Математичка гимназија

МАТУРСКИ РАД

- из математике -

Раманујанови графови

Ученик:
Ирина Ђанковић IVд

Ментор:
др Соња Чукић

Београд, јун 2020.

Садржај

1

Увод

Тема овог рада ће бити проналажење графова који су добро повезани, а имају релативно мали број ивица – такозваних *експандера*. Брзо је уочено да су експандери уско повезани са графовима који имају велики хроматски број и велику дужину најкраћег циклуса. Ердош је још 1959. године доказао пробабилистичким методама постојање графова са великим хроматским бројем и великом дужином најкраћег циклуса [E], а комбинаторним пребројавањем Пинскер [P] је показао да експандери постоје, но дуго након тога није пронађена експлицитна конструкција. Прве експлицитне конструкције дали су скоро истовремено Лубоцки, Филипс и Сарнак у [LPS] и Маргулис [M1], [M2] 1988. године. И не само да су дали експлицитну конструкцију, већ су се њихови графови показали као оптимални експандери – тзв. Раманујанови графови. У овом раду изложићемо конструкцију Лубоцког, Филипса и Сарнака, која је сама по себи елементарна, али доказ да ти графови јесу оптимални добро повезани графови са мало ивица, залази у теорију *модуларних форми*. Ова теорија је срж великог броја дубоких резултата математике двадесетог и двадесет првог века – на пример, Ендру Вајлс је користио ову теорију у свом доказу Велике Фермаове Теореме! Једну од најважнијих хипотеза о модуларним формама формулисао је индијски математичар Раманујан још почетком двадесетог века. Ову хипотезу је доказао Делињ тек 1974. године, као последицу његовог доказа Вејлових хипотеза за који је добио Филдсову медаљу. Срж доказа да наши графови јесу оптимални експандери је баш оцена из Раманујанове хипотезе, па отуда и њихово име. Упркос томе, моћи ћемо да докажемо да конструисани графови јесу добро повезани и да имају мали број ивица користећи не толико напредне алате.

Проучимо мало боље наше захтеве. Посматрајмо наш граф као телекомуникациону мрежу. Природно је да желимо што бољу повезаност мреже, и можемо тако нешто остварити са, на пример, комплетним графом. Но, у стварном свету морамо узети у обзир и трошкове прављења те мреже - за комплетан граф број ивица расте квадратно са бројем чворова. Дакле, желимо да пронађемо графове којима број ивица расте отприлике линеарно са бројем чворова, а добро су повезани.

Сада кад смо објаснили шта значи мали број ивица, природно се намеће питање шта значи да је граф добро повезан? Уведимо следећу величину која ће нумерички

окарактерисати повезаност графа.

Дефиниција 1.1. Нека је $X(V, E)$ неусмерен прост граф (између свака два чвора постоји највише једна ивица). Онда је *изопериметријска константа* или *константа експанзије* графа X, у ознаци $h(X)$, дефинисана на следећи начин:

$$h(X) = \inf \left\{ \frac{|\partial F|}{\min\{|F|, |V - F|\}} : F \subseteq V, 0 < |F| < +\infty \right\},$$

при чему је ∂F граница подскупа F скупа чворова V графа G дефинисана као скуп свих ивица са једним крајем у F, а другим у $V - F$.

Погледајмо сад на примерима како се понаша изопериметријска константа. Ако је K_n комплетан граф са n чворова онда је $|\partial F| = |F|(n - |F|)$ тј. $h(K_n) = n - \lfloor \frac{n}{2} \rfloor \sim \frac{n}{2}$. Насупрот добро повезаном комплетном графу, за циклус дужине n, C_n важи $|\partial F| = 2 \Rightarrow h(C_n) \leqslant \frac{2}{[\frac{n}{2}]} \sim \frac{4}{n}$, наиме $h(C_n) \to 0$ када $n \to \infty$.

Наредно поглавље овог рада посвећено је претварању тражених комбинаторних својстава у нумеричке услове, које ћемо релативно лако моћи да израчунамо. У другом поглављу ћемо такође дефинисати шта значи да је неки граф оптималан експандер, односно да је неки граф Раманујанов. У трећем поглављу налази се целокупна теоријска припрема за конструкцију Раманујанових графова, као и сама конструкција, док се у последњем поглављу налази доказ.

Посебну захвалност дугујем свом ментору др Соњи Чукић на корисним саветима, али пре свега на посвећеним и инспиративним предавањима и математичком знању којим је обогатила моје четворогодишње школовање и мотивисала моје будуће изборе.

2

Графови и њихов спектар

2.1 Матрица повезаности и спектар графа

У овом поглављу ћемо граф, као комбинаторни објекат, окарактерисати нумерички уз помоћ линеарне алгебре. Посматраћемо графове $X = (V, E)$ где је V скуп чворова, а E скуп ивица (грана). У овом раду увек ћемо посматрати неусмерене графове и наши графови ће најчешће бити коначни.

Дефиниција 2.1. Нека је $V = \{v_1, v_2, v_3, ...\}$ скуп чворова нашег графа. Онда је *матрица повезаности* графа X матрица A индексирана по $v_i, v_j \in V$ тако да је $A = (A_{ij})$ при чему је $A_{ij} =$ број ивица које повезују v_i са v_j.

Граф је *прост* ако постоји највише једна ивица између свака два чвора. Преведено на језик матрице повезаности, сваки елемент матрице припада скупу $\{0, 1\}$. Додатно, граф не садржи петље ако и само ако је $\forall v_i \in V \quad A_{ii} = 0$.

Дефиниција 2.2. Нека је $k \geqslant 2$ природан број. Граф $X(V, E)$ је k-регуларан ако за све $v_i, v_j \in V$ важи $\sum_{v_j \in V} A_{ij} = k$.

Ако граф нема петље, ово значи да сваки чвор има тачно k суседа.

Претпоставимо надаље да је граф X коначан и да има n чворова, $n \in \mathbb{N}$. Онда је његова матрица повезаности симетрична $n \times n$ матрица. Дакле, пошто су симетричне матрице дијагонализабилне, матрица повезаности има n реалних сопствених вредности рачунајући вишеструкости и n одговарајућих сопствених вектора који чине ортонормирану базу. Те сопствене вредности можемо поређати у опадајућем редоследу на следећи начин:

$$\mu_0 \geqslant \mu_1 \geqslant \mu_2 \geqslant \cdots \geqslant \mu_{n-1}.$$

Скуп сопствених вредности матрице повезаности A се назива *спектар* графа X.

За произвољан граф $X(V, E)$ посматрајмо све функције $f : V \to \mathbb{R}$ из скупа чворова у скуп реалних бројева и дефинишимо простор

$$\ell^2(V) = \{f : V \to \mathbb{R} \mid \sum_{v \in V} |f(v)|^2 < +\infty\}.$$

Простор $\ell^2(E)$ се дефинише аналогно.

Јасно је да, уколико је V коначан, тј. $|V| = n$, свака функција $f : V \to \mathbb{R}$ припада $\ell_2(V)$. Штавише, сваку функцију можемо посматрати као вектор у $\mathbb{R}^n$.

$$Af = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix} \begin{pmatrix} f(v_1) \\ f(v_2) \\ \vdots \\ f(v_n) \end{pmatrix} = \begin{pmatrix} A_{11}f(v_1) + A_{12}f(v_2) + \cdots + A_{1n}f(v_n) \\ A_{21}f(v_1) + A_{22}f(v_2) + \cdots + A_{2n}f(v_n) \\ \vdots \\ A_{n1}f(v_1) + A_{n2}f(v_2) + \cdots + A_{nn}f(v_n) \end{pmatrix}$$

Дакле знамо да је $(Af)(v_i) = \sum_{j=1}^{n} A_{ij} f(v_i)$. Надаље ћемо, ради једноставности записа, индексе у матрици повезаности поистоветити са чворовима графа тј. за $x, y \in V$ матрица повезаности A је $(A_{xy})_{x,y \in V}$. У оваквом запису претходна формула постаје $(Af)(x) = \sum_{y \in V} A_{xy} f(y)$ за $x \in V$.

Теорема 2.1. Нека је X коначан k-регуларан граф са n чворова. Онда је:

(1) $\mu_0 = k$,

(2) $|\mu_i| \leqslant k$ за $1 \leqslant i \leqslant n-1$,

(3) μ_0 има вишеструкост 1 ако и само ако је граф X повезан.

Доказ: Уочимо најпре да је $f \equiv 1$ сопствени вектор наше матрице повезаности чија је сопствена вредност баш k. Сада докажимо да су све сопствене вредности матрице A по апсолутној вредности мање или једнаке од k и тиме ћемо доказати прва два тврђења.

Нека је f сопствени вектор који одговара сопственој вредности μ. Нека је $x \in V$ такав да је

$$|f(x)| = \max_{y \in V} |f(y)|.$$

Замењујући f са $-f$ уколико је то потребно, можемо претпоставити да је $f(x) > 0$ (важи строга неједнакост јер би у супротном f био нула вектор, што је немогуће јер је он сопствени вектор). Онда је:

$$f(x)|\mu| = |f(x)\mu| = |\sum_{y \in V} A_{xy} f(y)| \leqslant \sum_{y \in V} A_{xy} |f(y)| \leqslant f(x) \sum_{y \in V} A_{xy} = f(x)k.$$

Скраћивањем члана $f(x)$ са обе стране неједнакости добијамо тражену неједнакост.

Докажимо сада тврђење (3). Најпре претпоставимо да је X повезан. Нека је f произвољан сопствени вектор који одговара сопственој вредности k. Како смо већ доказали да је $f_0 \equiv 1$ сопствени вектор за сопствену вредност k, довољно је да докажемо да је f константан вектор тј. линеарно зависан од f_0. Нека је, као и раније, $x \in V$ такав да је $|f(x)| = \max_{y \in V} |f(y)|$. Онда је:

$$f(x) = \frac{Af(x)}{k} = \sum_{y \in V} \frac{A_{xy}}{k} f(y).$$

Приметимо и да је $\sum_{y\in V}\frac{A_{xy}}{k}\cdot 1 = 1$ јер је $f_0 \equiv 1$ сопствени вектор за k, што значи да је $f(x)$ написано као конвексна комбинација реалних бројева $f(y)$ који су сви по апсолутној вредности мањи или једнаки $f(x)$. То значи да је $f(x) = f(y)$ за све y за које $A_{xy} \neq 0$, тј. за све y који су повезани са x. Истим аргументом функција f узима вредност $f(x)$ и за све чворове који су суседи таквих y итд. Како је граф X повезан, евентуално добијамо да функција f узима вредност $f(x)$ на свим чворовима, тј. константна је, чиме завршавамо овај смер.

Други смер тврђења (3) ћемо доказати контрапозицијом. Претпоставимо да X није повезан. Онда постоје дисјунктни непразни подскупови $V_1, V_2 \subseteq V$ такви да за сваке $v_1 \in V_1, v_2 \in V_2$ ивица $\{x, y\}$ није у E. Посматрајмо функцију f дефинисану на следећи начин:

$$f(x) = \begin{cases} 1, & x \in V_1; \\ -1, & x \in V_2. \end{cases}$$

За њу важи:

$$x \in V_1 \ : \ Af(x) = \sum_{y\in V} A_{xy}f(y) = \sum_{y\in V_1} A_{xy}f(y) = f(x)\sum_{y\in V_1} A_{xy} = f(x)k.$$

Иста ова једнакост важи и за $x \in V_2$, те је овако дефинисано f сопствени вектор за вредност k. Но поново, константна функција је сопствени вектор за k, па смо нашли два независна вектора за која важи $Af = kf \Rightarrow \mu_0$ има вишеструкост бар 2, контрадикција. Овиме завршавамо наш доказ. □

Дефиниција 2.3. Граф је *бипартитан* уколико постоји партиција скупа чворова $V = V_+ \cup V_-$ таква да за све чворове x, y за које је $A_{xy} \neq 0$, важи ако $x \in V_+$ ($x \in V_-$) онда $y \in V_-$ ($y \in V_+$).

Дакле граф је бипартитан ако чворове можемо обојити у две боје тако да никоја два чвора исте боје нису суседни. Наведимо сад пар својстава спектра бипартитних графова.

Теорема 2.2. Нека је X повезан k-регуларан граф са n чворова. Онда су следећи искази еквивалентни:

(1) граф X је бипартитан,

(2) спектар графа X је симетричан око 0,

(3) $\mu_{n-1} = -k$.

Доказ. (1) $\Rightarrow$ (2) Нека је $V = V_+ \cup V_-$ одговарајућа партиција графа X. Нека је f сопствени вектор који одговара некој фиксираној сопственој вредности μ. Нека је

$$g(x) = \begin{cases} f(x), & x \in V_+; \\ -f(x), & x \in V_-. \end{cases}$$

Лако се показује да је $(Ag)(x) = -\mu g(x)$, што значи да је спектар графа симетричан око нуле.
(2) $\Rightarrow$ (3) Овај смер је тривијалан користећи теорему 2.1.
(3) $\Rightarrow$ (1) Нека је f сопствена функција која одговара сопственој вредности $-k$. Нека је $x \in V$ такав да је $|f(x)| = \max_{y\in V} |f(y)|$. Замењујући f са $-f$ уколико је то потребно, можемо претпоставити да је $f(x) > 0$. Онда је:

$$f(x) = -\frac{Af(x)}{k} = -\sum_{y\in V} \frac{A_{xy}}{k} f(y) = \sum_{y\in V} \frac{A_{xy}}{k}(-f(y)).$$

Сада смо написали $f(x)$ као конвексну комбинацију бројева који нису већи од њега, дакле они му морају баш бити једнаки - за сваки чвор y који је повезан са чвором x важи да је $f(x) = -f(y)$. Поново се за сваки такав чвор y достиже максимум функције $|f|$ те и сваки њихов сусед z задовољава $f(y) = -f(z)$ итд. Како је наш граф повезан евентуално ћемо на овај начин обићи све чворове и природно се намеће партиција скупа чворова $V = V_+ \cup V_-$ где је $V_+ = \{v \in V : f(v) > 0\}$, а $V_- = \{v \in V : f(v) < 0\}$. Очигледно су све гране графа између чворова из V_+ и V_- чиме завршавамо наш доказ. □

Дакле доказали смо да је за сваки коначан повезан k-регуларан граф X највећа сопствена вредност његове матрице повезаности баш k. Додатно, уколико је X и бипартитан његова најмања сопствена вредност је $-k$. Сопствене вредности k и $-k$, ако се $-k$ појављује, називамо *тривијалним*. Разлика $\mu_0 - \mu_1 = k - \mu_1$ се назива *спектрални размак* графа X.

2.2 Оцене спектралног размака

Нека је $X(V, E)$ граф и нека је $F \subseteq V$. Присетимо се дефиниције границе скупа F и изопериметријске константе графа X.

Дефиниција 2.4. Нека је $X(V, E)$ неусмерен прост граф (између свака два чвора постоји највише једна ивица). Онда је *изопериметријска константа* или *константа експанзије* графа X, у ознаци $h(X)$, дефинисана на следећи начин:

$$h(X) = \inf\left\{\frac{|\partial F|}{\min\{|F|, |V - F|\}} : F \subseteq V, 0 < |F| < +\infty\right\},$$

при чему је ∂F граница подскупа F скупа чворова V графа G дефинисана као скуп свих ивица са једним крајем у F, а другим у $V - F$.

Како ћемо у току већине рада посматрати коначне графове вреди напоменути да за њих ова дефиниција изгледа нешто једноставније:

$$h(X) = \min\left\{\frac{|\partial F|}{|F|} : F \subseteq V, 0 < |F| \leqslant \frac{|V|}{2}\right\}.$$

Дефиниција 2.5. Нека је $(X_m)_{m\geqslant 1}$ фамилија коначних, повезаних, k-регуларних графова, при чему $|V_m| \to +\infty$ када $m \to +\infty$. Кажемо да је $(X_m)_{m\geqslant 1}$ *фамилија експандера* ако постоји $\varepsilon > 0$ за које је $h(X_m) \geqslant \varepsilon$ за свако $m \geqslant 1$.

