcal{O}/2\mathcal{O}$). It will turn out that all such lattices are left $\mathcal{O}$-ideals.

Lemma 2.5. *Define $\mathcal{O}$ as in Example 2.4. Then $\mathcal{O}/2\mathcal{O} \cong M_2(\mathbb{Z}/2\mathbb{Z})$, the group of 2×2 matrices with coefficients in $\mathbb{Z}/2\mathbb{Z}$.*

Proof. We can check that the map

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{1+2i+3j}{2}a + \frac{i-2j+k}{2}b + \frac{2+i-k}{2}c + \frac{1-2i-3j}{2}d \pmod{2\mathcal{O}}$$

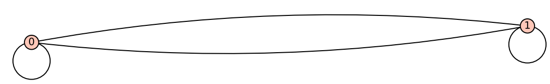
is an isomorphism. (The proof of Lemma 3.7 will explain how we found this isomorphism.) □

For any vector subspace $V \subset (\mathbb{Z}/2\mathbb{Z})^2$, the set of matrices whose rows are in V is a left ideal of $M_2(\mathbb{Z}/2\mathbb{Z})$. In fact, these are the only left ideals of $M_2(\mathbb{Z}/2\mathbb{Z})$.

V	left ideal of $\mathcal{O}/2\mathcal{O}$
0	0
$((1,0))$	$\left(\frac{1+2i+3j}{2}, \frac{2+i-k}{2}\right)$
$((0,1))$	$\left(\frac{1-2j+k}{2}, \frac{1-2i-3j}{2}\right)$
$((1,1))$	$\left(\frac{1+3i+j+k}{2}, \frac{3-i-3j-k}{2}\right)$
V	$\mathcal{O}/2\mathcal{O}$

Then we get three lattices strictly contained in $\mathcal{O}$ and strictly containing $2\mathcal{O}$. The first lattice, corresponding to $((1,0))$, is actually $\mathcal{O} \cdot \frac{2+i-k}{2}$, so it is equivalent to $\mathcal{O}$. Let Λ be the lattice corresponding to $((0,1))$. It turns out that Λ is not equivalent to $\mathcal{O}$. The lattice corresponding to $((1,1))$ is equivalent to Λ. In fact, every left $\mathcal{O}$-lattice is equivalent to $\mathcal{O}$ or Λ.

So, of the lattices strictly containing $\mathcal{O}$ and strictly contained in $2\mathcal{O}$, one is equivalent to $\mathcal{O}$ and two are equivalent to Λ. One can check similarly that, of the lattices strictly containing Λ and strictly contained in 2Λ, two are equivalent to $\mathcal{O}$ and one is equivalent to Λ. We can represent this information in matrix form as $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ or in graph form as:



We can verify these computations in Sage using the following commands.

```
M = BrandtModule(3,5)
M.hecke_matrix(2)
```

Sage is open source, so if you are interested, you can read the source code for Brandt modules to see precisely what it is doing. The code usually contain links to papers that explain the algorithms.

The Ramanujan graph in Example 1.5 was constructed in a similar way. Let $\mathcal{O}$ be the order in $D_{1,1}$ generated by

$$\frac{1+i+7j+5k}{2}, \quad i+7j+5k, \quad 25j+5k, \quad 7k\,.$$

Then there are 20 equivalence classes of left $\mathcal{O}$-ideals $\Lambda_1, \ldots, \Lambda_{20}$. Let $B_3(\mathcal{O})$ be the matrix whose ij entry is the number of lattices Λ' such that Λ' is equivalent to Λ_i and $\Lambda_j \supsetneq \Lambda' \supsetneq 3\Lambda_j$. Then $B_3(\mathcal{O})$ is the adjacency matrix of the graph in Example 1.5.

