修士論文

ラマヌジャングラフの構成についての考察

三重大学大学院 教育学研究科 教科教育専攻 数学教育専修 206M016

藤田　友美

2008年2月12日

別紙様式第３

論　文　目　録

三重大学大学院教育学研究科

教科教育　専攻	数学教育　専修	氏名	藤田友美

論　文 （実技等の課題を含む）	題目 ラマヌジャングラフの構成についての考察
添付資料	

別紙様式第４

論　文　要　旨

三重大学大学院教育学研究科

教科教育 専攻	数学教育 専修	氏名	藤田 友美

この論文はラマヌジャングラフの構成について考察した結果である．1章ではDavidoff, Sarnak, Valetteによる具体的なラマヌジャングラフの構成についてまとめた．有限で連結なk-regularグラフXの，全ての非自明な固有値μが$|\mu| \leq 2\sqrt{k-1}$を満たすとき，Xをラマヌジャングラフという．Gを群とする．Sを空でないGの部分集合とし，$S = S^{-1}$が成り立つとする．頂点の集合$V = G$，辺の集合$E = \{(x, y) : x, y \in G \text{ で } y = xs \text{ となる } s \in S \text{ が存在する}\}$でできるグラフ$\mathcal{G}(G, S)$をケーリーグラフという．以下のグラフを考える．ただし，ここで$S^{p,q}$は1.3節で定義する集合である．

$\left(\frac{p}{q}\right) = 1$のときの，$S_{p,q}$に関する$\mathrm{PSL}_2(q)$のケーリーグラフ

$$X^{p,q} = \mathcal{G}(\mathrm{PSL}_2(q), S_{p,q})$$

と，$\left(\frac{p}{q}\right) = -1$のときの，$S_{p,q}$に関する$\mathrm{PGL}_2(q)$のケーリーグラフ

$$X^{p,q} = \mathcal{G}(\mathrm{PGL}_2(q), S_{p,q})$$

は，$(p+1)$-regularのグラフであり，$p^8 < q$のときについては，どの2頂点も何本かの辺によってつながっている連結グラフであることが示されている．また，ラマヌジャングラフであり，$\left(\frac{p}{q}\right) = 1$のとき，大きなgirthと大きな彩色数を持つ良いグラフであることが示されている．

2章ではこれの頂点の群を位数4の部分群で左から割ったものについて考察している．つまりここからは，頂点の集合Vを群に限らず集合とし，頂点の集合Vには右から群Gが作用しているとする．

$\left(\frac{p}{q}\right) = 1$のとき，$Z^{p,q}$を$S_{p,q}$に関する$H\backslash\mathrm{PSL}_2(q)$のケーリーグラフとする．

$$Z^{p,q} = \mathcal{G}(H\backslash\mathrm{PSL}_2(q), S_{p,q}).$$

$\left(\frac{p}{q}\right) = -1$のとき，$Z^{p,q}$を$S_{p,q}$に関する$H\backslash\mathrm{PGL}_2(q)$のケーリーグラフとする．

$$Z^{p,q} = \mathcal{G}(H\backslash\mathrm{PGL}_2(q), S_{p,q}).$$

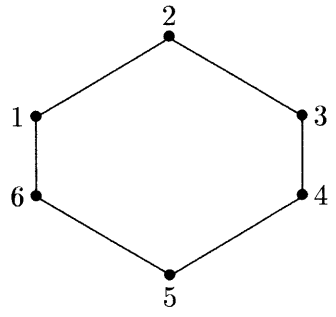
このグラフは頂点推移的ではないが，$(p+1)$-regularであることには変わりはなく，$X^{p,q}$の連結性が$p^8 < q$のときに示せたのに対して，$Z^{p,q}$では$p > 5$, $p^7 < q$のとき，ただし，$p^7 < q \leq p^8$については3, 5, 11, 17, 29, 41以外のときに，連結であることを示すことができた．また，ループがない$Z^{p,q}$に対して，$p > 5$, $p^8 < q$を満たす奇素数p, qで，ラマヌジャングラフであり，良いグラフであるということを示すことができた．