Теорема 2.3. Нека је $X = (V, E)$ коначан, повезан k-регуларан граф који не садржи петље. Нека је μ_1 прва нетривијална сопствена вредност матрице повезаности графа X. Онда важи:

$$\frac{k-\mu_1}{2} \leqslant h(X) \leqslant \sqrt{2k(k-\mu_1)}.$$

Доказ. Почнимо од прве неједнакости. Доделимо најпре свакој ивици из E насумичну оријентацију. Приметимо да је на овај начин свакој ивици додељен њен почетак e_- и крај e_+. Сада можемо дефинисати оператор $d : \ell^2(V) \to \ell^2(E)$, где је за $f \in \ell^2(V)$ и $e \in E$,

$$df(e) = f(e_+) - f(e_-).$$

Имајући на уму да је $\ell^2(V)$ заправо реалан векторски простор коначне димензије, користићемо стандардни скаларни производ

$$\langle f, g\rangle = \sum_{x\in V} f(x)g(x).$$

Аналогно дефинишимо и скаларни производ у $\ell^2(E)$. Дефинишимо и адјунговани оператор $d^* : \ell^2(E) \to \ell^2(V)$ за који важи $\langle df, g\rangle = \langle f, d^*g\rangle \quad \forall f \in \ell^2(V), g \in \ell^2(E)$. Нека је $\delta : V \times E \to \{-1, 0, 1\}$ индикаторска функција таква да је за $x \in V, e \in E$:

$$\delta(x,e) = \begin{cases} 1, & x = e_+; \\ -1, & x = e_-; \\ 0, & \text{у осталим случајевима.} \end{cases}.$$

Лако се проверава да је за $e \in E$ и $f \in \ell^2(V)$

$$df(e) = \sum_{x\in V} \delta(x,e)f(x),$$

док је за $v \in V$ и $g \in \ell^2(E)$

$$d^*g(x) = \sum_{e\in E} \delta(x,e)g(e).$$

Дефинишимо *комбинаторни Лапласов оператор* $\Delta = d^*d : \ell^2(V) \to \ell^2(V)$. Имамо да је:

$$\Delta f(x) = d^*df(x) = \sum_{e\in E} \delta(x,e)df(e) = \sum_{e\in E} \left(\delta(x,e) \cdot \sum_{y\in V} \delta(y,e)f(y) \right)$$

$$= \sum_{\substack{e\in E\\ x=y}} \delta(x,e)^2 f(x) + \sum_{e\in E}\sum_{\substack{y\in V\\ x\neq y}} \delta(x,e)\delta(y,e)f(y) = \sum_{\substack{e\in E\\ x\in e}} 1\cdot f(x) + \sum_{\substack{xy\in E\\ x\neq y}} -1\cdot f(y)$$

$$= \deg(x)\cdot f(x) - \sum_{xy\in E} f(y) = kf(x) - \sum_{y\in V} A_{xy}f(y) = kf(x) - Af(x).$$

Дакле $\Delta = k\cdot \mathrm{Id} - A$, при чему је Id ознака за јединичну матрицу димензије n. Приметимо да Лапласов оператор не зависи од произвољно изабране оријентације ивица. У ортонормираној бази сопствених вектора матрице повезаности A Лапласов оператор има следећи облик:

$$\Delta = \begin{pmatrix} 0 & & & \bigcirc \\ & k-\mu_1 & & \\ & & \ddots & \\ \bigcirc & & & k-\mu_{n-1} \end{pmatrix},$$

при чему сопствена вредност 0 одговара константним функцијама на V. Нека је f вектор у $\ell^2(V)$ који је нормалан на константну функцију. Онда је $\sum_{x\in V} f(x) = 0$. Додатно, у нашој ортонормираној бази, координата вектора f која одговара константном сопственом вектору једнака је 0 (Парсевалова једнакост). Онда имамо :

$$\|df\|_2^2 = \langle df, df\rangle = \langle \Delta f, f\rangle = \sum_{i=1}^{|V|} (k-\mu_{i-1})\cdot f(x_i)^2 \geqslant (k-\mu_1)\|f\|_2^2.$$

Изаберимо сад одговарајућу функцију на коју ћемо применити ову неједнакост. Фиксирајмо подскуп F скупа чворова V. Нека је

$$f(x) = \begin{cases} |V-F| & , x\in F; \\ -|F| & , x\in V-F. \end{cases}$$

Лако се види да је $\sum_{x\in V} f(x) = 0$, као и да је $\|f\|_2^2 = |F|\cdot|V-F|^2 + |V-F|\cdot|F|^2 = |F|\cdot|V-F|\cdot|V|$. Додатно,

$$df(e) = \begin{cases} 0 & \text{, ако је } e \text{ ивица која спаја два чвора из } F \text{ или два чвора из } V-F \\ \pm|V| & \text{, ако ивица } e \text{ спаја чвор из } F \text{ са чвором из } V-F \end{cases}.$$

Дакле, $\|df\|_2^2 = |V|^2|\partial F|$. Убацивањем у претходну неједнакост добијамо:

$$|V|^2|\partial F| \geqslant (k-\mu_1)|F|\cdot|V-F|\cdot|V|.$$

Даље уз претпоставку да је $|F| \leqslant \left|\frac{V}{2}\right|$ имамо:

$$\frac{|\partial F|}{F} \geqslant (k-\mu_1)\frac{|V-F|}{V} \geqslant \frac{k-\mu_1}{2}.$$

Сада из дефиниције следи $h(X) \geqslant \dfrac{k-\mu_1}{2}$.

Докажимо сада и другу неједнакост. Фиксирајмо ненегативну функцију f на V и нека је

$$B_f = \sum_{e\in E} |f(e_+)^2 - f(e_-)^2|.$$

Означимо са $\beta_r > \beta_{r-1} > \cdots > \beta_0$ вредности које узима функција f. Посматрајмо следеће скупове:

$$L_i = \{x \in V : f(x) \geqslant \beta_i\} \qquad (i = 0, 1, \ldots, r).$$

Геометријски посматрано, можемо замислити да смо на овај начин поделили чворове графа на „енергетске нивое", где се ниво β_i састоји од свих чворова за које је $f(x) = \beta_i$, а у скупу L_i се налазе сви чворови који имају „енергију"већу или једнаку β_i. Поделимо наш доказ у неколико једноставнијих корака:

Корак 1: $B_f = \sum_{i=1}^{r} |\partial L_i|(\beta_i^2 - \beta_{i-1}^2)$.

Посматрајмо само оне ивице e за које је $f(e_-) \neq f(e_+)$. Назовимо тај скуп ивица E_f. За $e = xy \in E_f$ означимо са $i(e)$ и $j(e)$ индексе такве да је $f(x) = \beta_{i(e)}$, $f(y) = \beta_{j(e)}$ и $i(e) > j(e)$. Онда је:

$$B_f = \sum_{e\in E_f} (\beta_{i(e)}^2 - \beta_{j(e)}^2) = \sum_{e\in E_f} (\beta_{i(e)}^2 - \beta_{i(e)-1}^2 + \beta_{i(e)-1}^2 - \cdots - \beta_{j(e)+1}^2 + \beta_{j(e)+1}^2 - \beta_{j(e)}^2)$$

$$= \sum_{e\in E_f} \sum_{l=j(e)+1}^{i(e)} (\beta_l^2 - \beta_{l-1}^2).$$

Дакле, овиме смо за сваку ивицу e која означава прелазак са нивоа $i(e)$ на ниво $j(e)$ тај прелазак разбили на преласке између узастопних нивоа. У нашем изразу сваком том преласку одговара по један члан $\beta_l^2 - \beta_{l-1}^2$. То значи да се члан $\beta_l^2 - \beta_{l-1}^2$ појављује у изразу тачно онолико пута колико имамо прелазака са нивоа енергије веће или једнаке од β_l на нивое са нижом енергијом од β_l, но овај број је тачно $|\partial L_l|$ - границу скупа L_l чине све оне гране графа које повезују чворове из L_l са чворовима на мањим енергетским нивоима. Овиме је корак 1 завршен.

Корак 2: $B_f \leqslant \sqrt{2k}\|df\|_2\|f\|_2$.

$$B_f = \sum_{e\in E} |f(e_+) + f(e_-)||f(e_+) - f(e_-)|$$

$$\leqslant \left[\sum_{e\in E} (f(e_+) + f(e_-))^2\right]^{1/2} \cdot \left[\sum_{e\in E} (f(e_+) - f(e_-))^2\right]^{1/2}$$

$$\leqslant \sqrt{2}\left[\sum_{e\in E} f(e_+)^2 + f(e_-)^2\right]^{1/2} \|df\|_2 = \sqrt{2k}\left[\sum_{x\in V} f(x)^2\right]^{1/2} \|df\|_2 = \sqrt{2k}\|df\|_2\|f\|_2,$$

при чему прва неједнакост следи из Коши-Шварца, а друга из $(a+b)^2 \leqslant 2(a^2+b^2)$.

Корак 3: *Носач* функције f је дефинисан као $supp\ f = \{x \in V : f(x) \neq 0\}$. Нека је f таква да је $|supp\ f| \leqslant \frac{|V|}{2}$. Онда је $B_f \geqslant h(x)\|f\|_2$.

Како је f ненегативна функција, уз услов да је $|supp\ f| \leqslant \frac{|V|}{2}$ можемо закључити да је $\beta_0 = 0$ и $|L_i| \leqslant \frac{|V|}{2}$ за $i = 1, 2, \ldots, r$. Онда, из дефиниције $h(X)$ знамо да важи $|\partial L_i| \geqslant h(X)|L_i|$, те на основу корака 1 имамо:

$$B_f \geqslant h(X) \sum_{i=1}^{r} |L_i|(\beta_i - \beta_{i-1}) = h(X) \left[|L_r|\beta_r^2 + (|L_{r-1}| - |L_r|)\beta_{r-1}^2 + \cdots + (|L_0| - |L_1|)\beta_1^2\right].$$

Присетимо се да је разлика $|L_{i-1}| - |L_i|$ управо број чворова на енергетском нивоу β_{i-1} за $i = 1, 2, \ldots, r$, $|L_r|$ је број чворова на нивоу β_r, а $\beta_0 = 0$, те је члан у загради баш једнак $\|f\|_2^2$ чиме завршавамо и овај део доказа.

Корак 4: У овом кораку ћемо пажљиво изабрати функцију f и применити претходне кораке да бисмо доказали тражену неједнакост. Нека је g сопствена функција Лапласовог оператора Δ која одговара сопственој вредности $k - \mu_1$. Нека је $V_+ = \{x \in V : g(x) > 0\}$ ($V_+ \neq \emptyset$ јер је $\sum_{x \in V} g(x) = 0$, а g није нула функција). Променом g са $-g$, уколико је потребно, можемо претпоставити $|V_+| \leqslant \frac{|V|}{2}$. Нека је f таква да је $f(x) = \max(g(x), 0)$. Како је $g(v) \leqslant f(v)$ за сваки чвор v, за $x \in V_+$:

$$(\Delta f)(x) = kf(x) - \sum_{y \in V} A_{xy} f(y) \leqslant kg(x) - \sum_{y \in V} A_{xy} g(y) = (\Delta g)(x) = (k - \mu_1)g(x).$$

Користећи ову оцену добијамо:

$$\|df\|_2^2 = \langle \Delta f, f \rangle = \sum_{x \in V_+} (\Delta f)(x) g(x) \leqslant (k - \mu_1) \sum_{x \in V_+} g(x)^2 = (k - \mu_1)\|f\|_2^2.$$

Уз корак 2 и корак 3 добијамо:

$$h(X)\|f\|_2^2 \leqslant B_f \leqslant \sqrt{2k}\|df\|_2\|f\|_2 \leqslant \sqrt{2k(k - \mu_1)}\|f\|_2^2.$$

Скраћивањем $\|f\|_2^2 > 0$ добијамо тражену неједнакост и завршавамо доказ теореме. □

Ова теорема нам у суштини омогућава да изопериметријску константу, која је релативно тешка за манипулисање, заменимо значајно једноставнијом величином - спектралним размаком графа.

Последица 1. Нека је $(X_m)_{m \geqslant 1}$ фамилија коначних, повезаних, k-регуларних графова, при чему $|V_m| \to +\infty$ када $m \to +\infty$. Фамилија $(X_m)_{m \geqslant 1}$ је фамилија експандера ако и само ако постоји $\varepsilon > 0$ за које је $k - \mu_1(X_m) \geqslant \varepsilon$ за свако $m \geqslant 1$.

Овиме смо спектрално окарактерисали фамилије експандера: $(X_m)_{m \geqslant 1}$ је фамилија експандера акко је спектрални размак ових графова одвојен од нуле (не тежи нули). Штавише, из теореме 2.3 следи да што је већи спектрални размак, то је бољи „квалитет"наших експандера.

2.3 Асимптотско понашање сопствених вредности

У претходном делу смо доказали да је квалитет експандера одређен доњом границом спектралног размака тог графа. Но, испоставља се да, асимптотски, спектрални размак не може да буде много велики. Надаље радимо са графовима који немају петље.

Теорема 2.4. Нека је $(X_m)_{m\geqslant 1}$ фамилија коначних, повезаних, k-регуларних графова, при чему $|V_m| \to +\infty$ када $m \to +\infty$. Онда је

$$\liminf_{m\to+\infty} \mu_1(X_m) \geqslant 2\sqrt{k-1}.$$

Дефиниција 2.6. Коначан повезан k-регуларан граф X се назива *Раманујанов* ако за сваку нетривијалну сопствену вредност тог графа μ важи $|\mu| \leqslant 2\sqrt{k-1}$.

Нека је $(X_m)_{m\geqslant 1}$ фамилија k-регуларних Раманујанових графова који немају петље таква да $|V_m| \to +\infty$ када $m \to +\infty$. Онда X_m-ови достижу највећи могући спектрални размак и стога они чине најоптималнију фамилију експандера.
Коментар: Теорему 2.4 доказали су Алон и Бопана (за доказ види [N] и [LPS] или [DSV]).

Следећи одељак је посвећен проналажењу формуле која ће служити као темељ за добијање оцена сопствених вредности тј. спектралног размака у последњем поглављу.

2.4 Траг матрице повезаности

Нека је $X(V, E)$ повезан, прост, k-регуларан граф, при чему није неопходно да је X коначан. Пут дужине r *без враћања* у X је низ

$$\underline{e} = (x_0, x_1, \ldots, x_r)$$

чворова из V, таквих да за свако $i \in \{0, 1, \ldots, r-1\}$ грана $x_i x_{i+1}$ припада E и да је $x_{i-1} \neq x_{i+1}$ за свако $i \in \{1, 2, \ldots, r-1\}$. *Почетак* пута $\underline{e}$ је чвор x_0, а *крај* је x_r. За $r \in \mathbb{N}$ дефинишимо матрице A_r индексиране по $V \times V$ које ће представљати уопштење матрице повезаности, а биће полиноми по A:

$(A_r)_{xy}$ = број путева дужине r без враћања чији је почетак чвор x а крај чвор y.

Приметимо да је $A_0 = \mathrm{Id}$, а $A_1 = A$, при чему је стандардно A матрица повезаности. Веза између ових матрица је окарактерисана следећом лемом:

Лема 2.1. (а) $A_1^2 = A_2 + k \cdot \mathrm{Id}$,

(б) за $r \geqslant 2$ важи $A_1 A_r = A_r A_1 = A_{r+1} + (k-1)A_{r-1}$.

Доказ. (а) За $x, y \in V$ елемент матрице $(A_1^2)_{xy}$ је број свих путева дужине 2 од x до y. Ако $x \neq y$, сваки од ових путева мора да буде и пут без враћања, дакле $(A_1^2)_{xy} = (A_2)_{xy}$. Ако је $x = y$, сваки од избројаних путева јесте пут са враћањем, и како је X прост и k-регуларан, број тих путева је тачно k; следи $A_1^2 = A_2 + k \cdot Id$.

(б) Докажимо да је $A_r A_1 = A_{r+1} + (k-1)A_{r-1}$. Доказ да је $A_1 A_r = A_{r+1} + (k-1)A_{r-1}$ је аналоган. $(A_r A_1)_{xy}$ представља број путева $(x = x_0, x_1, \ldots, x_r, x_{r+1} = y)$ дужине $r+1$ без враћања осим можда у последњем кораку. Издвојмо онда 2 случаја у зависности да ли је у последњем кораку дошло до враћања или не:

(1) Ако је $x_{r-1} \neq y$, у последњем кораку није дошло до враћања и број оваквих путева је баш $(A_{r+1})_{xy}$;

(2) Ако је $x_{r-1} = y$, у последњем кораку јесте дошло до враћања и онда последња два корака можемо да изаберемо на $k-1$ начина ($y = x_{r-1}$ има $k-1$ суседа различитих од x_{r-2}), а првих $r-1$ корака нам чине пут без враћања дужине $r-1$ те њих бирамо на $(A_{r-1})_{xy}$ начина; дакле укупно $(k-1)(A_{r-1})_{xy}$ оваквих путева.

Овиме завршавамо наш доказ.

□

Као директну последицу претходне леме, можемо лако израчунати генераторну функцију низа A_i-ова, наиме:

Лема 2.2.

$$\sum_{r=0}^{\infty} A_r t^r = \frac{1-t^2}{1-At+(k-1)t^2}.$$

Ради једноставности, покушајмо да избацимо бројилац $1-t^2$ у претходној формули. Уведимо низ матрица T_m које су такође полиноми по A као:

$$T_m = \sum_{0 \leqslant r \leqslant \frac{m}{2}} A_{m-2r} \qquad (m \in \mathbb{N}_0).$$

Лема 2.3. Генераторна функција низа T_m је:

$$\sum_{m=0}^{\infty} T_m t^m = \frac{1}{1-At+(k-1)t^2}.$$

Доказ.

$$\sum_{m=0}^{\infty} T_m t^m = \sum_{m=0}^{\infty} \sum_{0 \leqslant r \leqslant \frac{m}{2}} A_{m-2r} t^m = \sum_{r=0}^{\infty} \sum_{m \geqslant 2r} A_{m-2r} t^m = \sum_{r=0}^{\infty} t^{2r} \sum_{m \geqslant 2r} A_{m-2r} t^{m-2r}$$

$$= \left(\sum_{r=0}^{\infty} t^{2r}\right)\left(\sum_{l=0}^{\infty} A_l t^l\right) = \frac{1}{1-t^2}\cdot\frac{1-t^2}{1-At+(k-1)t^2} = \frac{1}{1-At+(k-1)t^2}.$$

□

Лема 2.3 веома подсећа на генераторну функцију јако важне класе полинома- Чебишевљевих полинома.

Дефиниција 2.7. Чебишевљеви полиноми се дефинишу као полиноми степена m који се добијају када покушамо да изразимо $\dfrac{\sin(m+1)\theta}{\sin\theta}$ преко $\cos\theta$ тј.

$$U_m(\cos\theta) = \frac{\sin(m+1)\theta}{\sin\theta}, \qquad m \in \mathbb{N}_0.$$

На пример $U_0(x) = 1$, $U_1(x) = 2x$, $U_2(x) = 4x^2 - 1, \ldots$ Користећи тригонометријске идентитете добијамо да за ове полиноме важи следећа рекурентна формула:

$$U_{m+1}(x) = 2x \cdot U_m - U_{m-1}(x).$$

Даље из ове рекурентне формуле добијамо да за генераторну функцију Чебишевљевих полинома важи:

$$\sum_{m=0}^{\infty} U_m(x)t^m = \frac{1}{1-2xt+t^2}.$$

Уз просту смену промењиве можемо израчунати генераторну функцију фамилије полинома $(k-1)^{m/2}\cdot U_m\left(\dfrac{x}{2\sqrt{k-1}}\right)$:

$$\sum_{m=0}^{\infty}(k-1)^{m/2}\cdot U_m\left(\frac{x}{2\sqrt{k-1}}\right)t^m = \frac{1}{1-xt+(k-1)t^2}.$$

Посматрајући оператор T_m као полином степена m по матрици повезаности, поређењем претходног израза са лемом 2.3 добијамо следећи идентитет:

Последица 2. За $m \in \mathbb{N}_0$ важи $T_m = (k-1)^{\frac{m}{2}} U_m\left(\dfrac{A}{2\sqrt{k-1}}\right)$.

Нека је $X(V,E)$ коначан, k-регуларан прост граф са n чворова чији је спектар

$$k = \mu_0 \geqslant \mu_1 \geqslant \cdots \geqslant \mu_{n-1}.$$

Сада ћемо траг матрице T_m одредити спектрално из претходне последице као и комбинаторно из саме дефиниције матрице T_m. Како је T_m полином по A у ортонормираној бази сопствених вектора матрице A и матрица T_m је дијагонална и важи следећа формула:

$$\operatorname{Tr} T_m = (k-1)^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{k-1}}\right).$$

Са друге стране, на основу дефиниције T_m имамо:

$$\operatorname{Tr} T_m = \sum_{0 \leqslant r \leqslant \frac{m}{2}} \operatorname{Tr} A_{m-2r} = \sum_{x \in V} \sum_{0 \leqslant r \leqslant \frac{m}{2}} (A_{m-2r})_{xx}.$$

За свако $x \in V$ означимо са $f_{\ell,x}$ број путева без враћања дужине ℓ чији су почетак и крај баш чвор x. Другим речима: $f_{\ell,x} = (A_l)_{xx}$.