Recall that we used the following Sage commands in Example 1.5:

```
M = BrandtModule(2,175)
G = Graph(M.hecke_matrix(3),format='adjacency_matrix')
```

The '2' specifies the quaternion algebra (I will explain in the next lecture why 2 corresponds to $D_{1,1}$), the '175' specifies the order inside the quaternion algebra (we choose an order $\mathcal{O}$ so that there is a maximal order $\mathcal{O}_{\max}$ satsfying $\mathcal{O}_{\max}/\mathcal{O} \cong (\mathbb{Z}/175\mathbb{Z})^2$), and the '3' specifies that we are looking for pairs of left $\mathcal{O}$-ideals Λ_1, Λ_2 so that $\Lambda_1 \supsetneq \Lambda_2 \supsetneq 3\Lambda_1$.

If you play around with Brandt modules in Sage, you may notice that unusual things happen sometimes.

```
M = BrandtModule(11)
M.hecke_matrix(2)
```

Sage prints out the matrix $\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$. This matrix is not symmetric, so it is not the adjacency matrix of an undirected graph. To understand why the matrix is usually symmetric, but isn't in this particular case, we will have to introduce some more theory.

3. Constructing Ramanujan graphs

Definition 3.1. The *conjugate* of an element of $D_{r,s}$ is defined by

$$(a + bi + cj + dk)^* := a - bi - cj - dk\,.$$

The *trace* of an element of $D_{r,s}$ is defined by $\operatorname{tr} z := z + z^*$, i.e.

$$\operatorname{tr}(a + bi + cj + dk) := 2a\,.$$

The *norm* of an element of $D_{r,s}$ is defined by $N(z) := zz^*$, i.e.

$$N(a + bi + cj + dk) := a^2 + rb^2 + sc^2 + rsd^2\,.$$

Lemma 3.2. *For $z, z' \in D_{r,s}$, $(zz')^* = z'^* z^*$, $\operatorname{tr}(z + z') = \operatorname{tr}(z) + \operatorname{tr}(z')$, and $N(zz') = N(z)N(z')$.*

Definition 3.3. Let Λ be a lattice in $D_{r,s}$, generated as an abelian group by x_1, x_2, x_3, x_4. The *discriminant* of Λ, denoted $\Delta(\Lambda)$ is the determinant of the matrix with entries $\operatorname{tr}(x_i x_j)$.

Lemma 3.4. *Let $\mathcal{O}$ be an order in a quaternion algebra D. For every $z \in \mathcal{O}$, $\operatorname{tr}(z)$ and $N(z)$ are integers, and $z^* \in \mathcal{O}$.*

Proof. Since $\mathcal{O}$ is a lattice, the norms of elements of $\mathcal{O}$ have bounded denominators. If $z \in \mathcal{O}$, then every power of $N(z)$ is a norm of an element of $\mathcal{O}$. So $N(z)$ must be an integer. Similarly, $N(z+1) = (z+1)(z^*+1) = zz^* + z + z^* + 1 = N(z) + \operatorname{tr}(z) + 1$ must be an integer. We have $z^* = \operatorname{tr} z - z \in \mathcal{O}$ since all integers are in $\mathcal{O}$. $\square$

Definition 3.5. Let $\mathcal{O}$ be an order in a quaternion algebra D, and let p be a prime number. We say that $\mathcal{O}$ is *unramified at p* if p does not divide the discriminant of $\mathcal{O}$.

Lemma 3.6 (Chevalley)**.** *Let p be a prime number. Let $Q(x_1, x_2, x_3)$ be a quadratic form in three variables with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Then there exist $x_1, x_2, x_3 \in \mathbb{Z}/p\mathbb{Z}$, not all zero, so that $Q(x_1, x_2, x_3) = 0$.*

Proof. We will show that the number of solutions to $Q(x_1, x_2, x_3) = 0$ is divisible by p. In particular, $(0, 0, 0)$ cannot be the only solution.