目 次

序文

この論文はラマヌジャングラフの構成について考察した結果である．1 章では Davidoff, Sarnak, Valette[1] による具体的なラマヌジャングラフの構成についてまとめた．ここでいうグラフとは，右のような頂点と，辺からなるものである．グラフ X の全ての頂点から同じ k 本ずつ辺が出ているとき，グラフ X は k-regular であるという．右の例は 2-regular のグラフである．

[例]



定義 0.0.1. 有限で連結な k-regular グラフ X の，全ての非自明な固有値 μ が $|\mu| \leq 2\sqrt{k-1}$ を満たすとき，X をラマヌジャングラフという．

G を群とする．S を空でない G の部分集合とし，$S = S^{-1}$ が成り立つとする．頂点の集合 $V = G$，辺の集合 $E = \{(x, y) : x, y \in G \text{ で } y = xs \text{ となる } s \in S \text{ が存在する }\}$ でできるグラフ $\mathcal{G}(G, S)$ をケーリーグラフという．以下のグラフを考える．ただし，ここで $S_{p,q}$ は 1.3 節で定義する集合である．
$\left(\frac{p}{q}\right) = 1$ のときの，$S_{p,q}$ に関する $\mathrm{PSL}_2(q)$ のケーリーグラフ

$$X^{p,q} = \mathcal{G}(\mathrm{PSL}_2(q), S_{p,q})$$

と，$\left(\frac{p}{q}\right) = -1$ のときの，$S_{p,q}$ に関する $\mathrm{PGL}_2(q)$ のケーリーグラフ

$$X^{p,q} = \mathcal{G}(\mathrm{PGL}_2(q), S_{p,q})$$

は，$(p+1)$-regular のグラフであり，$p \geq 5, p^8 < q$ のときについては，どの 2 頂点も何本かの辺によってつながっている連結グラフであることが示されている．また，全ての $v_i, v_j \in V$ で $\alpha(v_i) = v_j$ となるグラフ X の自己同型写像 α が存在するとき，頂点推移的であるというが，このグラフは頂点推移的なグラフである．そして，$X^{p,q}$ の，ある頂点から同じ頂点へとつながる道の数について，以下の公式が作られた．