Теорема 2.5.

$$\sum_{x \in V} \sum_{0 \leqslant r \leqslant \frac{m}{2}} f_{m-2r,x} = (k-1)^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m \left(\frac{\mu_j}{2\sqrt{k-1}} \right),$$

за свако $m \in \mathbb{N}_0$.

Како ћемо у наставку текста конструисати графове који су *транзитивни* погледајмо како ова теорема изгледа у случају таквих, веома симетричних графова. Граф се назива транзитивним ако за сваки пар чворова x и y постоји аутоморфизам f тог графа такав да је $f(x) = y$. Са овом додатном претпоставком број $f_{\ell,x}$ не зависи од чвора x и уместо њега ћемо писати само f_ℓ.

Последица 3. Нека је X коначан, транзитиван, k-регуларан граф са n чворова. Онда за свако $m \in \mathbb{N}_0$ важи:

$$n \cdot \sum_{0 \leqslant r \leqslant \frac{m}{2}} f_{m-2r} = (k-1)^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m \left(\frac{\mu_j}{2\sqrt{k-1}} \right).$$

3

Конструкција Раманујанових графова

У овом поглављу ћемо најпре проћи кроз неопходну теоријску припрему (прве три секције), а након тога ћемо конструисати две фамилије графова $X^{p,q}$ и $Y^{p,q}$ за које ћемо доказати да су изоморфне. Сврха конструкције две фамилије графова огледа се у томе што нека комбинаторна својства можемо тривијално видети код графова $X^{p,q}$ ($Y^{p,q}$), док у случају графова $Y^{p,q}(X^{p,q})$ она нису ни најмање очигледна. У наредном поглављу ћемо помоћу ових својстава доказати да ови графови заиста чине фамилију експандера.

3.1 Кејлијеви графови

Нека је G група и нека је S непразан коначан подскуп те групе. Додатно, нека је S симетричан тј. $S = S^{-1}$.

Дефиниција 3.1. *Кејлијев граф* $\mathcal{G}(G, S)$ је граф којем је скуп чворова V једнак G, а скуп ивица је дефинисан на следећи начин:

$$E = \{\{x, y\} : x, y \in G; \exists s \in S : y = xs\}.$$

Дакле два чвора су повезана уколико је један добијен од другог десним множењем неким елементом из S. Приметимо још и да је наш граф неусмерен - уколико ивица $xy \in G$ онда и ивица $yx \in G$ јер је скуп S по којем смо дефинисали релацију повезаности симетричан.

Наведимо сада и нека од својстава Кејлијевих графова која ће нам указати на везу комбинаторне структуре самог графа са структуром групе и њеног подскупа.

Лема 3.1. Нека је $\mathcal{G}(G, S)$ Кејлијев граф и нека је $|S| = k$.

(1) $\mathcal{G}(G, S)$ је прост, k-регуларан, транзитиван граф. Присетимо се притом да је својство транзитивности дефинисано на следећи начин: граф је транзитиван

уколико за сваки пар чворова x и y постоји аутоморфизам f тог графа такав да је $f(x) = y$.

(2) $\mathcal{G}(G, S)$ не садржи петље ако и само ако $1 \notin S$.

(3) $\mathcal{G}(G, S)$ је повезан ако и само ако S генерише G.

Доказ. (1) Како је $|S| = k$ и $y = xs_1$ и $y = xs_2$ повлачи $s_1 = s_2$, очигледно је да је наш граф прост и k-регуларан. Што се тиче транзитивности, фиксирајмо пар чворова $x, y \in G$ и докажимо да је $f : G \to G, \quad f(g) = yx^{-1}g$ одговарајући аутоморфизам графа који шаље чвор x у чвор y. Заиста $f(x) = y$. Очигледно је да је пресликавање f $1-1$ јер $f(g) = f(h) \Rightarrow yx^{-1}g = yx^{-1}h \Rightarrow g = h$. Такође, ово пресликавање је на јер за свако $g \in G$ постоји $h \in G$, наиме $h = xy^{-1}g$, такво да је $f(h) = g$. За крај, ако су чворови g и h повезани у $\mathcal{G}(G, S)$ они су повезани и у $f(\mathcal{G}(G, S))$ и обратно ($g = hs \Leftrightarrow yx^{-1}g = yx^{-1}hs$). Дакле овај граф је заиста транзитиван.

(2) Ово тврђење следи директно из дефиниције графа.

(3) Ако S генерише G онда за свако $g \in G$ постоји коначан низ елемената из S, назовимо их $s_1, s_2, \ldots s_n$ таквих да је $g = 1 \cdot s_1 s_2 \cdots s_n$. Дакле постоји пут од јединице до g, наиме пут $1, 1 \cdot s_1, 1 \cdot s_1 s_2, \ldots, 1 \cdot s_1 \cdots s_n$, што значи да је наш граф повезан. Обратно, ако је граф повезан слично као раније проналазимо пут од било ког чвора g до јединице, и тај пут генерише неко представљање елемента g помоћу елемената из S.

□

У наредном делу ћемо уз помоћ кватернионске алгебре пронаћи згодну групу G и њен симетричан подскуп S, који ће нам послужити за конструкцију графа $X^{p,q}$ као Кејлијевог графа $\mathcal{G}(G, S)$.

3.2 Кватернионска алгебра - припрема за конструкцију графа $X^{p,q}$

Дефиниција 3.2. Кватернионска алгебра над прстеном R, у ознаци $\mathbb{H}(R)$, је асоцијативна алгебра са јединицом, чија је презентација задата на следећи начин:

(1) $\mathbb{H}(R) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in R\}$,

(2) 1 је мултипликативна јединица,

(3) $i^2 = j^2 = k^2 = -1$,

(4) $ij = -ji = k; jk = -kj = i; ki = -ik = j$.

Ако је кватернион $q = a_0 + a_1 i + a_2 j + a_3 k$, његов конјугат је кватернион $\overline{q} = a_0 - a_1 i - a_2 j - a_3 k$. Норма кватерниона q је задата са $N(q) = q\overline{q} = \overline{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Лако је доказати да је кватернионска норма мултипликативна тј. $N(q_1 q_2) = N(q_1)N(q_2)\ \forall q_1, q_2 \in \mathbb{H}(R)$.

За конструкцију Раманујанових графова ће нам бити потребно да идентификујемо кватернионску алгебру над пољем K са алгебром матрица 2×2 над K, стога наведимо следећу лему:

Лема 3.2. Нека је K поље чија карактеристика није 2. Претпоставимо да постоје $x, y \in K$ такви да је $x^2 + y^2 + 1 = 0$. Онда је $\mathbb{H}(K)$ изоморфна са алгебром $M_2(K)$ матрица 2×2 над пољем K.

Пре него што започнемо доказ присетимо се дефиниције карактеристике прстена. *Карактеристика* прстена је или 0 или, уколико постоји, најмањи природан број m такав да је

$$0 = m \cdot 1 = 1 + 1 + \cdots + 1 \qquad (m \text{ пута}).$$

У случају поља карактеристика мора бити или 0 или прост број - нпр. за поља $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ карактеристика је 0, док је код коначних поља $\mathbb{F}_q$, где је $q = p^k$ степен простог броја p, њихова карактеристика p. Сада се вратимо на доказ.

Доказ. Нека је $\psi : \mathbb{H}(K) \to M_2(K)$ задато са:

$$\psi(a_0 + a_1 i + a_2 j + a_3 k) = \begin{pmatrix} a_0 y + a_1 x + a_3 y & -a_1 + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{pmatrix}.$$

Лако се проверава да је $\psi(q_1 q_2) = \psi(q_1)\psi(q_2)$ за све $q_1, q_2 \in \mathbb{H}(K)$. Како је ψ K-линеарно пресликавање између два K-векторска простора димензије 4, да бисмо доказали да је ψ изоморфизам довољно је да докажемо да је ψ '1-1' тј. да је $\dim \ker(\psi) = 0$. Но, ово тривијално следи из чињенице да из $\psi(a_0 + a_1 i + a_2 j + a_3 k) = 0$ добијамо 4×4 хомогени систем линеарних једначина чија је детерминанта различита од нуле:

$$\begin{vmatrix} 1 & x & 0 & y \\ 0 & -y & 1 & x \\ 0 & -y & -1 & x \\ 1 & x & 0 & -y \end{vmatrix} = -4(x^2 + y^2) = 4 \neq 0,$$

при чему је $4 \neq 0$ зато што карактеристика поља K није 2. □

У даљем тексту ћемо већином разматрати аритметичка својства кватерниона $\mathbb{H}(\mathbb{Z})$ над прстеном $\mathbb{Z}$, стога проучимо мало боље њихову структуру.
Лако је показати да су следећа три тврђења еквивалентна:

(1) α је јединични (инвертибилни) елемент у $\mathbb{H}(\mathbb{Z})$,

(2) $N(\alpha) = 1$,

(3) $\alpha \in \{\pm 1, \pm i, \pm j, \pm k\}$.

Дефиниција 3.3. (1) Кватернион $\alpha \in \mathbb{H}(\mathbb{Z})$ је *парaн* (*непарaн*) ако је $N(\alpha)$ паран (непаран) цео број.

(2) Кватернион $\alpha \in \mathbb{H}(\mathbb{Z})$ је *простo* ако α није јединица у $\mathbb{H}(\mathbb{Z})$, и за све $\beta, \gamma \in \mathbb{H}(\mathbb{Z})$ такве да је $\alpha = \beta\gamma$ важи да је бар један од β, γ јединични елемент.

(3) Два кватерниона $\alpha, \alpha' \in \mathbb{H}(\mathbb{Z})$ су *асоцирани* ако постоје јединични кватерниони ε и ε' такви да је $\alpha = \varepsilon\alpha\varepsilon'$.

(4) Кватернион δ је десни делилац кватерниона α ако постоји $\gamma \in \mathbb{H}(\mathbb{Z})$ такав да је $\alpha = \gamma\delta$.

Слично као и у прстенима $\mathbb{Z}$ и $\mathbb{Z}[i]$ и у прстену $\mathbb{H}(\mathbb{Z})$ постоји факторизација на просте елементе, додуше та факторизација неће бити јединствена. Такође, имајући у виду да прстен кватерниона није комутативан, морамо модификовати Еуклидов алгоритам у складу са тим. Испоставља се да се Еуклидов алгоритам може реализовати на паровима кватерниона $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ уколико је β непаран десним или левим дељењем. У даљем тексту ћемо се служити само десним дељењем.

$$\forall \alpha, \beta \in \mathbb{H}(\mathbb{Z}) \quad \exists \gamma, \delta \in \mathbb{H}(\mathbb{Z}) \qquad \alpha = \gamma\beta + \delta, N(\delta) < N(\beta).$$

Дефиниција 3.4. Нека су α, β цели кватерниони. Онда је $\delta \in \mathbb{H}(\mathbb{Z})$ десни највећи заједнички делилац кватерниона α, β у ознаци $\delta = (\alpha, \beta)_r$ ако је:

(1) δ је десни делилац од α и од β

(2) Ако је $\delta_0 \in \mathbb{H}(\mathbb{Z})$ десни делилац кватерниона α и β, онда је δ_0 десни делилац кватерниона δ.

Јасно је да је десни НЗД, уколико постоји, јединствен до на јединични елемент. Напоменимо и да десни и леви НЗД два кватерниона не морају бити исти.

Лема 3.3. Ако су α, β цели кватерниони, при чему је β непаран, онда постоји $(\alpha, \beta)_r$. Штавише, важи и уопштена Безуова теорема:

$$\exists \gamma, \delta \in \mathbb{H}(\mathbb{Z}\left[\frac{1}{2}\right]) \qquad \text{таквих да} \qquad (\alpha, \beta)_r = \gamma\alpha + \delta\beta,$$

при чему је $\mathbb{Z}\left[\frac{1}{2}\right]$ дефинисано као подпрстен прстена $\mathbb{Q}$ где је $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{k}{2^n} : k \in \mathbb{Z}, n \in \mathbb{N}_0\right\}$.

Карактеризација простих елемената у $\mathbb{H}(\mathbb{Z})$ је изненађујуће једноставна - цео кватернион α је прост ако и само ако му је норма прост број у $\mathbb{Z}$. У даљем тексту ћемо боље проучити целе кватернионе α за које је $N(\alpha) = p^k$ где је p непаран прост број у $\mathbb{Z}$. Иако за опште кватернионе неће постојати јединствена факторизација на просте, у овом случају можемо пронаћи облик факторизације који је јединствен.

За то ће нам бити потребна *Јакобијева теорема* из теорије бројева, која нам даје број представљања природног броја као збир четири квадрата. Она тврди:

Теорема 3.1. */Јакобијева теорема/* Нека је $n \in \mathbb{N}$. Онда је број четворки $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ за које је $a_0^2 + a_1^2 + a_2^2 + a_3^2 = n$ једнак $8 \sum_{d|n} d$.

Дакле нека је p непаран прост број у $\mathbb{Z}$. Користећи Јакобијеву теорему која тврди да једначина

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$$

има $8(p+1)$ решења у $\mathbb{Z}$ закључујемо да постоји $8(p+1)$ одговарајућих целих кватерниона $a_0 + a_1 i + a_2 j + a_3 k$ чија је норма p. Ако је $p \equiv 1 \pmod 4$ један a_i је непаран, а остали су парни; ако је $p \equiv 3 \pmod 4$ један a_i је паран, а остали су непарни. У сваком случају постоји један a_i који се разликује од осталих. Назовимо га a_i^0. Ако је $a_i^0 \neq 0$, међу 8 асоцираних елемената $\varepsilon\alpha$ елемента α постоји тачно један којем је нулта координата једнака $|a_i^0|$. Изаберимо баш тај кватернион да нам буде представник ове класе асоцираних кватерниона. Уколико је $a_i^0 = 0$, од укупно осам асоцираних елемената постоје тачно два којима је нулта координата a_i^0, наиме $\varepsilon\alpha$ и $-\varepsilon\alpha$. У овом случају изаберимо било који од њих као представника. Дакле овиме смо издвојили $p+1$ есенцијално различитих решења једначине

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p,$$

при чему кватерниони који одговарају решењима задовољавају: $\alpha \equiv 1 \pmod 2$ или $\alpha \equiv i + j + k \pmod 2$. Међу изабраним представницима се појављују и α и $\overline{\alpha}$ уколико је $a_0 > 0$, док се појављује само један кватернион из конјугованог пара ако је $a_0 = 0$. Сада можемо да дефинишемо скуп

$$S_p = \{\alpha_1, \overline{\alpha_1}, \ldots, \alpha_s, \overline{\alpha_s}, \beta_1, \ldots, \beta_t\},$$

при чему за α_i важи $a_0^{(i)} > 0$, а за β_i је $\beta_0^{(i)} = 0$, као и $\alpha_i\overline{\alpha_i} = -\beta_i^2 = p^2$. Приметимо и да је $2s + t = |S_p| = p + 1$.

Дефиниција 3.5. *Редукована реч* над S_p је реч над алфабетом S_p, која не садржи подреч облика $\alpha_i\overline{\alpha_i}, \overline{\alpha_i}\alpha_i, \beta_j^2 \quad (i = 1, 2, \ldots, s; \quad j = 1, 2, \ldots, t)$. *Дужина* речи је број симбола који се појављују у запису те речи.

Теорема 3.2. Нека је $k \in \mathbb{N}$ и $\alpha \in \mathbb{H}(\mathbb{Z})$ такав да је $N(\alpha) = p^k$. Онда постоји јединствена факторизација кватерниона α у облику $\alpha = \varepsilon p^r w_m$ где је ε јединични елемент у $\mathbb{H}(Z)$, w_m редукована реч над S_p дужине m и $k = 2r + m$.

Доказ. Најпре докажимо постојање овакве факторизације. Фиксирајмо $\alpha \in \mathbb{H}(\mathbb{Z})$ за које је $N(\alpha) = p^k$. Онда α можемо да запишемо као производ простих у $\mathbb{H}(\mathbb{Z})$ као:

$$\alpha = \delta_1\delta_2 \cdots \delta_n.$$

Имајући на уму карактеризацију простих у $\mathbb{H}(\mathbb{Z})$, као и то да је норма кватерниона мултипликативна, закључујемо да је $N(\delta_i) = p$ за $i \in \{1, 2, \ldots, n\}$, те је онда и $n = k$.

Како је $N(\delta_i) = p$, за свако i можемо изабрати $\gamma_i \in S_p$ такво да је $\delta_i = \varepsilon_i\gamma_i$, при чему је ε_i јединични елемент у $\mathbb{H}(\mathbb{Z})$. Онда је

$$\alpha = \varepsilon_1\gamma_1\varepsilon_2\gamma_2\cdots\varepsilon_k\gamma_k.$$

Сада приметимо да за свако $\gamma \in S_p$ и сваки јединични елемент ε постоје $\gamma' \in S_p$ и јединичан елемент ε' такви да је $\gamma\varepsilon = \varepsilon'\gamma'$. Дакле, можемо померити све ε_i на леву страну и добити факторизацију броја α у следећем облику:

$$\alpha = \varepsilon'\gamma_1'\gamma_2'\cdots\gamma_k'.$$

У овом тренутку смо α написали као реч над S_p, али та реч и даље није редукована. Но, то се лако поправља, наиме, уколико се у речи појављује $\alpha_i\overline{\alpha_i}$, $\overline{\alpha_i}\alpha_i$ или β_j^2, фактор p можемо извући на леву страну (број из $\mathbb{Z}$ комутира са свим кватернионима) и тиме смањити дужину речи за два. Понављајући овај процес докле год је то потребно на крају ћемо добити тражену факторизацију. Овај процес се завршава, јер почетна реч има коначно много слова, а у сваком кораку смањујемо број слова за 2. Овиме смо доказали постојање.