By Fermat's little theorem, if $Q(x_1, x_2, x_3) \neq 0$, then $Q(x_1, x_2, x_3)^{p-1} = 1$. So the number of solutions to $Q(x_1, x_2, x_3) = 0$ is congruent mod p to $\sum_{x_1,x_2,x_3 \in \mathbb{Z}/p\mathbb{Z}} 1 - Q(x_1, x_2, x_3)^{p-1}$. This polynomial has total degree $2(p-1) < 3(p-1)$. So in each term, the degree of either x_1, x_2, or x_3 must be strictly less than $p - 1$. We claim that $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^d = 0$ for all $d < p - 1$. Indeed,for any nonzero $y \in \mathbb{Z}/p\mathbb{Z}$, $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^d = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (xy)^d = y^d \sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^d$, and we can find some y so that $y^d \neq 1$. So $\sum_{x_1,x_2,x_3 \in \mathbb{Z}/p\mathbb{Z}} 1 - Q(x_1, x_2, x_3)^{p-1}$ must be divisible by p. $\square$

Lemma 3.7. *Let $\mathcal{O}$ be an order in a quaternion algebra D. Let p be a prime number such that $\mathcal{O}$ is unramified at p. Then $\mathcal{O}/p\mathcal{O}$ is isomorphic to the set of 2×2 matrices over $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Consider the space of elements of $\mathcal{O}/p\mathcal{O}$ with trace zero. It is a three-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. By Lemma 3.6, we can find $x \in \mathcal{O}/p\mathcal{O}$ with $\operatorname{tr} x = 0$ and $N(x) = 0$. Then also $x^2 = -x(\operatorname{tr} x - x) = -N(x) = 0$. By the nondegeneracy of the trace map, there must exist z so so that $\operatorname{tr} xz = 1$. Let

$y = xz$. Then the trace pairing on $(1, x, y, z)$ is given by a matrix $\begin{pmatrix} 2 & 0 & 1 & ? \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & ? \\ ? & 1 & ? & ? \end{pmatrix}$.
This matrix has determinant -1 (regardless of the unknown entries), so $1, x, y, z$ must be linearly independent. We leave it to the reader to verify that the map $\mathcal{O}/p\mathcal{O} \to M_2(\mathbb{Z}/p\mathbb{Z})$ sending

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad x \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad z \mapsto \begin{pmatrix} \mathrm{tr}(yz) & -N(z) \\ 1 & 0 \end{pmatrix}$$

is an isomorphism. □

Corollary 3.8. *Let $\mathcal{O}$ be an order in a quaternion algebra D, and let Λ be a left $\mathcal{O}$-lattice. Let p be a prime number such that $\mathcal{O}$ is unramified at p. Then the set of left $\mathcal{O}$-lattices Λ' satisfying $\Lambda \supsetneq \Lambda' \supsetneq p\Lambda$ is in bijection with the set of one-dimensional subspaces of $(\mathbb{Z}/p\mathbb{Z})^2$. In particular, this set has $p+1$-elements.*

If Λ is a left $\mathcal{O}$-ideal, then the Λ' are as well.

Definition 3.9. Let Λ_1, Λ_2 be left $\mathcal{O}$-lattices. Let $\mathrm{Hom}_{\mathcal{O}}(\Lambda_1, \Lambda_2)$ denote the set of left $\mathcal{O}$-linear maps $\Lambda_1 \to \Lambda_2$.

For $f \in \mathrm{Hom}_{\mathcal{O}}(\Lambda_1, \Lambda_2)$ nonzero, define the *degree* of f by

$$\deg f := \sqrt{[\Lambda_2 : f(\Lambda_1)]}$$

if $f \neq 0$ and $\deg 0 = 0$.

For any nonnegative integer m, let $\mathrm{Hom}_{\mathcal{O}}(\Lambda_1, \Lambda_2)_m$ be the subset of $\mathrm{Hom}_{\mathcal{O}}(\Lambda_1, \Lambda_2)$ consisting of those maps of degree m.