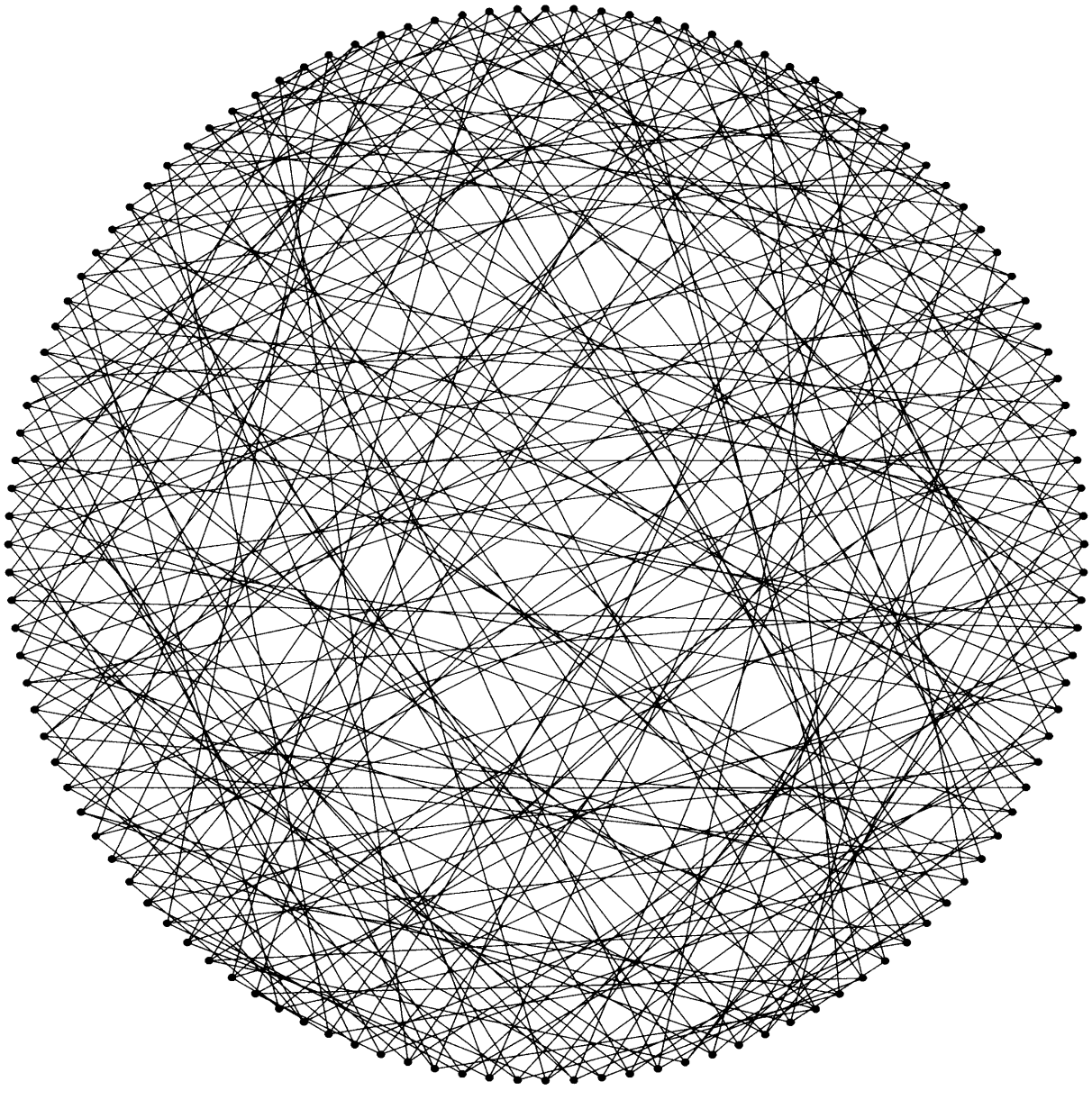
定理 0.0.2 (トレース公式)**.** k-regular で連結なループがない単純グラフを X とする．その頂点の集合を V とする．全ての $m \in \mathbb{N} \cup \{0\}$ で