Јединственост ћемо доказати комбинаторним аргументом. Наиме, број кватерниона за које је $N(\alpha) = p^k$ је по Јакобијевој теореми једнак

$$8\sum_{i=0}^{k} p^i = 8\left(\frac{p^{k+1}-1}{p-1}\right).$$

Сада избројимо колико има редукованих речи над S_p дужине m. За прво слово у речи имамо $|S_p| = p+1$ могућности, а за свако следеће p могућности да бисмо избегли појављивање $\alpha_i\overline{\alpha_i}$, $\overline{\alpha_i}\alpha_i$ или β_j^2. Ако је $m = 0$ број редукованих речи дужине m је 1. Онда знамо да је број израза облика $\varepsilon p^r w_m$, где је ε јединични елемент, w_m редукована реч над S_p дужине m, и важи $2r + m = k$ баш:

$$\begin{cases} 8\left(1 + \sum_{r=0}^{\frac{k}{2}-1}(p+1)p^{k-2r-1}\right) & \text{ако је } k \text{ паран;} \\ 8\sum_{r=0}^{\frac{k-1}{2}}(p+1)p^{k-2r-1} & \text{ако је } k \text{ непаран.} \end{cases}$$

У оба случаја лако добијамо да су ти изрази баш једнаки $8\left(\frac{p^{k+1}-1}{p-1}\right)$, тј. број израза $\varepsilon p^r w_m$ који задовољавају одговарајуће услове је једнак броју кватерниона чија је норма p^k. По претходном делу, у којем смо доказали да се сваки кватернион норме p^k може записати у облику $\varepsilon p^r w_m$, закључујемо да је таква факторизација јединствена. Овиме завршавамо наш доказ. □

Уведимо још и следећи скуп, који ће нам помоћи при конструкцији наше фамилије експандера:

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod 2 \text{ или } \alpha \equiv i+j+k \pmod 2, N(\alpha) = p^k \text{ за неко } k \in \mathbb{N}\}.$$

Лако се види да је Λ' затворен у односу на множење, као и то да $S_p \subseteq \Lambda'$. Додатно, претходна лема за кватернионе из скупа Λ' има још лепши облик:

Последица 4. Сваки елемент $\alpha \in \Lambda'$ норме p^k може се на јединствен начин записати као $\alpha = \pm p^r w_m$, где је w_m редукована реч над S_p дужине m и $2r + m = k$.

Доказ. По претходној леми α можемо записати као $\varepsilon p^r w_m$, где r и w_m имају тражена својства, а ε је јединичан. Дакле треба да докажемо да је $\varepsilon = \pm 1$. Редукцијом модуло 2 добијамо $\alpha \equiv \varepsilon w_m \pmod 2$. За $\alpha_i, \beta_j \in S_p$ које се појављују у запису речи w_m важи да су конгруентни са 1 или са $i+j+k$ модуло 2. Означимо са γ број слова у w_m која су конгруентна са $i+j+k$ модуло 2. Онда знамо да је

$$\begin{cases} \alpha \equiv \varepsilon \pmod 2, & \text{ако је } \gamma \text{ паран;} \\ \alpha \equiv \varepsilon(i+j+k) \pmod 2, & \text{ако је } \gamma \text{ непаран.} \end{cases}$$

Како је $\alpha \in \Lambda'$ знамо да је $\alpha \equiv 1$ или $(i+j+k) \pmod 2$, те је у оба случаја $\varepsilon \equiv \pm 1 \pmod 2$, па како је ε јединични елемент, знамо да је баш једнак ± 1. Овиме завршавамо доказ.
Коментар: У току доказа смо свуда користили $(i+j+k)^2 = -3 \equiv 1 \pmod 2$. □

3.3 Алгебра матрица 2×2

У претходном делу смо лемом 3.2 најавили да ћемо кватернионе заправо посматрати као матрице 2×2, те ће тема овог поглавља бити управо алгебра ових матрица. Увешћемо пар веома битних група и доказаћемо нека њихова својства која ће помоћи при анализи Раманујанових графова $X^{p,q}$ које ћемо конструисати у наредном поглављу.

Нека је K произвољно поље.

Дефиниција 3.6. *Општа линеарна група* над пољем K, у ознаци $GL_2(K)$, је група инвертибилних матрица 2×2 чији су елементи из поља K.
Специјална линеарна група над пољем K, у ознаци $SL_2(K)$, је група матрица чија је детерминанта 1. Другим речима $SL_2(K)$ је језгро пресликавања $\det : GL_2(K) \to K^\times$.
Општа пројективна линеарна група у ознаци $PGL_2(K)$ је количничка група дефинисана са

$$PGL_2(K) = GL_2(K) / \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in K^\times \right\}.$$

Специјална пројективна линеарна група у ознаци $PSL_2(K)$ је количничка група дефинисана са

$$PSL_2(K) = GL_2(K) / \left\{ \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix} : \varepsilon = \pm 1 \right\}.$$

Како је $PGL_2(K)$ дефинисана као количничка група, знамо да постоји природан хомоморфизам

$$\varphi : GL_2(K) \to PGL_2(K),$$

чије је језгро баш група ненула скаларних матрица.

Додатно, постоји још један природан начин на који можемо дефинисати пројективне линеарне групе. Наиме, утопићемо групе $PGL_2(K)$ и $PSL_2(K)$ у групу $\mathrm{Sym}\ (P^1(K))$,

групу пермутација пројективне праве $P^1(K)$. Пројективна права $P^1(K)$ дефинисана је као $K \cup \{\infty\}$. Свакој матрици $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ доделићемо Мебијусову трансформацију $\varphi_A : P^1(K) \to P^1(K)$ дефинисану на следећи начин:

$$\varphi_A(z) = \frac{az+b}{cz+d}.$$

Додатно дефинисаћемо $\varphi_A(\infty) = \begin{cases} \frac{a}{c} & \text{ако } c \neq 0 \\ \infty & \text{ако } c = 0 \end{cases}$, као и $\varphi_A\left(-\frac{c}{d}\right) = \infty$. Овиме смо дефинисали хомоморфизам група $\varphi : GL_2(q) \to \mathrm{Sym}\,(P^1(K))$ где је $\varphi(A) = \varphi_A$. Језгро овог хомоморфизма је баш група скаларних матрица, те лако видимо да можемо идентификовати $PGL_2(K)$ и $\mathrm{Im}\ \varphi$. Слично важи и за специјалну пројективну линеарну групу.

Коментар : Иако елементи $PGL_2(K)$ и $PSL_2(K)$ нису исти у смислу да косет једне матрице у $PGL_2(K)$ неће имати исти број елемената као и косет те исте матрице у $PSL_2(K)$, уколико постоје два иста представника косета из $PGL_2(K)$ и $PSL_2(K)$ сматраћемо да су они исти, тј. природно ћемо утопити $PSL_2(K)$ у $PGL_2(K)$.

Нека је $\mathbb{F}_q$ коначно поље реда q. Ради једноставнијег записа ћемо групе матрица над овим пољем означавати са $GL_2(q), PGL_2(q), SL_2(q)$ и $PSL_2(q)$.

Лема 3.4. (а) $|GL_2(q)| = q(q-1)(q^2-1)$

(б) $|SL_2(q)| = |PGL_2(q)| = q(q^2-1)$

(в) $|PSL_2(q)| = \begin{cases} q(q^2-1), & \text{ако је } q \text{ паран} \\ \frac{q(q^2-1)}{2}, & \text{ако је } q \text{ непаран} \end{cases}$

Доказ. Што се тиче дела (а), за избор прве колоне у матрици из $GL_2(q)$ имамо q^2-1 ненула могућности, а како друга колона мора да чини вектор који је линеарно независан од првог за њу имамо $q^2-1-(q-1) = q(q-1)$ могућности; дакле укупно $q(q-1)(q^2-1)$. Делови под (б) и (в) следе тривијално из дела под (а) и Лагранжове теореме. □

Дефиниција 3.7. Група G се назива *скоро Абелова*, уколико постоји њена нормална подгрупа N, таква да су и N и G/N Абелове групе.

Дефиниција 3.8. Нека је G група и нека су $g_1, g_2 \in G$. *Комутатор* $[g_1, g_2]$ је дефинисан као $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$. Комутатор је једнак неутралу ако и само ако g_1 и g_2 комутирају. Скуп свих комутатора једне групе у општем случају није затворен у односу на операцију групе, али постоји *комутаторска подгрупа* групе G, која је дефинисана као затворење скупа комутатора у односу на операцију групе. Величина комутаторске подгрупе указује на то у којој мери је операција групе комутативна - нпр. код Абелових група комутаторску подгрупу чини само неутрал.

Лема 3.5. Група G је скоро Абелова ако и само ако је за све $g_1, g_2, g_3, g_4 \in G$

$$[[g_1, g_2], [g_3, g_4]] = 1.$$

Доказ. ($\Rightarrow$) Претпоставимо најпре да је G скоро Абелова. Онда постоји нормална подгрупа N таква да су и N и G/N Абелове групе. Нека су $g_1, g_2, g_3, g_4 \in G$. Како косети $g_1^{-1}N$ и $g_2^{-1}N$ комутирају знамо да је $g_1^{-1}g_2^{-1}N = g_2^{-1}g_1^{-1}N$ те знамо да постоји $n \in N$ такво да је $g_1^{-1}g_2^{-1} = g_2^{-1}g_1^{-1}n$. Онда је по дефиницији комутатор $[g_1, g_2]$ једнак баш n. Аналогно постоји и $m \in N$ такво да је $[g_3, g_4] = m$. Сада, како је N Абелова, знамо да n и m комутирају, тј. да је $1 = [m, n] = [[g_1, g_2], [g_3, g_4]]$. Овиме завршавамо овај део доказа.
($\Leftarrow$) Претпоставимо сада да за све $g_1, g_2, g_3, g_4 \in G$ важи $[[g_1, g_2], [g_3, g_4]] = 1$. Означимо са N комутаторску подгрупу групе G. На основу $[[g_1, g_2], [g_3, g_4]] = 1$ закључујемо да свака два комутатора међусобно комутирају, а самим тим и свака два елемента комутаторске подгрупе. Заиста, сваки елемент комутаторске подгрупе може се записати као производ коначно много комутатора, те они сви комутирају међусобно. Дакле комутаторска подгрупа је Абелова. Докажимо сада да је и G/N Абелова група. Тиме ћемо показати да је G заиста скоро Абелова. Нека су a и b произвољна два елемента из G. Наш задатак је да покажемо да су косети $abN = aN \cdot bN$ и $baN = bN \cdot aN$ једнаки. Нека је $n \in N$, онда је

$$abn = ab \cdot [b^{-1}, a^{-1}] \cdot [a^{-1}, b^{-1}] \cdot n = ba \cdot ([a^{-1}, b^{-1}] \cdot n) \in baN,$$

баш зато што $[a^{-1}, b^{-1}] \in N$. Овиме смо показали да је $abN \subseteq baN$. Аналогно се показује $baN \subseteq abN$ те су ова два косета једнака. Овиме завршавамо доказ теореме. □

Лема 3.6. Нека је q прост број. Ако је H права подгрупа од $PSL_2(q)$ и $|H| > 60$, онда је H скоро Абелова.

Доказ. Доказ ове леме поделићемо на два случаја у зависности од тога да ли q дели $|H|$ или не. У наставку текста навешћемо доказ када q дели $|H|$, а други случај остављамо читаоцу, јер је технички захтеван, а не пружа боље разумевање самих Раманујанових графова који су тема овог рада.

Дакле нека q дели $|H|$. Треба да докажемо да ако је H права подгрупа од $PSL_2(q)$, онда је H скоро Абелова. Да бисмо доказали овај случај потребна нам је карактеризација елемената реда q у $PSL_2(q)$. Но, најпре наведимо тврђење о пермутацијама које ће нам помоћи при проналажењу ове карактеризације (сетимо се, φ_A су пермутације пројективне праве!).
Тврђење: Нека је σ пермутација скупа X и нека је њен ред прост број q. Онда сваки елемент скупа X у односу на пермутацију σ има ред 1 или q.
Доказ: Нека је H подгрупа групе Sym (X) генерисана пермутацијом σ. Познато је онда да је $|\Omega_x| = \dfrac{|H|}{|H_x|}$, при чему је Ω_x орбита елемента x у односу на групу H, а

$H_x = \{\alpha \in H : \alpha(x) = x\}$ је стабилизатор тог елемента, такође у групи H. Онда како је $|H| = q$ прост број, знамо да $|\Omega_x|$ мора да буде или 1 или q, чиме завршавамо доказ тврђења.
Приметимо да је тачка чија је орбита величине 1 заправо фиксна тачка.
Лема: Ако је $A \in SL_2(q)$ онда су следећа три тврђења еквивалентна:

(i) φ_A има ред q;

(ii) постоји јединствени једнодимензиони потпростор D простора $\mathbb{F}_q^2$ такав да или A или $-A$ фиксира D (фиксира сваки елемент од D понаособ);

(iii) φ_A је конјугат у $PGL_2(q)$ некој φ_{C_b}, где је $b \in \mathbb{F}_q^\times$.

Матрица C_b дефинисана је као $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, где $b \in \mathbb{F}_q$.
Доказ: $(i) \Rightarrow (ii)$ φ_A је Мебијусова трансформација на $P^1(\mathbb{F}_q)$, тј. то је пермутација скупа који има $|P^1(\mathbb{F}_q)| = q + 1$ елемената. Како је ред те пермутације баш q на основу претходног тврђења знамо да та пермутација мора имати бар једну фиксну тачку (сума величине свих орбита је $q + 1$, а орбите могу бити величине 1 или q). Фиксна тачка у $P^1(\mathbb{F}_q)$ одговара једном једнодимензионом потпростору D у $\mathbb{F}_q^2$ који је глобално инваријантан у односу на линеарни оператор A. Сада, како је језгро пресликавања φ из $SL_2(q)$ у $PSL_2(q)$ дводимензионално, и како је φ_A реда q, закључујемо да ред матрице A у $SL_2(q)$ може бити q или $2q$. Онда разликујемо следећа два случаја:

(1) A има ред q. Онда рестрикција оператора A на D представља пермутацију скупа $\mathbb{F}_q$ величине q чији је ред q, а како знамо да ова трансформација има бар једну фиксну тачку (тачку $(0, 0)$), онда по горенаведеном тврђењу знамо да свака тачка има орбиту величине 1 (збир величина свих орбита је q, а постоји једна која је величине 1). Дакле све тачке су фиксне тачке тј. A фиксира D тачку-по-тачку.

(2) A има ред $2q$. Онда сва претходна запажања важе за матрицу A^2, те A^2 фиксира D тачку-по-тачку. Онда A делује на D тако што шаље x у $-x$, те оператор $-A$ фиксира D тачку-по-тачку. Овиме смо завршили овај део доказа.

$(ii) \Rightarrow (iii)$ Изаберимо базу $\{e_1, e_2\}$ од $\mathbb{F}_q^2$ такву да $e_1 \in D$. У тој бази матрица A има облик $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, при чему $a = d = \pm 1$ и $b \neq 0$. Ово значи да је φ_A у $PSL_2(q)$ конјугат од $\varphi_{C_{ab}}$, $ab \neq 0$.
$(iii) \Rightarrow (i)$ Ово је тривијално јер сваки φ_{C_b} има ред q. Овиме завршавамо доказ целе леме.

Приметимо да из доказа претходне леме можемо закључити следеће: Нека су A и B матрице такве да су φ_A и φ_B реда q. Ако оне чувају исти правац D у $\mathbb{F}_q^2$ онда φ_A и φ_B генеришу исту подгрупу реда q у $PSL_2(q)$. Наиме, то важи јер у бази чији је

први вектор из D, обе матрице A и B имају облик C_λ за $\lambda \neq 0$, а тривијално се види да свака матрица облика C_λ за $\lambda \neq 0$ генерише целу подгрупу $\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_q \right\}$. Сада се можемо вратити доказу главне теореме. Тврдимо да H има јединствену подгрупу реда q. И заиста, како q дели ред групе H, онда знамо да у H постоји елемент реда q који генерише подгрупу реда q, дакле постоји бар једна подгрупа реда q. Претпоставимо сада да постоји две и назовимо их C_1 и C_2. На основу претходне леме и пропратног коментара закључујемо да генераторима ових двеју подгрупа одговарају два различита правца у $\mathbb{F}_q^2$ која су њима глобално фиксирана. Приметимо да генератори ових група постоје јер, по Кошијевој теореми, у групи реда q мора постојати елемент реда q за просте q. Онда посматрајмо базу простора $\mathbb{F}_q^2$ којој се први вектор налази у D_1, а други у D_2. У таквој бази генератори, а самим тим и одговарајуће подгрупе C_1 и C_2 имају следећи облик:

$$C_1 = \varphi \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in \mathbb{F}_q \right\} \quad \text{и} \quad C_2 = \varphi \left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in \mathbb{F}_q \right\}.$$

Но сада, лако се види да унија ове две подгрупе генерише цело $PSL_2(q)$, што значи да је $H = PSL_2(q)$, што је у контрадикцији са тим да је H права подгрупа од $PSL_2(q)$. Дакле, сада смо доказали да у H постоји јединствена подгрупа C реда q. Она због своје јединствености мора да буде нормална у H. У супротном можемо изабрати неки елемент $h \in H$ такав да је $hCh^{-1} \neq C$, а тривијално се види да је и hCh^{-1} подгрупа од H реда q. Сада, на основу горенаведене леме можемо наћи базу од $\mathbb{F}_q^2$ у којој је $C = \varphi \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in \mathbb{F}_q \right\}$. У оваквој бази C дејствује на $P^1(\mathbb{F}_q)$ као скуп транслација $z \mapsto z + \lambda$. Јединствена фиксна тачка целог C на $P^1(\mathbb{F}_q)$ је ∞, те уз чињеницу да је C нормална у H знамо да за свако $\varphi_A \in C$ и $\varphi_B \in H$ важи:

$$\varphi_A(\varphi_B(\infty)) = \varphi_B(\varphi_{B^{-1}AB}(\infty)) = \varphi_B(\infty).$$

Онда је $\varphi_B(\infty)$ фиксна тачка за $\varphi_A \in C$, те онда мора да буде $\varphi_B(\infty) = \infty$ за свако $\varphi_B \in H$. Ово значи да је H подгрупа стабилизатора елемента ∞ у $PSL_2(q)$, који је баш једнак:

$$B_0 = \varphi \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^\times \text{ и } b \in \mathbb{F}_q \right\}.$$

Ова група се назива Борелова група и она је скоро Абелова. Заиста, лако се проверава да је група $N = \varphi \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_q \right\}$ Абелова подгрупа групе B_0. Додатно, B_0/N је скуп косета елемената $\varphi \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^\times \right\}$, који такође чине Абелову групу. Онда је група H као подгрупа скоро Абелове групе B_0 такође скоро Абелова. Овиме завршавамо наш доказ. □

Наредни део овог поглавља је посвећен новом концепту који ће нам помоћи при анализи наших линеарних група - теорији репрезентација. Наиме, теорија репрезентација представља веома дубок концепт у математици који прожима огроман број

области - користи се у теорији група, Лијевој теорији, теорији бројева, квантној механици, комбинаторици... У даљем тексту увешћемо појам репрезентације неке групе и навешћемо пар основних теорема које су нам потребне за грубо разумевање ове теорије. Након тога навешћемо и теорему која се конкретно тиче групе $PSL_2(q)$ и коју ћемо користити у доказу да наши графови заиста чине фамилију експандера.