We will write $\mathrm{Aut}_{\mathcal{O}}(\Lambda)$ for $\mathrm{Hom}_{\mathcal{O}}(\Lambda, \Lambda)_1$.

Lemma 3.10. *Let Λ_1, Λ_2 be left $\mathcal{O}$-lattices. Then any left $\mathcal{O}$-linear map $f\colon \Lambda_1 \to \Lambda_2$ is of the form $x \mapsto xy$ for some $y \in D$. Furthermore, $\deg f = N(y)(\Delta(\Lambda_1)/\Delta(\Lambda_2))^{1/4}$.*

Definition 3.11. The quaternion algebra $D_{r,s}$ is *definite* if $r, s > 0$ (equivalently, every nonzero element of $D_{r,s}$ has positive norm).

Lemma 3.12. *Let $\mathcal{O}$ be an order in a definite quaternion algebra. For any left $\mathcal{O}$-ideals Λ_1, Λ_2 and any nonnegative integer m, $\mathrm{Hom}_{\mathcal{O}}(\Lambda_1, \Lambda_2)_m$ is a finite set.*

From now on, we will assume that our quaternion algebras are definite.

Lemma 3.13. *Let Λ_1, Λ_2 be left $\mathcal{O}$-ideals. Let p be a prime number, and assume $\mathcal{O}$ is unramified at p. Then the number of left $\mathcal{O}$-ideals Λ' such that $\Lambda' \sim \Lambda_1$ and $\Lambda_2 \supsetneq \Lambda_1 \supsetneq p\Lambda_2$ is*

$$\frac{|\,\mathrm{Hom}_{\mathcal{O}}(\Lambda_1, \Lambda_2)|}{|\,\mathrm{Aut}_{\mathcal{O}}(\Lambda_1)|}\,.$$

Lemma 3.14. *For any left $\mathcal{O}$-ideals Λ_1, Λ_2 and any positive integer m,*

$$|\,\mathrm{Hom}_{\mathcal{O}}(\Lambda_1, \Lambda_2)_m| = |\,\mathrm{Hom}_{\mathcal{O}}(\Lambda_2, \Lambda_1)_m|\,.$$

Proof. For any $f \in \mathrm{Hom}_{\mathcal{O}}(\Lambda_1, \Lambda_2)_m$, $m\Lambda_2 \subseteq f(\Lambda_1)$. So $f^* = f^{-1} \cdot (\deg f)$ defines a map $\Lambda_2 \to \Lambda_1$ of degree m. One can check that $(f^*)^* = f$. So * defines a bijection between $\mathrm{Hom}_{\mathcal{O}}(\Lambda_1, \Lambda_2)_m$ and $\mathrm{Hom}_{\mathcal{O}}(\Lambda_2, \Lambda_1)_m$. □

Definition 3.15. We say that $\mathcal{O}$ is *neat* if no left $\mathcal{O}$-ideal has an automorphism other than $\pm\,\mathrm{id}$ (equivalently, for any left $\mathcal{O}$-ideal Λ, $\mathcal{O}_r(\Lambda)^\times = \{\pm 1\}$).

Definition 3.16. Let $\mathcal{O}$ be an order in a quaternion algebra D, and let m be a nonnegative integer. Let $\Lambda_1, \ldots, \Lambda_n$ be representatives of the set of equivalence classes of left $\mathcal{O}$-ideals.

For any nonnegative integer m, define the *Brandt matrix* $B_m(\mathcal{O})$ to be the matrix whose ij entry is $\frac{|\operatorname{Hom}_{\mathcal{O}}(\Lambda_i, \Lambda_j)|}{|\operatorname{Aut}(\Lambda_i)|}$.

If $\mathcal{O}$ is neat, then $B_m(\mathcal{O})$ is symmetric. Define the *Brandt graph* $G_m(\mathcal{O})$ to be the (multi)graph whose adjacency matrix is the Brandt matrix $B_m(\mathcal{O})$.