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

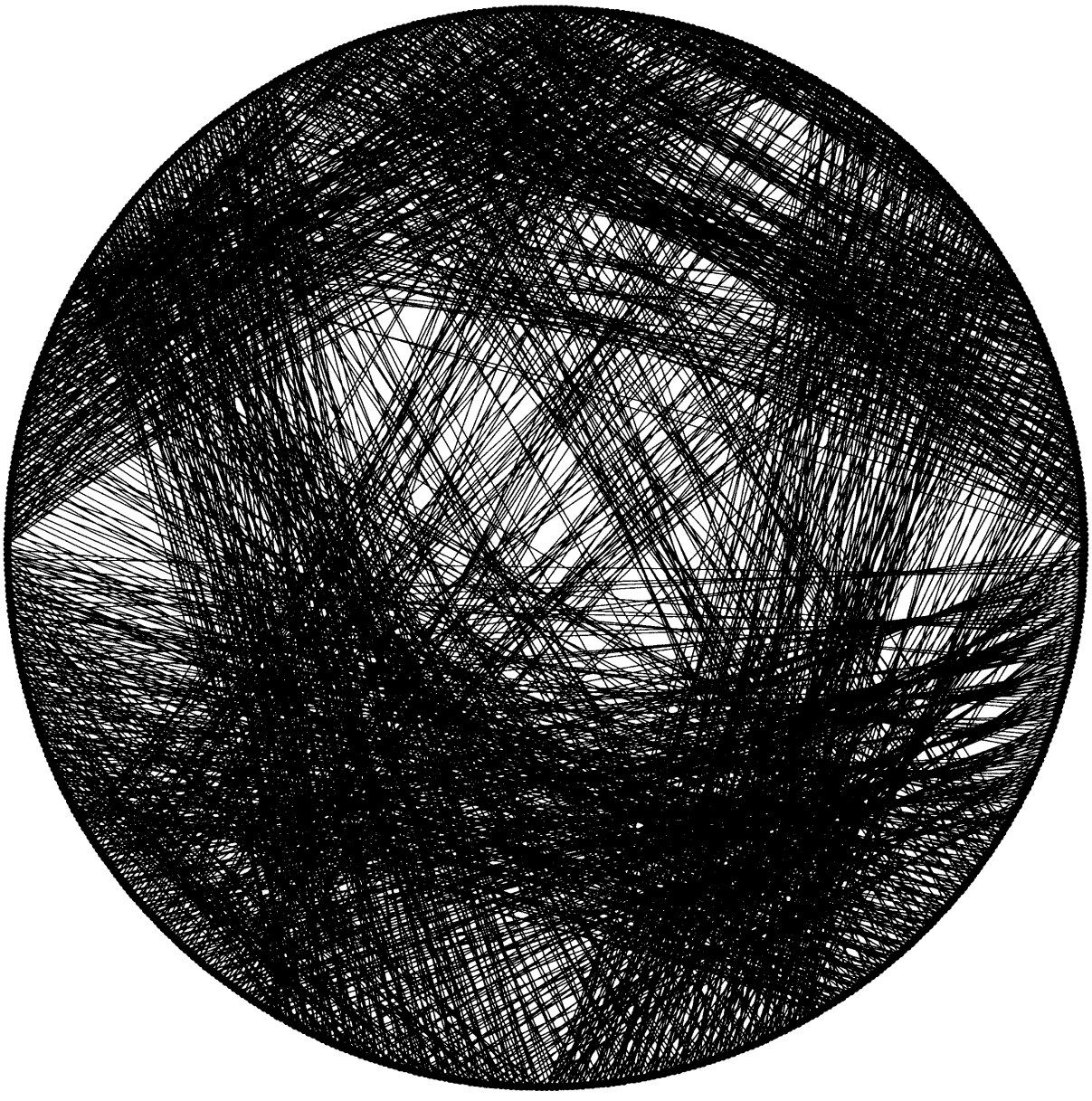
ただし，U_m は m 次のチェビシェフ多項式，すなわち，$m \in \mathbb{N} \cup \{0\}$ で $U_m(\cos\theta) = \sin(m+1)\theta / \sin\theta$ を満たす式である．この公式に対して，ラマヌジャン予想を使うことにより，$p \geq 5, p^8 < q$ を満たす奇素数 p, q で q が十分大きいとき，グラフ $X^{p,q}$ は，ラマヌジャングラフであることが示された．そしてこれが Davidoff, Sarnak, Valette[1] による具体的なラマヌジャングラフの例である．また，ここで仮定になっている $p^8 < q$ は $X^{p,q}$ の連結性と単純性を示すものであり，連結で単純なグラフであればこの範囲でなくとも成り立つ．また，ある頂点から同じ頂点に戻る，いくつかの辺でできた道をサーキットとい

うが，その中で最小のものを girth と呼ぶ．さらに，隣接した 2 点が同じ色にならないように塗り分けるときに必要な色の数の最小値を彩色数という．当然，辺が増えれば彩色数は大きくなるが，girth は大きくならない．むしろ小さくなってしまうこともある．