Дефиниција 3.9. Нека је G група. *Репрезентација групе* G је уређени пар (π, V), где је V комплексан векторски простор, а π је хомоморфизам $\pi : G \to GL(V)$, при чему је $GL(V)$ група линеарних трансформација простора V. *Степен* репрезентације (π, V) је комплексна димензија простора V, тј. $\dim_{\mathbb{C}} V$.

Наведимо и неке примере репрезентација:

(1) Константан хомоморфизам из G у $GL(V)$ представља *тривијалну репрезентацију* групе G на V;

(2) Сваки хомоморфизам $G \to \mathbb{C}^\times$ представља репрезентацију степена 1 групе G на $\mathbb{C}$;

(3) Нека је X коначан скуп, такав да G дејствује на X, тј. постоји хомоморфизам $G \to \mathrm{Sym}\,(X)$ и нека је са $\mathbb{C}X$ означен скуп свих функција $f : X \to \mathbb{C}$ (приметимо да је ово заправо комплексан векторски простор димензије $|X|$). Онда је *лева регуларна репрезентација* λ_X групе G на $\mathbb{C}G$ дефинисана коришћењем левог множења у G као:

$$(\lambda_G(g)f)(x) = f(g^{-1}x) \qquad (f \in \mathbb{C}G; \quad g, x \in G).$$

Десна регуларна репрезентација ρ_X групе G на $\mathbb{C}G$ дефинисана је коришћењем десног множења у G као:

$$(\rho_G(g)f)(x) = f(xg) \qquad (f \in \mathbb{C}G; \quad g, x \in G).$$

Дефиниција 3.10. Нека је (π, V) репрезентација групе G. Потпростор W простора V је *инваријантан* ако за свако $g \in G$ важи $\pi(g)(W) = W$. Рестрикција наше репрезентације на W даје нову репрезентацију $(\pi|_W, W)$ која се назива *подрепрезентација* репрезентације (π, V). Потпростори 0 и V се називају *тривијални* инваријантни потпростори.

Дефиниција 3.11. Репрезентација (π, V), $V \neq 0$ је *иредуцибилна* ако не постоји ни један нетривијалан потпростор од V инваријантан у односу на (π, V).

Дефиниција 3.12. Нека су (π, V) и (ρ, W) две репрезентације групе G. Линеарно пресликавање $T : V \to W$ за које важи $T\pi(g) = \rho(g)T$, за свако $g \in G$, назива се *интертвајнер* између π и ρ. Кажемо да су две репрезентације π и ρ групе G *еквивалентне* ако постоји инвертибилни интертвајнер који их повезује тј. постоји T такав да за све $g \in G$ важи $\rho(g) = T\pi_g T^{-1}$.

Приметимо да претходна дефиниција подразумева да, ако је T интертвајнер између π и ρ, онда следећи дијаграм комутира:

$$\begin{array}{ccc} & V & \stackrel{\pi(g)}{\to} & V & \\ T & \downarrow & & \downarrow & T \\ & W & \stackrel{\rho(g)}{\to} & W & \end{array}.$$

Дефиниција 3.13. *Директна сума* репрезентација (π, V) и (ρ, W) групе G, у ознаци $(\pi \oplus \rho, V \oplus W)$, је такође репрезентација групе G на $V \oplus W$, дефинисана као:

$$(\pi \oplus \rho)(g)(v, w) = (\pi(g)v, \rho(g)w) \qquad (g \in G, v \in V, w \in W).$$

Сада стижемо до две теореме које представљају основне резултате који се тичу репрезентације коначних група.

Теорема 3.3. Свака репрезентација (π, V), $V \neq 0$ коначне групе G може се записати као директна сума коначно много иредуцибилних репрезентација

$$\pi = \rho_1 \oplus \cdots \oplus \rho_k.$$

Штавише, ово растављање је јединствено до на распоред и еквивалентност иредуцибилних компонената.

Теорема 3.4. Нека је $(\rho_1, W_1), \ldots, (\rho_h, W_h)$ листа свих иредуцибилних репрезентација коначне групе G до на еквиваленцију и нека је $n_i = \dim_{\mathbb{C}} W_i$ степен репрезентације ρ_i. Онда важи $|G| = \sum_{i=1}^{h} n_i^2$.

Дакле, сваку нетривијалну репрезентацију коначне групе G можемо разложити на иредуцибилне, а иредуцибилних репрезентација има коначно много. Додатно, збир квадрата њихових димензија је једнак величини групе G. Надаље, теорија репрезентација постаје специфична за сваку групу. Не постоји универзални алат којим можемо наћи све иредуцибилне репрезентације неке групе, али за конкретну групу која нам је потребна можемо исконструисати одређени број репрезентација, и ако квадрати њихових димензија у збиру дају G, знамо да смо их пронашли све.

Следећи резултат односиће се на иредуцибилне репрезентације групе $PSL_2(q)$.

Теорема 3.5. Нека је $q \geqslant 5$ прост број. Онда свака нетривијална репрезентација групе $PSL_2(q)$ има степен бар $\dfrac{q-1}{2}$.

Ова теорема има леп доказ који се заснива на најпре карактеризацији репрезентација Борелове групе, која је једноставнија од $PSL_2(q)$, а онда у неком смислу „усложњавања" тих репрезентација тако да од њих добијемо репрезентације групе $PSL_2(q)$. Но, мање више „праволинијски" доказ би био наћи листу свих иредуцибилних репрезентација групе $PSL_2(q)$, из које се тривијално види да је степен сваке од њих већи једнак од $\dfrac{q-1}{2}$. Заинтересовани читаоци могу наћи у литератури књигу [DSV] у којој је исписан доказ претходне тврдње.

Ради бољег разумевања претходних концепата можете проучити листу иредуцибилних репрезентација групе S_3 као најједноставнији могући пример, која се налази у књизи [E]. У овој књизи налази се још пар листа иредуцибилних репрезентација за више основних група (међу којима су и $GL_2(q)$ и $PGL_2(q)$), као и доказ претходних теорема о репрезентацијама коначних група, заједно са значајно дубљим резултатима теорије репрезентација.

3.4 Конструкција графа $X^{p,q}$

Нека су p и q различити прости бројеви. У поглављу 3.2 смо дефинисали скуп S_p који се састоји од $p+1$ целих кватерниона норме p.

Посматрајмо редукцију модуло q:

$$\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q).$$

Присетимо се леме 3.2. Претходним кораком смо кватернионе над прстеном целих бројева идентификовали са кватернионима над пољем $\mathbb{F}_q$ карактеристике $q \neq 2$, те сада користећи лему можемо њих идентификовати са матрицама 2×2 над $\mathbb{F}_q$. Потребно је само да докажемо да постоје $x, y \in \mathbb{F}_q$ такви да је $x^2 + y^2 + 1 = 0$. Заиста, у $\mathbb{F}_q$ постоји тачно $\frac{q+1}{2}$ квадрата рачунајући и 0 ($\frac{q+1}{2}$ квадратних остатака модуло q), стога су кардиналности скупова

$$A_+ = \{1 + x^2 : x \in \mathbb{F}_q\}, \qquad A_- = \{-y^2 : y \in \mathbb{F}_q\}$$

баш $\frac{q+1}{2}$, те та два скупа имају непразан пресек. Изаберимо један пар таквих x, y и посматрајмо њима одређен изоморфизам

$$\psi_q : \mathbb{H}(\mathbb{F}_q) \to M_2(\mathbb{F}_q).$$

Лако се проверава да за овај изоморфизам важе следећа тврђења:

(а) $N(\alpha) = \det(\psi_q(\alpha))$ за све $\alpha \in \mathbb{H}(\mathbb{F}_q)$;

(б) ако је α „реалан" кватернион, тј. ако је $\alpha = \overline{\alpha}$ онда је $\psi_q(\alpha)$ скаларна матрица.

За $\alpha \in S_p$ матрица $\psi_q(\tau_q(\alpha))$ припада групи инвертибилних матрица $GL_2(q)$ прстена $M_2(\mathbb{F}_q)$, јер је $N(\alpha) = p \neq q$. Такође $\psi_q(\tau_q(\alpha\overline{\alpha})) = \psi_q(\tau_q(\overline{\alpha}\alpha))$ је ненула скаларна матрица у $GL_2(q)$. Сада даље компонујемо наше пресликавање са пресликавањем

$$\varphi : GL_2(q) \to PGL_2(q),$$

чије је језгро тачно подгрупа скаларних матрица.
Нека је:

$$S_{p,q} = (\varphi \circ \psi_q \circ \tau_q)(S_p).$$

На основу својстава компонованих хомоморфизама закључујемо да за свако $\alpha_i \in S_p$ важи $\overline{\alpha_i} \in S_p$ и $(\varphi \circ \psi_q \circ \tau_q)(\alpha_i\overline{\alpha_i}) = \mathrm{Id}$, а за свако $\beta_i \in S_p$ важи $(\varphi \circ \psi_q \circ \tau_q)(\beta_i^2) = \mathrm{Id}$. Дакле сваки члан из $S_{p,q}$ има инверз у $S_{p,q}$, тј. $S_{p,q}$ је симетричан подскуп групе $PGL_2(q)$.

Лема 3.7. Ако је q довољно велико у односу на p (нпр. ако је $q > 2\sqrt{p}$) скуп $S_{p,q}$ има $p+1$ елемената.

Доказ. Нека су $\alpha = a_0+a_1i+a_2j+a_3k$ и $\beta = b_0+b_1i+b_2j+b_3k$ различити кватерниони из S_p. Онда постоји $i \in \{0,1,2,3\}$ такво да је $a_i \neq b_i$. Како је $N(\alpha) = N(\beta) = p$ имамо да је $-\sqrt{p} < a_i, b_i < \sqrt{p}$, те ако је $q > 2\sqrt{p}$ знамо да је $a_i \neq b_i \pmod q$ тј. $\tau_q(\alpha) \neq \tau_q(\beta)$. Даље, на основу дефиниције пресликавања ψ_q закључујемо и да је $A = (\psi_q \circ \tau_q)(\alpha)$ различито од $B = (\psi_q \circ \tau_q)(\beta)$ у $GL_2(q)$. Сада, ради контрадикције претпоставимо да је $\varphi(A) = \varphi(B)$. То значи да постоји скалар $\lambda \in \mathbb{F}_q^\times, \lambda \neq 1$ такав да је $A = \lambda B$. Када узмемо детерминанту добијамо $p = \det A = \lambda^2 \det B = \lambda^2 p \Rightarrow \lambda^2 = 1 \Rightarrow \lambda = -1$ (сетимо се $\lambda \neq 1$). Дакле $A = -B$, из чега следи $\alpha \equiv -\beta \pmod q$; тј. $a_i \equiv -b_i \pmod q$ за $i \in \{0,1,2,3\}$, но уз услов $q > 2\sqrt{p}$ закључујемо и да је $\alpha = -\beta$. По дефиницији скупа S_p имамо $a_0, b_0 \geqslant 0$ те мора да важи $a_0 = b_0 = 0 \Rightarrow \alpha = \overline{\beta}$, што води у контрадикцију јер смо скуп S_p бирали тако да, ако је $\alpha \in S_{p,q}$ и $a_0 = 0$, онда $\overline{\alpha} \notin S_{p,q}$. Уз чињеницу да је $|S_p| = p+1$ завршавамо наш доказ. □

Ако је p квадратни остатак модуло q, тј. $\left(\frac{p}{q}\right) = 1$, скуп $S_{p,q}$ је заправо подскуп $PSL_2(q)$. Заиста, нека је $\alpha \in S_p$. Означимо $(\psi_q \circ \tau_q)(\alpha)$ са A. Онда је $\det A = p^k$. Како је $\left(\frac{p}{q}\right) = 1$ знамо да постоји $x \in \mathbb{F}_q^\times$ такво да је $x^2 \equiv p^k \pmod q$. Сада тривијално закључујемо да се матрица $A \in GL_2(q)$ налази у косету неке матрице $B \in SL_2(q) \subset GL_2(q)$ чија је детерминанта 1 ($B \cdot \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} = A$). Дакле не само да се $\varphi(A)$ налази у $PGL_2(q)$ већ се налази и у $PSL_2(q)$. Конструишимо сада граф $X^{p,q}$ као Кејлијев граф

$$X^{p,q} = \mathcal{G}(PSL_2(q), S_{p,q}).$$

Ако p није квадратни остатак модуло q, тј. $\left(\frac{p}{q}\right) = -1$, слично као у претходном случају закључујемо да је $S_{p,q} \subset PGL_2(q) - PSL_2(q)$. Сада $X^{p,q}$ дефинишемо као Кејлијев граф

$$X^{p,q} = \mathcal{G}(PGL_2(q), S_{p,q}).$$

3.5 Конструкција графа $Y^{p,q}$

Циљ овог поглавља је конструкција друге фамилије графова $Y^{p,q}$, за коју ће се испоставити да је изоморфна графовима $X^{p,q}$. Штавише, за графове $Y^{p,q}$ ћемо моћи да докажемо пар лепих својстава, међу којима је и повезаност, која ће бити значајна за разумевање њихове структуре, као и за доказ да наши графови заиста јесу експандери.

Нека је p непаран прост број. Сетимо се да смо у поглављу о кватернионима дефинисали скуп $\Lambda' \subset \mathbb{H}(\mathbb{Z})$ као:

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod 2 \text{ или } \alpha \equiv i+j+k \pmod 2,\ N(\alpha) = p^k \text{ за неко } k \in \mathbb{N}\}.$$

Дефинишимо на Λ' релацију еквиваленције $\sim : \alpha \sim \beta$ ако постоје $m, n \in \mathbb{N}$ такви да је $p^m\alpha = \pm p^n\beta$. Са $[\alpha]$ ћемо означавати класу еквиваленције елемента $\alpha \in \Lambda'$, а са $\Lambda = \Lambda'/\sim$ ћемо означити скуп ових класа еквиваленција. Са

$$\pi_\sim : \Lambda' \to \Lambda$$

означимо пресликавање које слика α у $[\alpha]$. Приметимо да је операција множења добро дефинисана и на скупу Λ: $\alpha_1 \sim \alpha_2$ и $\beta_1 \sim \beta_2 \Rightarrow \alpha_1\beta_1 \sim \alpha_2\beta_2$. Штавише Λ са операцијом множења чини групу. Лако уочавамо да је множење асоцијативно, као и да постоји јединица. Што се тиче инверза ако $\alpha \in \Lambda'$ онда је и $\overline{\alpha} \in \Lambda'$, те уз $\alpha\overline{\alpha} = \overline{\alpha}\alpha \sim 1$ добијамо $[\alpha]^{-1} = [\overline{\alpha}] \in \Lambda$.
Као и код графова $X^{p,q}$, желимо да целе кватернионе са којима располажемо претворимо у кватернионе над пољем $\mathbb{F}_q$. Но, како ћемо у овом случају радити са класама еквиваленције, а не са самим кватернионима морамо пазити да добро дефинишемо пројекцију која ће поштовати релацију еквиваленције.
Дакле, раније смо посматрали обичну редукцију модуло q:

$$\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q),$$

која Λ' шаље у групу $\mathbb{H}(\mathbb{F}_q)^\times$ инвертибилних елемената из $\mathbb{H}(\mathbb{F}_q)$. Уочимо централну подгрупу Z_q групе $\mathbb{H}(\mathbb{F}_q)^\times$:

$$Z_q = \{\alpha \in \mathbb{H}(\mathbb{F}_q)^\times : \alpha = \overline{\alpha}\}.$$

Централна подгрупа неке групе је свака подгрупа те групе која се налази у центру те групе; *центар* групе чине сви елементи те групе који комутирају са свим осталим елементима групе. Посматрајмо групу $\mathbb{H}(\mathbb{F}_q)^\times/Z_q$. Уколико важи $\alpha, \beta \in \Lambda'$ и $\alpha \sim \beta$, онда су $\tau_q(\alpha)$ и $\tau_q(\beta)$ у истом косету централне групе Z_q ($\tau_q(\alpha)\tau_q(\beta)^{-1} = \tau_q(\alpha\beta^{-1}) = \tau_q(p^k) \in Z_p$). Дакле $\tau_q : \Lambda' \to \mathbb{H}(\mathbb{F}_q)^\times$ се на нивоу количничких група своди на добро дефинисани хомоморфизам:

$$\Pi_q : \Lambda \to \mathbb{H}(\mathbb{F}_q)^\times.$$

Означимо са $\operatorname{Im}\Pi_q$ слику скупа Λ при овом пресликавању. Како знамо да постоји добро дефинисан изоморфизам који шаље $\Lambda/\ker\Pi_q$ у $\operatorname{Im}\Pi_q$, надаље ћемо у тексту ове две групе поистоветити. Нека је $T_{p,q} = (\Pi_q \circ \pi_\sim)(S_p)$. Као и у претходном поглављу код графова $X^{p,q}$, за довољно велико q (наиме, $q > 2\sqrt{p}$) имаћемо $|T_{p,q}| = p + 1$. Дефинишимо сада граф $Y^{p,q}$ као Кејлијев граф:

$$Y^{p,q} = \mathcal{G}(\Lambda/\ker\Pi_q, T_{p,q}).$$

Како је $|T_{p,q}| = p + 1$, $Y^{p,q}$ је $p + 1$-регуларан. Докажимо и да је повезан. На основу леме 3.1, да бисмо доказали да је граф $Y^{p,q}$ повезан довољно је да докажемо да $T_{p,q}$ генерише $\Lambda/\ker\Pi_q$. Но, због конструкције, ово би следило из чињенице да $\pi_\sim(S_p)$ генерише Λ. И заиста, на основу последице 4 сваки кватернион $\alpha \in \Lambda'$ еквивалентан је некој редукованој речи над S_p, те је очигледно да $\pi_\sim(S_p)$ генерише Λ.