Theorem 3.17. *If p is a prime unramified in $\mathcal{O}$, then the Brandt graph $G_p(\mathcal{O})$ is Ramanujan.*

Unfortunately, I will not be able to give a proof of this theorem. The proof requires some rather technical ingredients, including algebraic geometry in characteristic p. However, I will explain a part of the proof, which is a connection between Brandt matrices and modular forms.

4. Theta functions and the Ramanujan–Petersson conjecture

Let $\mathcal{O}$ be as in Example 2.4. There are two equivalence classes of left $\mathcal{O}$-ideals, so the Brandt matrices $B_m(\mathcal{O})$ are two-dimensional. For each m, the vectors $\begin{pmatrix}1\\1\end{pmatrix}$ and $\begin{pmatrix}1\\-1\end{pmatrix}$ are eigenvectors. The eigenvalues of the $B_m(\mathcal{O})$ acting on $\begin{pmatrix}1\\-1\end{pmatrix}$ are

$$1,\ -1,\ -1,\ -1,\ 1,\ 1,\ 0,\ 3,\ 1,\ -1,\ -4,\ \ldots .$$

Now consider the power series

$$\begin{aligned} g(q) &= q\prod_{n=1}^{\infty}(1-q^n)(1-q^{3n})(1-q^{5n})(1-q^{15n}) \\ &= q - q^2 - q^3 - q^4 + q^5 + q^6 + 3q^8 + q^9 - q^{10} - 4q^{11} + \cdots \end{aligned}$$

The coefficients of this power series are the smame as the eigenvalues of $B_m(\mathcal{O})$. This is not a coincidence!

Let us mention another surprising fact about $g(q)$: it is a modular form.

Definition 4.1. Let k be a nonnegative integer, and let N be a positive integer. A holomorphic function f on the upper half complex plane is a *modular function* of weight k and level $\Gamma_0(N)$ if, for any integers a, b, c, d satisfying $ad - bc = 1$ and $N \mid c$,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)\,.$$

We say that f is a *cuspidal modular form* if, in addition, $\lim_{z\to t} f(z) = 0$ for any $t \in \mathbb{Q}\cup\{\infty\}$.

We write $S_k(\Gamma_0(N))$ for the space of all cuspidal modular forms of weight k and level $\Gamma_0(N)$.

Proposition 4.2.

$$g(e^{2\pi iz}) \in S_2(\Gamma_0(15))\,.$$

This is not at all obvious. There is a proof using Fourier analysis and a proof using complex analysis. I will give some references below when I state a more general theorem.

We can also iterpret the coefficients of f as eigenvalues of operators called *Hecke operators*. Let p be a prime number. Let T_p to be the operator defined by $T_p(\sum a_n q^n) = \sum b_n q_n$ where

$$b_n = \begin{cases} a_{pn} + p a_{n/p}, & p \mid n \\ a_{pn}, & p \nmid n\,. \end{cases}$$

Let's compute $T_2(g)$.

$$T_2(g) = -q + q^2 + q^3 + q^4 - q^5 + \cdots . = -g\,.$$

Every element of $S_k(\Gamma_0(N))$ has an expansion of the form $f(z) = \sum_{n=1}^{\infty} a_n q^n$, where $q = e^{2\pi iz}$. One can show that whenever $p \nmid N$, T_p preserves $S_k(\Gamma_0(N))$. Furthermore, $S_2(\Gamma_0(15))$ is one-dimensional. Therefore, g is an eigenvector of T_p for $p \notin \{3, 5\}$. The coefficient of q^1 in f is 1, while the cofficient of q^1 in $T_p g$ is the same as the coefficient of q^p in g. Therefore, the T_p-eigenvalue is the coefficient of q^p.