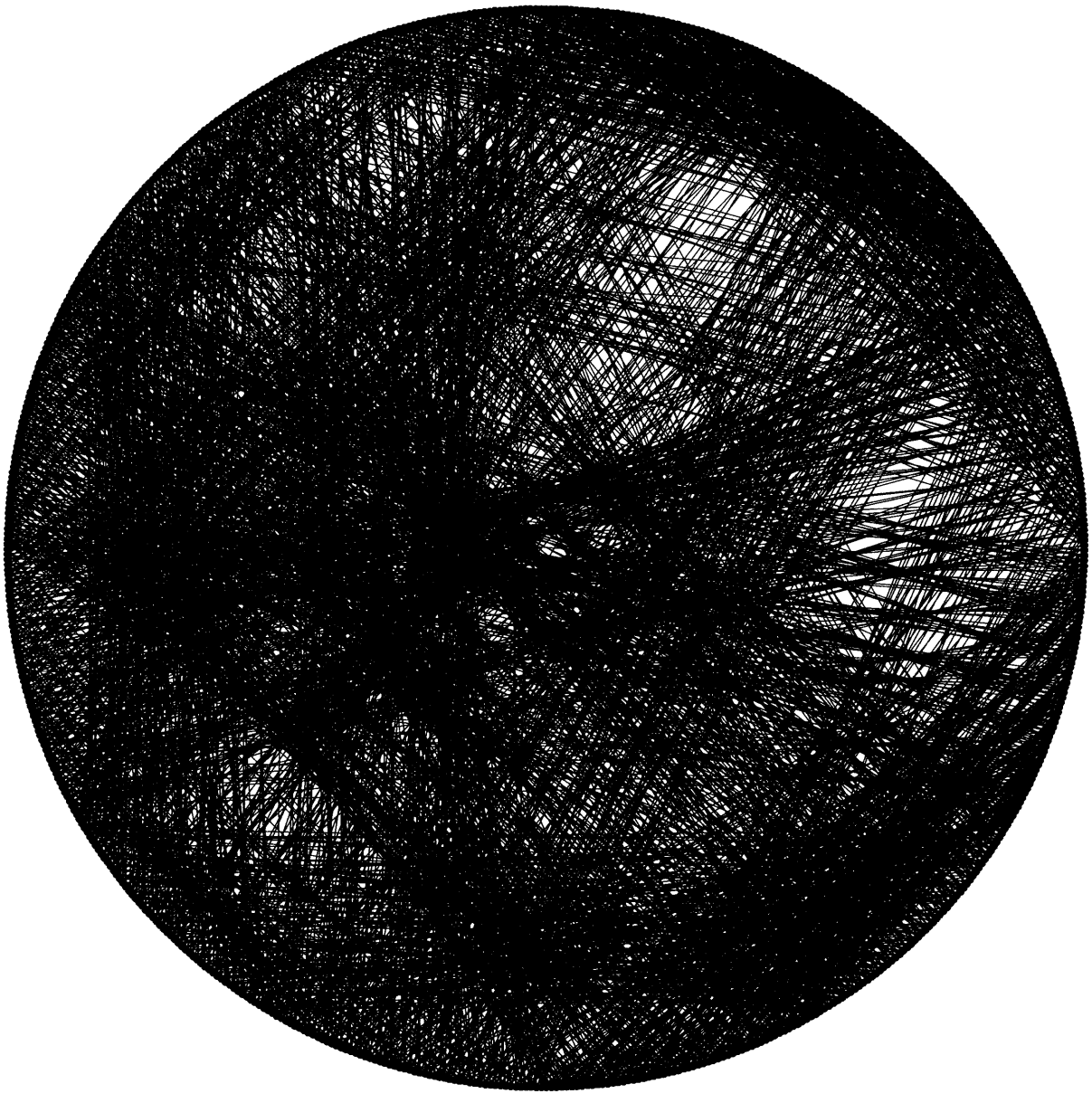
以下のグラフは $X^{3,5}, X^{3,11}, X^{5,11}$ のグラフである．どれも連結グラフであり，ラマヌジャングラフでもある．