У претходном поглављу смо у овом тренутку увели и изоморфизам $\psi_q : \mathbb{H}(\mathbb{F}_q)^\times \to GL_2(q)$. Погледајмо шта се дешава са овим изоморфизмом сада када радимо са

количничким групама. Приметимо да ψ_q шаље Z_q у групу инвертибилних скаларних матрица у $GL_2(q)$, које заправо формирају језгро пресликавања $\varphi : GL_2(q) \to PGL_2(q)$. Због овога се изоморфизам ψ_q своди на добро дефинисан изоморфизам

$$\beta : \mathbb{H}(\mathbb{F}_q)^\times / Z_q \to PGL_2(q).$$

Сада можемо, уз помоћ следећег комутирајућег дијаграма упоредити конструкције графова $X^{p,q}$ и $Y^{p,q}$.

$$\begin{array}{ccccc} S_p \subset \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^\times & \xrightarrow{\psi_q} & GL_2(q) \\ \downarrow \pi_\sim & & \downarrow & & \downarrow \varphi \\ \Lambda & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^\times / Z_q & \xrightarrow{\beta} & PGL_2(q) \end{array}$$

За сада знамо од које групе је настао граф $X_{p,q}$ - у случају да је p квадратни остатак модуло q то је $PSL_2(q)$, а ако је неостатак то је група $PGL_2(q)$, али не знамо да је $X^{p,q}$ повезан. У случају графа $Y^{p,q}$ смо доказали да је он повезан, али нисмо идентификовали групу $\Lambda/\ker \Pi_q$ од које је овај граф настао, па самим тим немамо информацију о његовом броју чворова. Међутим, са претходног комутирајућег дијаграма се види да је $\beta(T_{p,q}) = S_{p,q}$ па свакако знамо да је $Y^{p,q}$ повезана компонента графа $X^{p,q}$. Поредећи даље ове графове, утврдићемо да је $X^{p,q}$ повезан за $q > p^8$ па су графови $Y^{p,q}$ и $X^{p,q}$ изморфни.

Проучимо мало боље комбинаторна својства графа $Y^{p,q}$. Дужина најкраћег циклуса у неком графу је веома битно својство неког графа и биће од велике важности у нашем доказу. Такође, помоћу ње ћемо моћи да пронађемо доњу оцену за број чворова нашег графа, што је веома значајно јер до сада нисмо нашли ни једну информацију о овој величини. Наиме:

Лема 3.8. Нека је $g(Y^{p,q})$ дужина најкраћег циклуса у графу $Y^{p,q}$. Онда је $2\log_p |Y^{p,q}| + 2 \geqslant g(Y^{p,q})$, при чему је са $|Y^{p,q}|$ означен број чворова тог графа.

Доказ. Ако је $g(Y^{p,q})$ паран, нека је $r = \dfrac{g(Y^{p,q}) - 2}{2}$, а ако је $g(Y^{p,q})$ непаран, нека је $r = \dfrac{g(Y^{p,q}) - 1}{2}$. У оба случаја је $\dfrac{g(Y^{p,q})}{2} - 1 \leqslant r < \dfrac{g(Y^{p,q})}{2}$. Посматрајмо фиксиран чвор $x_0 \in Y^{p,q}$ и посматрајмо подграф W графа $Y^{p,q}$ који чине сви чворови који су на растојању не већем од r од чвора x_0. Растојање два чвора је број ивица које садржи најкраћи пут између та два чвора. Тврдимо да је W дрво и да сваки чвор који није лист има тачно $p+1$ суседа. Ово је очигледно, јер уколико би постојао циклус унутар W, онда би у $Y^{p,q}$ постојао циклус чија је дужина $\leqslant 2r < g(Y^{p,q})$ контрадикција. Даље, уколико је чвор x_1 на растојању строго мањем од r од чвора x_0, онда су и свих његових $p+1$ суседа из $Y^{p,q}$ (сетимо се, $Y^{p,q}$ је $p+1$-регуларан) на растојању мањем или једнаком од r од x_0 те се налазе у W. Сада лако добијамо да се у W налази тачно $\dfrac{(p+1)p^r - 2}{p-1}$ чворова. Онда је:

$$\frac{(p+1)p^r - 2}{p-1} \leqslant |Y^{p,q}|$$

$$p^r \leqslant \frac{(p-1)|Y^{p,q}|+2}{p+1},$$

што је након логаритмовања

$$\frac{g(Y^{p,q})}{2} - 1 \leqslant r \leqslant \log_p \frac{(p-1)|Y^{p,q}|+2}{p+1} \leqslant \log_p \frac{(p+1)|Y^{p,q}|}{p+1} = \log_p |Y^{p,q}|,$$

што сређивањем даје тражену неједнакост. □

Како смо конструисали граф $Y^{p,q}$ као специјалан Кејлијев граф, можемо наћи и доњу оцену за дужину најкраћег циклуса:

Теорема 3.6. Најкраћи циклус у графу $Y^{p,q}$ је дужине бар $g(Y^{p,q}) \geqslant 2\log_p q$. Ако је p квадратни неостатак модуло q важи још боља неједнакост: $g(Y^{p,q}) \geqslant 4\log_p q - \log_p 4$.

Доказ. Ради једноставности записа уместо $g(Y^{p,q})$ писаћемо само g. Нека су $x_0, x_1, \ldots,$ $x_g = x_0$ чворови који формирају циклус дужине g. Уз чињеницу да граф $Y^{p,q}$ као Кејлијев граф има особину транзитивности, можемо без умањења општости да претпоставимо да је $x_0 = x_g = 1$ у $\Lambda/\ker\Pi_q$. Такође, због тога што је $Y^{p,q}$ Кејлијев граф, знамо да постоје $t_1, t_2, \ldots, t_g \in T_{p,q}$ такви да је

$$x_i = t_1 t_2 \cdots t_i, \qquad (i = 1, 2, \ldots, g).$$

Сада, због конструкције скупа $T_{p,q}$, имамо да постоје $\gamma_i \in S_p$ за $i \in \{1, 2, \ldots, g\}$ такви да је $t_i = \Pi_q([\gamma_i])$. Нека је $\alpha \in \Lambda'$ такво да је $\alpha = \gamma_1\gamma_2\cdots\gamma_g$ и нека је $\alpha = a_0 + a_1 i + a_2 j + a_3 k$; знамо да је $\gamma_1\gamma_2\cdots\gamma_g$ заправо редукована реч над S_p, јер је $x_{k-1} \neq x_{k+1}$ за $k \in \{1, 2, \ldots, g-1\}$. Заиста, уколико се појаве заредом α_i и $\overline{\alpha_i}$ или се два пута заредом појави β_i, то значи да смо у нашем најкраћем циклусу прешли исту грану два пута ($\delta\alpha_i\overline{\alpha_i} \sim \delta$), па самим тим изабрани циклус није најкраћи, контрадикција.
Знамо да је $t_1 t_2 \cdots t_g = 1$ у $\Lambda/\ker\Pi_q$, па хајде да погледамо да ли је и $[\gamma_1][\gamma_2]\cdots[\gamma_g] = [1]$ у Λ. Претходни израз можемо записати на следећи начин: постоје $m, n \in \mathbb{N}$ такви да је $p^m = \pm p^n \gamma_1\gamma_2\cdots\gamma_g$. Но $\gamma_1\gamma_2\cdots\gamma_g$ је нетривијална редукована реч над S_p, тако да због јединствености факторизације доказаној у теореми 3.2, долазимо до контрадикције. Дакле $[\alpha] \neq [1]$ у Λ тј. α није еквивалентно са 1 у Λ'. Ово значи да је бар један од a_1, a_2, a_3 раличит од нуле.
Са друге стране $\Pi_q([\alpha]) = 1$, па $[\alpha] \in \ker\Pi_q \Leftrightarrow \tau_q(\alpha) \in Z_p \Leftrightarrow q \nmid a_0$ и $q | a_1, a_2, a_3$. Како је бар један од њих различит од нуле, имамо да је

$$q^2 \leqslant a_0^2 + a_1^2 + a_2^2 + a_3^2 = N(\alpha) = p^g.$$

Из овога логаритмовањем директно добијамо $g \geqslant 2\log_p q$, чиме завршавамо први део доказа.
Претпоставимо сад да је $\left(\frac{p}{q}\right) = -1$. Како је

$$p^g = N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 \equiv a_0^2 \pmod{q^2} \Rightarrow p^q \equiv a_0^2 \pmod{q}$$

и како је:

$$1 = \left(\frac{p^g}{q}\right) = \left(\frac{p}{q}\right)^g = (-1)^g,$$

имамо да је g паран број тј. $g = 2h$ за неко $h \in \mathbb{N}$. Онда је

$$p^{2h} \equiv a_0^2 \pmod{q^2}$$

$$q^2 | (p^{2h} - a_0^2) = (p^h - a_0)(p^h + a_0)$$

$$\Rightarrow p^h \equiv \pm a_0 \pmod{q^2},$$

јер $(p^h - a_0, p^h + a_0) | 2a_0$, а $q \nmid a_0$. Додатно $a_0^2 \leqslant p^g \Rightarrow |a_0| \leqslant p^h$. Претпоставимо да је $g < 4\log_p q - \log_p 4 = \log_p \frac{q^4}{4}$; дакле $p^{2h} < \frac{q^4}{4} \Rightarrow p^h < \frac{q^2}{2}$. Онда је и $|a_0| < p^h < \frac{q^2}{2} \Rightarrow |p^h \pm a_0| < q^2$. Уз $p^h \equiv \pm a_0 \pmod{q^2}$, добијамо $p^h = \pm a_0 \Rightarrow p^g = a_0 \Rightarrow a_1, a_2, a_3 = 0$, где долазимо до контрадикције са $[\alpha] \neq 1$. Дакле $g \geqslant 4\log_p q - \log_p 4$ чиме завршавамо овај доказ. □

Комбиновањем последња два тврђења добијамо следећу последицу:

Последица 5. $2\log_p q \leqslant g(Y^{p,q}) \leqslant 2\log_p |Y^{p,q}| + 2 \Rightarrow \frac{q}{p} \leqslant |Y^{p,q}|$

Сада имамо све што нам је потребно да докажемо да је граф $X^{p,q}$ повезан.

Теорема 3.7. Нека је $p \geqslant 5$ и $q > p^8$. Онда је граф $X^{p,q}$ повезан. Додатно, изоморфан је са $Y^{p,q}$.

Доказ. На основу леме 3.1, да бисмо доказали да је $X^{p,q}$ повезан, довољно је да докажемо да $S^{p,q}$ генерише $PSL_2(q)$ ако је $\left(\frac{p}{q}\right) = 1$, односно $PGL_2(q)$ ако је $\left(\frac{p}{q}\right) = -1$. Како S_p генерише цело Λ и Π_q је хомоморфизам, да бисмо доказали да $\beta(T_{p,q}) = S_{p,q}$ генерише цело $PSL_2(q)$, односно $PGL_2(q)$, довољно је да докажемо да $\beta(\mathrm{Im}\ \Pi_q)$ генерише одговарајућу пројективну линеарну групу. Раније у тексту смо нагласили да ћемо идентификовати $\mathrm{Im}\ \Pi_q$ са $\Lambda/\ker \Pi_q$, те сада желимо да докажемо да

$$\beta(\Lambda/\ker \Pi_q) \text{ генерише } \begin{cases} PSL_2(q), & \text{ако } \left(\frac{p}{q}\right) = 1; \\ PGL_2(q), & \left(\frac{p}{q}\right) = -1. \end{cases}$$

Нека је $H_{p,q} = PSL_2(q) \cap \beta(\Lambda/\ker \Pi_q)$.
Тврђење: За доказ теореме у оба случаја довољно да покажемо да важи $H_{p,q} = PSL_2(q)$.

Доказ тврђења. Ако је p квадратни остатак модуло q тврђење је очигледно. Сада претпоставимо да је p квадратни неостатак. Раније смо доказали да је $S_{p,q} \subset PGL_2(q) - PSL_2(q) \Rightarrow \exists A \in S_{p,q}$ такво да је $A \in PGL_2(q) - PSL_2(q)$. Нека је B било која матрица из $PGL_2(q) - PSL_2(q)$; онда матрица $A^{-1} \cdot B$ припада $PSL_2(q)$ зато што јој

је детерминанта квадратни остатак модуло q (неостатак пута неостатак даје остатак). Уз претпоставку $H_{p,q} = PSL_2(q)$ имамо да је $A^{-1} \cdot B$ генерисано елементима скупа $\beta(\Lambda/\ker\Pi_q)$. Сада је тривијално и $A\cdot(A^{-1}B) = B$ генерисана елементима скупа $S_{p,q} \Rightarrow$ цео скуп $PGL_2(q)$ је изгенерисан скупом $\beta(\Lambda/\ker\Pi_q)$, што је и требало доказати. □

Вратимо се сад на доказ. Присетимо се леме 3.6. Она нам говори, заједно са претходним тврђењем, да је за завршетак доказа довољно да докажемо да је $|H_{p,q}| > 60$ и да H није скоро Абелова група. Заиста, онда $H_{p,q}$, као подгрупа од $PSL_2(q)$ која није скоро Абелова и има више од 60 елемената, не може бити права подгрупа, већ мора бити баш једнака групи $PSL_2(q)$.
Најпре се уверимо да је $|H_{p,q}| > 60$. Заиста, како је $p \geqslant 5$ и $q > p^8$, на основу претходне последице имамо:

$$|Y^{p,q}| = |\Lambda/\ker\Pi_q| \geqslant \frac{q}{p} > 120.$$

Присетимо се следеће теореме из алгебре:
Теорема */Друга теорема о изоморфизмима/* Нека је G група, S њена подгрупа и N њена нормална подгрупа. Онда важи:

(1) производ SN је подгрупа од G,

(2) пресек $S \cap N$ је нормална подгрупа групе G,

(3) групе $(SN)/N$ и $S/(S \cap N)$ су изоморфне.

Нека је овде $G = PGL_2(q)$, $N = PSL_2(q)$ и $S = \beta(\Lambda/\ker\Pi_q)$ (S је група јер је β изоморфизам, Λ је група, а $\ker\Pi_q$ је њена нормална подгрупа). Онда је $H_{p,q} = S \cap N = PSL_2(q) \cap \beta(\Lambda/\ker\Pi_q)$, а $SN = PSL_2(q) \cdot \beta(\Lambda/\ker\Pi_q)$. У случају да је $\beta(\Lambda/\ker\Pi_q) \subset PSL_2(q)$ аутоматски имамо $|H_{p,q}| = |\beta(\Lambda/\ker\Pi_q)| > 120 > 60$, те нам преостаје да погледамо случај где је $\beta(\Lambda/\ker\Pi_q) \cap (PGL_2(q) - PSL_2(q)) \neq \emptyset$. У доказу теореме смо већ показали да у овом случају $\beta(\Lambda/\ker\Pi_q) \cdot PSL_2(q)$ генерише цело $PGL_2(q)$ те је $SN = PGL_2(q)$. Онда из дела (3) имамо да је :

$$PGL_2(q)/PSL_2(q) \cong \beta(\Lambda/\ker\Pi_q)/H_{p,q}.$$

Како смо у леми 3.4 доказали да је $|PGL_2(q)| = 2 \cdot |PSL_2(q)|$, из претходног следи да је $|\beta(\Lambda/\ker\Pi_q)| = 2|H_{p,q}|$ тј. $|H_{p,q}| = \dfrac{|\beta(\Lambda/\ker\Pi_q)|}{2} > \dfrac{120}{2} = 60$. Овиме завршавамо доказ да је $|H_{p,q}| > 60$.
Сада покажимо да $H_{p,q}$ није скоро Абелова. Према леми 3.5 довољно је да пронађемо $g_1, g_2, g_3, g_4 \in H_{p,q}$ такве да

$$[[g_1, g_2], [g_3, g_4]] \neq 1.$$

Испитајмо два случаја:

(a) Ако је $\left(\dfrac{p}{q}\right) = 1$: $S_{p,q} = \beta(T_{p,q}) \subset PSL_2(q)$ и $T_{p,q} \subset \Lambda/\ker\Pi_q \Rightarrow S_{p,q} \subset H_{p,q}$. Онда за g_1 изаберимо било који елемент из $S_{p,q}$. За g_2 изаберимо било који елемент $S_{p,q}$ различит од $g_1^{\pm 1}$. Нека је $g_3 = g_1$ и нека је g_4 било који елемент

$S_{p,q}$ који је различит од $g_1^{\pm 1}$ и $g_2^{\pm 1}$. Онда је $[[g_1, g_2], [g_3, g_4]]$ редукована реч над $S_{p,q}$ дужине 16. Претпоставимо да је ова реч једнака 1. Како је пресликавање β изоморфизам, у графу $Y^{p,q}$ онда постоји циклус дужине 16 који одговара датој речи, али то је у контрадикцији са теоремом 3.6 која каже:

$$g(Y^{p,q}) \geqslant 2 \log_p q > 16,$$

због претпоставке $q > p^8$. Овиме завршавамо доказ у овом случају.

(б) Ако је $\left(\frac{p}{q}\right) = -1$ знамо да $S_{p,q} \subset PGL_2(q) - PSL_2(q)$ па било који производ два елемента из $S_{p,q}$ припада $PSL_2(q)$, а самим тим и скупу $H_{p,q}$. Нека је h_1 било који елемент из $S_{p,q}$; нека је $h_2 \in S_{p,q} - \{h_1^{\pm 1}\}$; нека је $h_3 \in S_{p,q} - \{h_1^{\pm 1}, h_2^{\pm 1}\}$. Изаберимо онда $g_1 = h_1 h_3, g_2 = h_2 h_3, g_3 = h_1 h_2, g_4 = h_2 h_3 \in H_{p,q}$. Расписивањем видимо да је $[[g_1, g_2], [g_3, g_4]]$ редукована реч над $S_{p,q}$ дужине 24, па уз помоћ теореме 3.6 завршавамо доказ као и у претходном случају:

$$g(Y^{p,q}) \geqslant 4 \log_p q - \log_p 4 > 24.$$

Дакле, овиме смо доказали да је граф $X^{p,q}$ повезан, а како смо раније напоменули, $Y_{p,q}$ је његова повезана компонента $\Rightarrow X^{p,q}$ и $Y^{p,q}$ су изоморфни. □

4

Доказ - спектралне оцене

У претходном поглављу смо конструисали две изоморфне фамилије графова $X^{p,q}$ и $Y^{p,q}$. Наш задатак у овом поглављу биће да докажемо да за фиксирано p оне јесу заправо фамилије експандера, и то ћемо учинити тако што ћемо пронаћи горњу границу спектралног размака ових графова за довољно велике q. Ови графови ће заправо бити и Раманујанови графови (за које смо рекли да су оптимални експандери), но како смо најавили на почетку рада, тај доказ је превише теоријски захтеван. Упркос томе, доказ да су наши графови заправо Раманујанови прати овај доказ до једне тачке (наиме, формуле (♠)), а кључна разлика настаје код проналажења горње оцене, где ћемо ми искористити елементаран резултат из теорије бројева, а Лубоцки, Филипс и Сарнак посежу за оценом која је последица Раманујанове хипотезе из модуларних форми. Заинтересовани читаоци могу наћи потпун доказ у Сарнаковој књизи [S].