Theorem 4.3 (Ramanujan–Petersson conjecture)**.** *Let $k \geq 2$ and N be positive integers. Let p be a prime not dividing N. Then the eigenvalues of T_p acting on $S_k(\Gamma_0(N))$ satisfy*

$$|\lambda| \leq 2p^{(k-1)/2}\,.$$

The conjecture was proved by Eichler for $k = 2$ and by Deligne for all k. The proof uses some techniques (in particular, algebraic geometry over $\mathbb{Z}/p\mathbb{Z}$) that I will not be able to cover in this course.

In particular, when $k = 2$, we get $|\lambda| \leq 2\sqrt{p}$. To prove that the graph $G_p(\mathcal{O})$ is Ramanujan, one constructs cuspidal modular forms whose T_p-eigenvalues are the nontrivial eigenvalues of $B_p(\mathcal{O})$. The Ramanujan–Petersson conjecture then implies that $G_p(\mathcal{O})$ is Ramanujan. Let us now explain how these modular forms are constructed.

Definition 4.4. Define a matrix-valued function on the upper half complex plane by

$$\theta_{\mathcal{O}}(z) = \sum_{n=0}^{\infty} B_n(\mathcal{O}) \exp(2\pi i n z)\,.$$

Proposition 4.5. *Let*

$$\mathcal{O}^* := \{x \in D | \operatorname{tr} xy \in \mathbb{Z} \textit{ for all } y \in \mathcal{O}\}\,.$$

Let N be the smallest positive integer such that $N\mathcal{O}^* \subseteq \mathcal{O}$. The entries of $\theta_{\mathcal{O}}$ are modular functions of weight 2 and level $\Gamma_0(N)$: for any integer matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfying $ad - bc = 1$ and $N \mid c$,

$$\theta_{\mathcal{O}}\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 \theta_{\mathcal{O}}(z)\,.$$

For a proof, see [Shi73, Proposition 2.1]. You may find it useful to read about the simpler case of the Jacobi theta function first. Some good references are [Bel61, Cou03].

Proposition 4.6. *Let e be an eigenvector of the $B_p(\mathcal{O})$ with real entries. Define a function θ_e on the upper half complex plane by*

$$\theta_e(z) = e^T \theta_{\mathcal{O}}(z) e\,.$$

Then $\theta_e(z) \neq 0$ and $T_p\theta_e(z) = \lambda\theta_e(z)$. If $\lambda \neq p$, then $\theta_e(z)$ is a cuspidal modular form.

Proof. To see that $\theta_e(z) \neq 0$, observe that the coefficient of $\exp(2\pi i z)$ in $\theta_e(z)$ is $e^T B_1(\mathcal{O}) e = e^T e > 0$.

To see that $\theta_e(z) \to 0$ as $z \to \infty$, recall that e is orthogonal to the eigenvector $e_1 = (1, \ldots, 1)$, which has eigenvalue p. As $z \to \infty$, $\theta_e(z)$ approaches $e^T B_0(\mathcal{O}) e = \frac{1}{2} e^T (e_1 e_1^T) e = 0$. To show that $\theta_e(z) \to 0$ as z approaches a rational number, use [Shi73, (2.8)] to relate this limit as the limit as $z \to \infty$. $\square$

The fact that $G_p(\mathcal{O})$ is Ramanujan is then a consequence of the Ramanujan–Petersson conjecture.

References

[Bel61] R. Bellman. *A brief introduction to theta functions*. Athena Series: Selected Topics in Mathematics. Holt, Rinehart and Winston, New York, 1961.

[Cou03] W. Couwenberg. A simple proof of the modular identity for theta functions. *Proc. Amer. Math. Soc.*, 131(11):3305–3307, 2003.

[Nil91] A. Nilli. On the second eigenvalue of a graph. *Discrete Math.*, 91(2):207–210, 1991.

[Shi73] G. Shimura. On modular forms of half integral weight. *Ann. of Math. (2)*, 97:440–481, 1973.