Темељ нашег доказа биће последица 3. Она нам даје нумеричку карактеризацију сопствених вредности која ће послужити за оцену спектралног размака. Ту последицу можемо искористити јер је граф $X^{p,q}$ транзитиван и $(p+1)-$регуларан граф (као Кејлијев граф над скупом кардиналности $p+1$). Означимо са n број чворова грава $X^{p,q}$ који смо израчунали у леми 3.4. Нека је, као и раније, спектар графа $X^{p,q}$ означен са $\mu_0 = p+1 \geqslant \mu_1 \geqslant \cdots \geqslant \mu_{n-1}$. Онда формула из последице добија следећи облик:

$$\sum_{0 \leqslant r \leqslant \frac{m}{2}} f_{m-2r} = \frac{p^{\frac{m}{2}}}{n} \sum_{j=0}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{p}}\right).$$

Десна страна претходне једнакости нас мотивише да, ради веће једноставности, посматрамо смену променљиве која x шаље у $2\sqrt{p}\cos x$, којом ћемо сопствене вредности μ_j записати као $2\sqrt{p}\cos\theta_j$. Овакво пресликавање скуп

$$\Theta_p = [i\log\sqrt{p}, 0] \cup [0, \pi] \cup [\pi, \pi + i\log\sqrt{p}]$$

шаље у реалан интервал $[-p-1, p+1]$; штавише, оно је бијекција и шаље интервал $[0,\pi]$ у Раманујанов интервал $[-2\sqrt{p}, 2\sqrt{p}]$. Дакле, свакој сопственој вредности μ_j одговара јединствено $\theta_j \in \Theta_p$, такво да је $\mu_j = 2\sqrt{p}\cos\theta_j$. У оваквим ознакама,

горенаведен идентитет постаје:

$$\sum_{0\leqslant r\leqslant \frac{m}{2}} f_{m-2r} = \frac{p^{\frac{m}{2}}}{n}\sum_{j=0}^{n-1}\frac{\sin(m+1)\theta_j}{\sin\theta_j}. \qquad (*)$$

Нестандардна ознака интервала у комплексним бројевима означава дуж у комплексној равни са почетком у првој тачки „интервала", а крајем у другој. Додатно, косинус и синус комплексних бројева су дефинисани као

$$\cos z = \sum_{n=0}^{\infty}(-1)^n\frac{z^{2n}}{(2n)!} = \frac{e^{iz}+e^{-iz}}{2} \quad \text{и} \quad \sin z = \sum_{n=0}^{\infty}(-1)^n\frac{z^{2n+1}}{(2n+1)!} = \frac{e^{iz}-e^{-iz}}{2i}.$$

У оваквим ознакама, да бисмо доказали да је граф $X^{p,q}$ Раманујанов требало би доказати да су сви θ_j који одговарају нетривијалним сопственим вредностима *реални*. Како смо већ рекли, тај доказ је превише компликован и у даљем тексту ћемо доказати да је, за довољно велико q, имагинаран део бројева θ_j који одговарају нетривијалних сопственим вредностима ограничен одозго константом која зависи само од p.

Да бисмо то урадили, покушајмо да запишемо десну страну једнакости $(*)$ на погоднији начин.
Идентификујмо граф $X^{p,q}$ са графом $Y^{p,q}$. Посматрајмо пут без враћања дужине l $x_0 = 1, x_1, \ldots, x_{l-1}, x_l = 1$ који почиње и завршава се у јединици у графу $Y^{p,q}$. Онда постоје $t_1, \ldots, t_l \in T_{p,q}$ такви да је $x_i = t_1t_2\cdots t_i$ за $1 \leqslant i \leqslant l$. Нека је $t_i = \Pi_q([\alpha_i])$ за неке $\alpha_i \in S_p$ где $i \in \{1, 2, \ldots, l\}$. Сада је, слично као и у теореми 3.6, $[\alpha_1][\alpha_2]\cdots[\alpha_l]$ редукована реч дужине l над S_p, јер је изгенерисана путањом без враћања. Како је $\Pi_q([\alpha_1][\alpha_2]\cdots[\alpha_l]) = x_l = 1$, видимо да $[\alpha_1][\alpha_2]\cdots[\alpha_l]$ припада језгру $\ker\Pi_q$. Дакле, сваки пут без враћања дужине l у $X^{p,q}$ одговара једној редукованој речи дужине l над S_p који се налази у $\ker\Pi_q$, а реконструкцијом претходних разматрања уназад примећујемо и да свака редукована реч дужине l над S_p која се налази у $\ker\Pi_q$ генерише једну путању без враћања дужине l у $X^{p,q}$. Закључујемо да је онда f_l баш број редукованих речи дужине l над S_p које се налазе у $\ker\Pi_q$.
Класа кватерниона $[\alpha]$, где је $\alpha = a_0 + ia_1 + ja_2 + ka_3$, налази се у $\ker\Pi_q$ ако и само ако $\tau_q(\alpha) \in Z_q \Leftrightarrow q \nmid a_0$ и $q|a_1, a_2, a_3$. Оваква структура $\ker\Pi_q$ мотивише нас да посматрамо следећу квадратну форму:

$$Q(x_0, x_1, x_2, x_3) = x_0^2 + q^2(x_1^2 + x_2^2 + x_3^2).$$

Даље, посматрајмо величину:

$$s_Q(p^m) = |\{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4 \mid Q(x_0, x_1, x_2, x_3) = p^m \text{ и } x_0{+}1 \equiv x_1 \equiv x_2 \equiv x_3 \pmod 2\}|.$$

Услов о конгруенцијама мотивисан је структуром скупа Λ' у коме је сваки кватернион конгруентан или са 1 или са $i + j + k$ модуло 2. Лако видимо да свакој четворки бројева (x_0, x_1, x_2, x_3), која доприноси величини $s_Q(p^m)$, одговара кватернион $\alpha =$

$x_0 + qx_1 i + qx_2 j + qx_3 k$ који се налази у Λ' и чија класа еквиваленције припада $\ker \Pi_q$. Тј.

$$s_Q(p^m) = |\{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda' \mid N(\alpha) = p^m \text{ и } q | a_1, a_2, a_3\}|.$$

Нека сада кватернион α доприноси десној страни претходне формуле. На основу теореме 3.2, α се јединствено факторише као $\pm p^l w_{m-2l}$ где је w_{m-2l} редукована реч над S_p дужине $m-2l$. То повлачи да је $[\alpha]$ редукована реч дужине $m-2l$ у Λ, а због конструкције она припада и $\ker \Pi_q$. Обратно, свака редукована реч w_{m-2l} дужине $m-2l$ у $\ker \Pi_q$ генерише два кватерниона $\alpha = \pm p^l w_{m-2l}$ који доприносе горенаведеном изразу за $s_Q(p^m)$.
На основу претходних запажања закључујемо да је $s_Q(p^m) = 2\sum_{0 \leqslant j \leqslant \frac{m}{2}} f_{m-2l}$. Ово доводи до нове формуле :

$$s_Q(p^m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} \frac{\sin(m+1)\theta_j}{\sin \theta_j}. \qquad (\spadesuit)$$

Од овог тренутка, наш задатак ће бити да леву страну оценимо одозго неком константом по p, а да десном страном одозго оценимо имагинарне делове оних θ_k чији је имагинарни део већи од 0.

Нека је $\mu_j = 2\cos\theta_j$ нетривијална сопствена вредност која се не налази у Раманујановом интервалу $[-2\sqrt{p}, 2\sqrt{p}]$. Онда пишемо:

$$\begin{cases} \theta_j = i\psi_j & \text{ако } 2\sqrt{p} \leqslant \mu_j \leqslant p+1, \\ \theta_j = \pi + i\psi_j & \text{ако } -p-1 \leqslant \mu_j \leqslant -2\sqrt{p}, \end{cases}$$

при чему је у оба случаја $\psi_j \in [0, \ln\sqrt{p}]$.

Лема 4.1. Нека је μ_k фиксирана нетривијална сопствена вредност која не припада Раманујановом интервалу и нека је $M(\mu_k)$ њена вишеструкост. Онда за парне m важи:

$$s_Q(p^m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} \frac{\sin(m+1)\theta_j}{\sin\theta_j} \geqslant \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh\psi_k} - 2p^{\frac{m}{2}}(m+1).$$

Доказ. Како је m парно, за сваку нетривијалну сопствену вредност која није у Раманујановом интервалу важи:

$$\frac{\sin(m+1)\theta_j}{\sin\theta_j} = \frac{\sin i(m+1)\psi_j}{\sin i\psi_j} = \frac{\frac{e^{i(i(m+1)\psi_j)} - e^{-i(i(m+1)\psi_j)}}{2i}}{\frac{e^{i(i\psi_j)} - e^{-i(i\psi_j)}}{2i}}$$

$$= \frac{\frac{e^{(m+1)\psi_j} - e^{-(m+1)\psi_j}}{2}}{\frac{e^{\psi_j} - e^{-\psi_j}}{2}} = \frac{\sinh(m+1)\psi_j}{\sinh\psi_j} \geqslant 0,$$

при чему последња неједнакост важи јер $\sinh(m+1)\psi_j > 0 \Leftrightarrow \sinh\psi_j > 0$. Онда је:

$$s_Q(p^m) = \frac{2}{n}p^{\frac{m}{2}}M(\mu_k)\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} + \frac{2}{n}p^{\frac{m}{2}}\sum_{j:\mu_j\neq\mu_k}\frac{\sin(m+1)\theta_j}{\sin\theta_j}$$

$$\geqslant \frac{2}{n}p^{\frac{m}{2}}M(\mu_k)\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} + \frac{2}{n}p^{\frac{m}{2}}\sum_{j:|\mu_j|\leqslant 2\sqrt{p}}\frac{\sin(m+1)\theta_j}{\sin\theta_j}$$

$$\geqslant \frac{2}{n}p^{\frac{m}{2}}M(\mu_k)\frac{\sinh(m+1)\psi_k}{\sinh\psi_k} - 2p^{\frac{m}{2}}(m+1),$$

при чему последња неједнакост важи јер је $\left|\frac{\sin(m+1)\theta}{\sin\theta}\right| \leqslant m+1$ за реалне θ, а број сопствених вредности у Раманујановом интервалу није већи од $p+1$, па самим тим ни од n.

Коментар: Неједнакост $\left|\frac{\sin(m+1)x}{\sin x}\right| \leqslant m+1$ се лако показује индукцијом по m, наиме база за $m=0$ је тривијална, а индуктивни корак се доказује уз помоћ адиционе формуле и неједнакости троугла

$$\left|\frac{\sin(m+1)x}{\sin x}\right| = \left|\frac{\sin(mx)\cos x + \sin x\cos(mx)}{\sin x}\right| = \left|\cos(mx) + \frac{\sin(mx)}{\sin x}\cos x\right|$$

$$\leqslant |\cos(mx)| + \left|\frac{\sin(mx)}{\sin x}\right||\cos x| \leqslant 1 + m\cdot 1.$$

Последња неједнакост важи по индуктивној хипотези. □

Претходном лемом смо пронашли доњу оцену, те нам је сада преостало да пронађемо горњу оцену за величину $s_Q(p^m)$. Да би претходна лема била задовољена од сад па надаље m је парно.

Погледајмо поново дефиницију $s_Q(p^m)$:

$$s_Q(p^m) = |\{(x_0,x_1,x_2,x_3)\in\mathbb{Z}^4 \mid Q(x_0,x_1,x_2,x_3) = p^m \text{ и } x_0{+}1 \equiv x_1 \equiv x_2 \equiv x_3 \pmod 2\}|.$$

Како је m парно, имамо да је $p^m \equiv 1 \pmod 4$, те да би важило $Q(x_0,x_1,x_2,x_3) = x_0^2{+}q^2(x_1^2{+}x_2^2{+}x_3^2) = p^m \equiv 1 \pmod 4$, мора да важи $0 \equiv x_0{+}1 \equiv x_1 \equiv x_2 \equiv x_3 \pmod 2$. Сада лако видимо да је $s_Q(p^m)$ заправо број четворки целих бројева (x_0,x_1,x_2,x_3) за које важи $x_0^2 + 4q^2(x_1^2+x_2^2+x_3^2) = p^m$. Оценимо сада ову величину.

Најпре оценимо број могућих начина да изаберемо x_0. Очигледно важи $|x_0| \leqslant p^{\frac{m}{2}}$. Додатно:

$$x_0^2 \equiv p^m \pmod{q^2} \;\Rightarrow\; x_0^2 - p^m = (x_0 + p^{\frac{m}{2}})(x_0 - p^{\frac{m}{2}}) \equiv 0 \pmod{q^2},$$

$$\text{што уз НЗД}(x_0 + p^{\frac{m}{2}}, x_0 - p^{\frac{m}{2}}) \mid 2p^{\frac{m}{2}} \text{ даје } x_0 \equiv \pm p^{\frac{m}{2}} \pmod{q^2}.$$

Додатно, како су p и x_0 оба парни знамо да важи $x_0 \equiv \pm p^{\frac{m}{2}} \pmod{2q^2}$. Ово уз $|x_0| \leqslant p^{\frac{m}{2}}$ значи да имамо највише $2\cdot\left(\frac{p^{\frac{m}{2}}}{q^2}+1\right)$ потенцијалних могућности за x_0.

Када је x_0 фиксирано, наш проблем се своди на проналажење броја тројки целих бројева x_1, x_2, x_3 за које је

$$x_1^2 + x_2^2 + x_3^2 = \frac{p^{\frac{m}{2}} - x_0^2}{4q^2}.$$

Да бисмо разумели како расте број представљања природног броја n као збир три квадрата, потребно је да прво испитамо број представљања броја n као збир два квадрата. Ова тематика је веома изучена и постоје бројни резултати у овој области, од којих је најпознатија Ојлерова теорема:

Теорема 4.1. Природан број n може се записати као збир два квадрата ако и само ако је у факторизацији тог броја степен сваког простог делиоца који је конгруентан са 3 модуло 4 паран.

Имајући на уму да је $a^2+b^2 = (a+ib)(a-ib)$ проблем растављања броја на збир два квадрата би требало да нас подсети на поглавље о кватернионима. Иза збира четири квадрата крила се структура кватернионске алгебре; слично томе, срж растављања броја на збир два квадрата је структура коју називамо *прстен Гаусових целих*, у ознаци $\mathbb{Z}[i]$. Наиме, он је дефинисан као $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$ и лако се доказује да је то потпрстен прстена комплексних бројева. Као и код кватерниона, и овде можемо дефинисати:

(1) јединице прстена - то су инвертибилни елементи у односу на множење, тј. ± 1 и $\pm i$,

(2) асоциране елементе - елементи α и α' су асоцирани ако постоји јединични елемент ε такав да је $\alpha = \alpha'\varepsilon$,

(3) мултипликативну норму - ако је $\alpha = a + ib$, онда је норма дефинисана као $N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2 = a^2 + b^2$,

(4) просте елементе - кажемо да је $\pi \in \mathbb{Z}[i]$ прост ако за све $\alpha, \beta \in \mathbb{Z}[i]$ за које је $\pi = \alpha\beta$ важи да је бар један од α, β јединица у $\mathbb{Z}[i]$.

За разлику од кватернионске алгебре, овај прстен је комутативан, у њему важи Безуов став, и постоји јединствена факторизација на просте. Наиме, уколико је $\alpha \in \mathbb{Z}[i]$ и $\alpha = \pi_1\pi_2 \cdots \pi_k = \sigma_1\sigma_2 \cdots \sigma_l$ су две факторизације броја на просте елементе, онда је $k = l$ и постоји пермутација f бројева $1, 2, \ldots, k$, таква да су $\pi_{f(i)}$ и σ_i асоцирани за свако $i \in 1, 2, \ldots, k$. Међутим, карактеризација простих елемената у $\mathbb{Z}[i]$ није једноставна као у $\mathbb{H}(\mathbb{Z})$. Наиме, може се показати следеће:
Број $\alpha \in \mathbb{Z}[i]$ је прост ако и само ако је испуњен један од следећих случајева:

(1) $N(\pi) = 2$ тј. π $1 + i$;

(2) $N(\pi) = p$, где је p прост у $\mathbb{Z}$ и $p \equiv 1 \pmod 4$;

(3) π је асоцирани елемент од q, где је q прост у $\mathbb{Z}$ и $q \equiv 3 \pmod 4$.

Имајући ово на уму, спремни смо да докажемо Лежандрову формулу за број представљања неког броја у облику збира два квадрата. Уведимо најпре неке ознаке:

(1) $r_k(n) = \left|\left\{(x_0, \ldots, x_{k-1}) \in \mathbb{Z}^k \ : \ \sum_{i=0}^{k-1} x_i^2 = n\right\}\right|$;

(2) $d_1(n)$ је број делилаца броја $n \in \mathbb{N}$ који су конгруентни са 1 модуло 4;

(3) $d_3(n)$ је број делилаца броја $n \in \mathbb{N}$ који су конгруентни са 1 модуло 4;

(4) $d(n)$ је број делилаца броја $n \in \mathbb{N}$.

Теорема 4.2. */Лежандрова теорема/* За свако $n \in \mathbb{N}$ важи $r_2(n) = 4(d_1(n) - d_3(n))$.

Доказ. Нека је $\delta(n) = d_1(n) - d_3(n)$. Нека је $N = 2^t km$ при чему је

$$k = \prod_{h=0}^{a} p_h^{r_h},\ p_h \equiv 1 \pmod 4 \text{ и } m = \prod_{j=0}^{b} q_j^{r_j},\ q_h \equiv 3 \pmod 4.$$

Уз чињеницу да је неки делилац броја N конгруентан са 1 модуло 4 ако и само ако није дељив са 2 и ако је његов „$q-$део" конгруентан 1 модуло 3, на основу претходних дефиниција можемо извести следећи идентитет:

$$\delta(N) = d_1(N) - d_3(N) = d_1(km) - (d(km) - d_1(km)) = 2d_1(km) - d(km) =$$

$$= 2d(k)d_1(m) - d(k)d(m) = d(k)(2d_1(m) - d(m)) = d(k)(d_1(m) - (d(m) - d_1(m))) = d(k)\delta(m).$$

Тврђење: $\delta(m) = \begin{cases} 0, & \text{ако је бар један } s_j \text{ непаран} \\ 1, & \text{ако су сви } s_j \text{ парни, тј. } m \text{ је квадрат} \end{cases}$

Доказ: Уколико је неки s_j непаран, БУО претпоставимо да је то баш s_1, знамо да важи следеће:

$$d_1(m) = \frac{s_1 + 1}{2} d_1\left(\frac{m}{q_1^{s_1}}\right) + \frac{s_1 + 1}{2} d_3\left(\frac{m}{q_1^{s_1}}\right),$$

јер да би делилац броја m био конгруентан са 1 модуло 4, он мора у свом саставу имати паран број q-ова (рачунајући и мултиплицитете), те за изабрани делилац од $\frac{m}{q_1^{s_1}}$, имамо увек тачно $\frac{s_1 + 1}{2}$ начина да га допунимо степеном q_1 тако да он буде конгруентан 1 модуло 4. Аналогно се доказује да и за делиоце конгруентне са 3 модуло четири важи:

$$d_3(m) = \frac{s_1 + 1}{2} d_1\left(\frac{m}{q_1^{s_1}}\right) + \frac{s_1 + 1}{2} d_3\left(\frac{m}{q_1^{s_1}}\right),$$

тј. $d_3(m) = d_1(m) \Rightarrow \delta(m) = 0$.

Нека су сада сви s_j парни. Докажимо да је $\delta(m) = \delta\left(\frac{m}{q_j^{s_j}}\right)$, што ће уз чињеницу да

је $\delta(1)=1$ дати да је $\delta(m)=1$ за све m који су квадрати. Разматрања слична као у претходном случају дају следеће идентитете:

$$d_1(m)=\left(\frac{s_j}{2}+1\right)d_1\left(\frac{m}{q_j^{s_j}}\right)+\left(\frac{s_j}{2}\right)d_3\left(\frac{m}{q_j^{s_j}}\right),$$

$$d_3(m)=\left(\frac{s_j}{2}\right)d_1\left(\frac{m}{q_j^{s_j}}\right)+\left(\frac{s_j}{2}+1\right)d_3\left(\frac{m}{q_j^{s_j}}\right).$$

Након одузимања добијамо: $\delta(m)=d_1(m)-d_3(m)=d_1\left(\frac{s_j}{2}\right)-d_3\left(\frac{s_j}{2}\right)=\delta\left(\frac{s_j}{2}\right)$, чиме завршавамо доказ тврђења.

Из тврђења директно следи да је $\delta(N)=\begin{cases}d(k), & \text{ако је } m \text{ потпун квадрат;}\\ 0, & \text{иначе.}\end{cases}$

Сада када смо одредили величину $\delta(N)$, можемо прећи на анализу броја $r_2(N)$. Користимо исте ознаке као и у претходном делу доказа. Ако m није потпун квадрат, по Ојлеровој теореми знамо да се N не може записати као збир два квадрата тј. $r_2(N)=0$, што уз $\delta(N)=0$ завршава доказ теореме у овом случају. Нека је сада m потпун квадрат. Посматрајмо разлагање броја $N=A^2+B^2$. Идеја је да ово разлагање посматрамо као разбијање броја N на два фактора у $\mathbb{Z}[i]$ ($N=(A+iB)(A-iB)$) и да истовремено посматрамо разлагање броја N на просте факторе у $\mathbb{Z}[i]$. Како је норма у $\mathbb{Z}[i]$ мултипликативна величина, на основу карактеризације простих фактора у $\mathbb{Z}[i]$ закључујемо да факторизација броја N на просте у $\mathbb{Z}[i]$ изгледа овако:

$$N=(-1)^t(1+i)^{2t}\prod_{h=1}^{a}\pi_h^{r_h}\overline{\pi_h}^{r_h}\prod_{j=1}^{b}q_j^{s_j},$$

при чему су π_h прости елементи $\mathbb{Z}[i]$ за које је $N(\pi_h)=p_h$. Сада уз $N=(A+iB)(A-iB)$ и $N(A+iB)=N(A-iB)$ закључујемо да мора важити следеће:

$$A+iB=u(1+i)^t\prod_{h=1}^{a}\pi_h^{w_h}\overline{\pi_h}^{u_h}\prod_{j=1}^{b}q_j^{\frac{s_j}{2}}$$

$$A-iB=u'(1+i)^t\prod_{h=1}^{a}\pi_h^{u_h}\overline{\pi_h}^{w_h}\prod_{j=1}^{b}q_j^{\frac{s_j}{2}},$$

при чему су u и u' инвертибилни елементи такви да је $uu'=1$, а $w_h+u_h=r_h\quad(1\leqslant h\leqslant a)$. Наравно, сваки избор за u-ове и w_h-ове даје валидно решење (A,B), јер је очигледно да је конјугат десне стране прве једнакости једнак десној страни друге једнакости. Дакле важи: $r_2(N)=4\prod_{h=1}^{a}(r_h+1)=4d(k)=4\delta(N)$. Овиме завршавамо доказ теореме. □

Претходна теорема нам тривијално даје оцену за раст величине $r_2(n)$. Ради лакшег рачуна са овом оценом, уведимо следећу дефиницију:
За фиксирано $\varepsilon>0$ кажемо да је реална величина $f(n)$, која зависи од $n\in\mathbb{N}$, једнака $O_\varepsilon(n^\varepsilon)$ ако постоји константа $C=C(\varepsilon)>0$, таква да је $|f(n)|\leqslant Cn^\varepsilon$ за све $n\in\mathbb{N}$.

Последица 6. За све $\varepsilon > 0$ важи $r_2(n) = O_\varepsilon(n^\varepsilon)$.

Доказ. По претходној теореми знамо да је $r_2(n) = 4(d_1(n) - d_3(n)) \leqslant 4d_1(n) \leqslant 4d(n)$. Дакле довољно је да докажемо да за свако $\varepsilon > 0$ важи $d(n) = O_\varepsilon(n^\varepsilon)$. Фиксирајмо сада $\varepsilon > 0$. Онда је:

$$\frac{d(n)}{n^\varepsilon} = \prod_{p^\alpha \| n} \frac{\alpha+1}{p^{\alpha\varepsilon}} = \prod_{\substack{p^\alpha \| n \\ p < 2^{1/\varepsilon}}} \frac{\alpha+1}{p^{\alpha\varepsilon}} \cdot \prod_{\substack{p^\alpha \| n \\ p \geqslant 2^{1/\varepsilon}}} \frac{\alpha+1}{p^{\alpha\varepsilon}},$$

при чему смо факторе груписали у односу на величину простог делиоца p природног броја n. Наш задатак је да покажемо да постоји реална константа $C(\varepsilon)$ која је увек већа од горенаведеног израза.

За почетак посматрајмо случај када је $p \geqslant 2^{1/\varepsilon}$. Онда је $p^\varepsilon \geqslant 2$, па је $\dfrac{\alpha+1}{p^{\alpha\varepsilon}} \leqslant \dfrac{\alpha+1}{2^\alpha} \leqslant 1$. Дакле, други производ је ограничен јединицом одогзо, те је преостало да ограничимо први производ одозго неком константом која не зависи од n.

За сваки прост број p важи $p^{\alpha\varepsilon} \geqslant 2^{\alpha\varepsilon} = e^{\alpha\varepsilon \ln 2} > \alpha\varepsilon \ln 2$, па је:

$$\frac{\alpha+1}{p^{\alpha\varepsilon}} = \frac{1}{p^{\alpha\varepsilon}} + \frac{\alpha}{p^{\alpha\varepsilon}} < 1 + \frac{\alpha}{p^{\alpha\varepsilon}} < 1 + \frac{1}{\varepsilon \ln 2}.$$

Сада, како простих бројева за које важи $p < 2^{1/\varepsilon}$ има коначно много, за константу $C(\varepsilon)$ можемо узети следеће: $C(\varepsilon) = \prod_{p<2^{1/\varepsilon}} \left(1 + \dfrac{1}{\varepsilon \ln 2}\right)$. Овиме завршавамо наш доказ. □

Сада имамо све што нам је потребно да оценимо раст величине $r_3(n)$.

Последица 7. За свако $\varepsilon > 0$ важи $r_3(n) = O_\varepsilon(n^{\frac{1}{2}+\varepsilon})$.

Доказ. Користећи последицу 6 добијамо следеће:

$$r_3(n) = \sum_{k=0}^{[\sqrt{n}]} r_2(n-k^2) \leqslant C(\varepsilon) \sum_{k=0}^{[\sqrt{n}]} (n-k^2)^\varepsilon \leqslant C(\varepsilon)\sqrt{n} \cdot n^\varepsilon = C(\varepsilon) n^{\frac{1}{2}+\varepsilon}.$$

□

Вратимо се сада на главни проблем. До сада смо уочили да за четворку целих бројева (x_0, x_1, x_2, x_3) која доприноси величини $s_Q(p^m)$ (m парно) постоји највише $2 \cdot \left(\frac{p^{\frac{m}{2}}}{q^2} + 1\right)$ могућности за избор броја x_0, а за свако такво фиксирано x_0 остало нам је да пребројимо број тројки природних бројева чији је збир квадрата једнак $\dfrac{p^{\frac{m}{2}} - x_0^2}{q^2}$. На основу претходне последице знамо:

$$s_Q(p^m) = O_\varepsilon\left[\left(\frac{p^{\frac{m}{2}}}{q^2}\right)^{\frac{1}{2}+\varepsilon}\left(\frac{p^{\frac{m}{2}}}{q^2}+1\right)\right] = O_\varepsilon\left[\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q}\right].$$

Овај резултат уз лему 4.1 даје следећу неједнакост:

$$\frac{M(\mu_k)}{n} p^{\frac{m}{2}} \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} \leqslant C_\varepsilon \left[\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q} \right] + p^{\frac{m}{2}}(m+1),$$

за неко $C_\varepsilon > 0$. Скраћивањем са $p^{\frac{m}{2}}$ и коришћењем чињенице да је $n < q^3$ (лема 3.4) добијамо:

$$M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} \leqslant C_\varepsilon [p^{m(\frac{1}{2}+\varepsilon)} + q^2 p^{m\varepsilon}] + q^3(m+1).$$

Сетимо се да m није фиксирано и изаберимо такво m за које је $p^{\frac{m}{2}} \leqslant q^3$. Онда је

$$M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} \leqslant C_\varepsilon [q^{3+6\varepsilon} + q^{2+6\varepsilon}] + q^3(1 + 6\log_p q).$$

Уз $\sinh \psi_k \leqslant \sinh \ln \sqrt{p}$ (sinh растућа) и $\log_p q = O_\varepsilon(q^\varepsilon)$ добијамо:

$$M(\mu_k) \sinh(m+1)\psi_k = O_\varepsilon[q^{3+6\varepsilon}].$$

Сада, да бисмо оценили $\sinh(m+1)\psi_k$, изаберимо највеће могуће парно m такво да је $p^{\frac{m}{2}} \leqslant q^3$. Онда је за довољно велико q

$$\sinh(m+1)\psi_k \geqslant \frac{e^{(m+1)\psi_k}}{3} \geqslant \frac{e^{(-1+6\log_p q)\psi_k}}{3} \geqslant \frac{p^{-\frac{1}{2}}}{3} e^{6\log_p q \cdot \psi_k}.$$

Прва неједнакост важи за такве q за које је $e^{(m+1)\psi_k} \geqslant \sqrt{3}$, друга важи јер је m највећи паран број за који је $m \leqslant 6\log_p q$, а последња јер је $\psi_k \in [0, \ln \sqrt{p}]$. Онда је

$$M(\mu_k) = O_\varepsilon(q^{3+6\varepsilon - \frac{6\psi_k}{\ln p}}).$$

У овом тренутку смо дошли до поприлично лепе оцене за вишеструкост сопствене вредности $M(\mu_k)$ преко ψ_k. Дакле, једино што нам преостаје да завршимо доказ је да разумемо како се понаша величина $M(\mu_k)$. Овде наступа теорија репрезентација.

Лема 4.2. Нека је μ нетривијална сопствена вредност матрице повезаности графа $X^{p,q}$, тј. $|\mu| \neq p+1$. Онда је $M(\mu) > \dfrac{q-1}{2}$.

Доказ. Нека је V_μ сопствени простор који одговара сопственој вредности μ.
Тврђење: Постоји репрезентација групе G којом је изгенерисан граф $X^{p,q}$ (дакле, G је $PSL_2(q)$ или $PGL_2(q)$) на простору V_μ.
Доказ: Доказаћемо заправо да је V_μ инваријантан потпростор леве регуларне репрезентације групе G. Ово нам је довољно јер рестрикција репрезентације на инваријантном потпростору такође јесте репрезентација. Нека је $v \in V_\mu$ произвољан сопствени вектор. Наш задатак је да докажемо да је онда и $\lambda_G(g)v$ такође у V_μ. Но, ово се тривијално добија по дефиницији

$$(A\lambda_G(g)v)(x) = Av(g^{-1}x) = \mu v(g^{-1}x) = \mu(\lambda_G(g)v)(x) \qquad \forall g, x \in G,$$

при чему друга једнакост важи зато што $v \in V_\mu$.
Сада смо нашли репрезентацију групе G на V_μ, али како је у сваком случају $PSL_2(q) < G$ то значи да постоји репрезентација $PSL_2(q)$ на V_μ. Степен ове репрезентације је баш $M(\mu)$. Сетимо се сада теореме 3.5. Она тврди да је свака нетривијална репрезентација групе $PSL_2(q)$ бар $\dfrac{q-1}{2}$, те је да бисмо доказали тражено својство мултиплицитета $M(\mu)$, треба једино да докажемо да за $|\mu| \neq p+1$ наша репрезентација није тривијална. Претпоставимо супротно.

Ако је $\left(\frac{p}{q}\right) = 1$, граф $X^{p,q}$ је настао од $PSL_2(q)$. У том случају знамо да је $\lambda_G(g)v(x) = v(x)$ за све $g, x \in G$, $v \in V_\mu$, јер је наша репрезентација тривијална, али онда је по дефиницији $v(g^{-1}x) = v(x)$ за све $g \in PSL_2(q)$, те је сваки $v \in V_\mu$ константна функција, али онда је $\mu = p+1$, контрадикција!

Ако је $\left(\frac{p}{q}\right) = -1$, граф $X^{p,q}$ је настао од $PGL_2(q)$. Као и раније знамо да важи $v(g^{-1}x) = v(x)$ за све $g \in PGL_2(q)$, $x \in PSL_2(q)$ и $v \in V_\mu$. Дакле сваки вектор $v \in V_\mu$ је константан на сваком од косета групе $PSL_2(q)$ у $PGL_2(q)$, тј.

$$v = \begin{cases} a_+ & \text{на } PSL_2(q); \\ a_- & \text{на } PGL_2(q) - PSL_2(q). \end{cases}$$

Додатно $v \neq 0$ је сопствени вектор сопствене вредности μ те важи:

$$\mu a_- = (p+1)a_+ \qquad \text{и} \qquad \mu a_+ = (p+1)a_-.$$

Притом, ово важи јер је у овом случају $S_{p,q} \in PGL_2(q) - PSL_2(q)$, те су два чвора повезана једино ако је један у $PSL_2(q)$, а други у $PGL_2(q) - PSL_2(q)$. Множењем ове две једначине и скраћивањем са a_+a_- (може јер је $v \neq 0$) добијамо $\mu^2 = (p+1)^2$, па поново долазимо до контрадикије.
Овиме је наш доказ завршен. □

Сада имамо да је $M(\mu_k) = O_\varepsilon(q^{3+6\varepsilon-\frac{6\psi_k}{\ln p}}) \geqslant \frac{q-1}{2}$, што за довољно велико q даје:

$$3 + 6\varepsilon - \frac{6\psi_k}{\ln p} \geqslant 1 \Rightarrow \psi_k \leqslant \left(\frac{1}{3} + \varepsilon\right) \ln p.$$

Сетимо се да важи или $\theta_k = i\psi_k$ или $\pi + i\psi_k$, као и $\mu_k = 2\sqrt{p}\cos\theta_k$, те је онда

$$|\mu_k| = 2\sqrt{p}|\cos(i\psi_k)| = 2\sqrt{p}\cosh\psi_k \leqslant p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon}.$$

Овиме смо доказали да за довољно велико q наши графови $X^{p,q}$ заиста формирају фамилију експандера.

О Раманујану

Сриниваса Рамануџан је био један од најзначајнијих математичара са почетка двадесетог века. Иако је живео само 32 године, његов допринос многим областима математике је огроман. Међу његовим најпознатијим радовима налазе се бројни идентитети из теорије бројева, анализе, као и Харди-Рамануџанов метод круга, којим је нпр. први пут доказана асимптотска оцена за број партиција неког броја.

Срж његовог рада било је посматрање функција на хиперболичкој полуравни, које су у неком смислу „периодичне"– такозваних модуларних форми. Међу њима су Рамануџанове тета функције, као и генераторна функција функције броја партиција природног броја, а једна од његових најзначајнијих хипотеза произишла је из посматрања *Рамануџанове тау функције* $\tau(n)$, која је дефинисана као n-ти коефицијент у реду

$$\Delta(q) = q\prod_{n-1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

Прва хипотеза била је да је тау функција мултипликативна тј.

$$\tau(mn) = \tau(m)\tau(n) \qquad (m,n) = 1.$$

Друга хипотеза гласила је:

$$|\tau(n)| \leqslant d(n)n^{\frac{11}{2}}.$$

Прву хипотезу доказао је Мордел релативно брзо, већ 1917. године. Међутим друга хипотеза испоставила се тежа, и заиста, водила је ка једном дубоком резултату и развијању нове теорије - теорије модуларних форми. Другу хипотезу у уопштеном облику доказао је Делињ 1974. године и сматра се да је она један од најзначајнијих резултата у математици.

Литература

[DSV] Davidoff, Sarnak, Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, Cambridge University Press, New York, 2003.

[LPS] A.Lubotzky, R.Philips, P.Sarnak,*Ramanujan graphs*, Combinatorica 8 (1988), 261-277.

[S] Sarnak, *Some applications of modular forms*, Cambridge University Press, Cambridge, 1990.

[E] Etingof, Golberg, Hensel, Liu, Schwendner, Vaintrob, Yudovina, Gerovitch, *Introduction to Representation Theory*, American Mathematical Society, Providence, Rhode Island, 2011.

[M1] G.A.Margulis, *Arithmetic groups and graphs without short cycles, sixth Inter. Symp. on Infor. Theory*, Tashkent 1984, Abstracts, Vol. I 123-125.

[M2] G.A.Margulis, *Explicit constructions of combinatorial schemes and their applications for construction of expanders and concentrators*, Journal of Problems of Information Transmission, 1988.

[R] S.Ramanujan, *On certain trigonometrical sums and their application to the theory of numbers*, Trans. Cambridge Phil. Soc. XXII No. 13, (1918), 256-276.

[E] P.Erdos, *Graph theory and probability*, Can. J. Math. 11, (1959), 34-38.

[P] M.S.Pinsker, *On the complexity of a concentrator*, 7th International Teletraffic Conference, Stockholm, June 1973, 318/1-318/4.

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