$X^{3,5}$ のグラフ：girth は 6



$X^{3,11}$ のグラフ：girth は 9



$X^{5,11}$ のグラフ：girth は 6

近年，情報化社会の発展により，より良い通信網が望まれている．通信の途絶えにくさだけを考えれば，どの 2 地点もつながっていれば一番良いといえる．これは，グラフでいえば，任意の 2 頂点が隣接している完全グラフということである．同じ頂点数であれば，この状態が一番彩色数が大きい．しかし，現実に考えると，これでは経済面での負担が大きくなる．逆に経済面だけを求め，ひとつの経路ですべての地点をカバーしようとすると，一本の線でなければ，最初の例のような形になる．このグラフはサイクルグラフで，同じ頂点数であれば，この状態が一番 girth が大きい．しかしこれでは経路が少なすぎ，どこかでトラブルが起これば，その先の通信が途絶えてしまう可能性が高い．良い通信網は，この 2 つの相反する面を最大限に持ち合わせる通信網であるということである．これは，

つまり，大きなgirthと大きな彩色数をあわせ持つグラフを作ることと同意である．1959年にErdösにより，このようなグラフが存在することは示されている．このようなグラフを良いグラフと呼ぶ．グラフ $X^{p,q}$ は，p,q が $p^8 < q$, $p \geq 5$ を満たす奇素数で，$\left(\frac{p}{q}\right) = 1$ のとき，大きなgirthを持ち，大きな彩色数を持つ．つまり，この条件のグラフ $X^{p,q}$ は良いグラフである．2章からは別の良いグラフであり，ラマヌジャングラフであるグラフを構成することについて考察を行った．

2章で新たに作ったグラフ $Z^{p,q}$ の頂点は $X^{p,q}$ の頂点 $\mathrm{PSL}_2(q)$, $\mathrm{PGL}_2(q)$ を2.1節で定義する位数4の部分群 H で左から割ったものである．この章から次のようなグラフをケーリーグラフということにする．G を群とする．S を空でない G の部分集合とし，$S = S^{-1}$ が成り立つとする．頂点の集合 V には G が右から作用しているとする．頂点の集合 V と辺の集合 $E = \{(x,y) : x,y \in V \text{ で } y = xs \text{ となる } s \in S \text{ が存在する}\}$ でできるグラフ $\mathcal{G}(V,S)$ をケーリーグラフということにする．$\left(\frac{p}{q}\right) = 1$ のとき，$Z^{p,q}$ を $S_{p,q}$ に関する $H\backslash\mathrm{PSL}_2(q)$ のケーリーグラフとする．

$$Z^{p,q} = \mathcal{G}(H\backslash\mathrm{PSL}_2(q), S_{p,q}).$$

$\left(\frac{p}{q}\right) = -1$ のとき，$Z^{p,q}$ を $S_{p,q}$ に関する $H\backslash\mathrm{PGL}_2(q)$ のケーリーグラフとする．

$$Z^{p,q} = \mathcal{G}(H\backslash\mathrm{PGL}_2(q), S_{p,q}).$$

つまり，頂点の集合は $H\backslash\mathrm{PSL}_2(q)$, $H\backslash\mathrm{PGL}_2(q)$ であり，これはどちらも群ではない．また，このグラフは頂点推移的ではない．そのために，$X^{p,q}$ では頂点の集合に対応する群の単位元についてのみ考えれば良かったところが，それだけではすまず，様々なケースについて考える必要ができた．しかし，$(p+1)$-regular であることには変わりはなく，定理2.2.6では，$X^{p,q}$ の連結性が $p^8 < q$ のときに示せたのに対して，$Z^{p,q}$ では $p \geq 5$, $p^7 < q$ のとき，ただし，$p^7 < q \leq p^8$ については p が 3, 5, 11, 17, 29, 41 以外のときに，連結であることを示すことができた．また，ループがない $Z^{p,q}$ に対して，$X^{p,q}$ 同様に，ある頂点から同じ頂点へとつながる道の数について以下の公式ができた．ただし，$s_{\mathcal{Q}_1}(p^m)$, $s_{\mathcal{Q}_2}(p^m)$ は1.3節，3.1節で定義する数である．

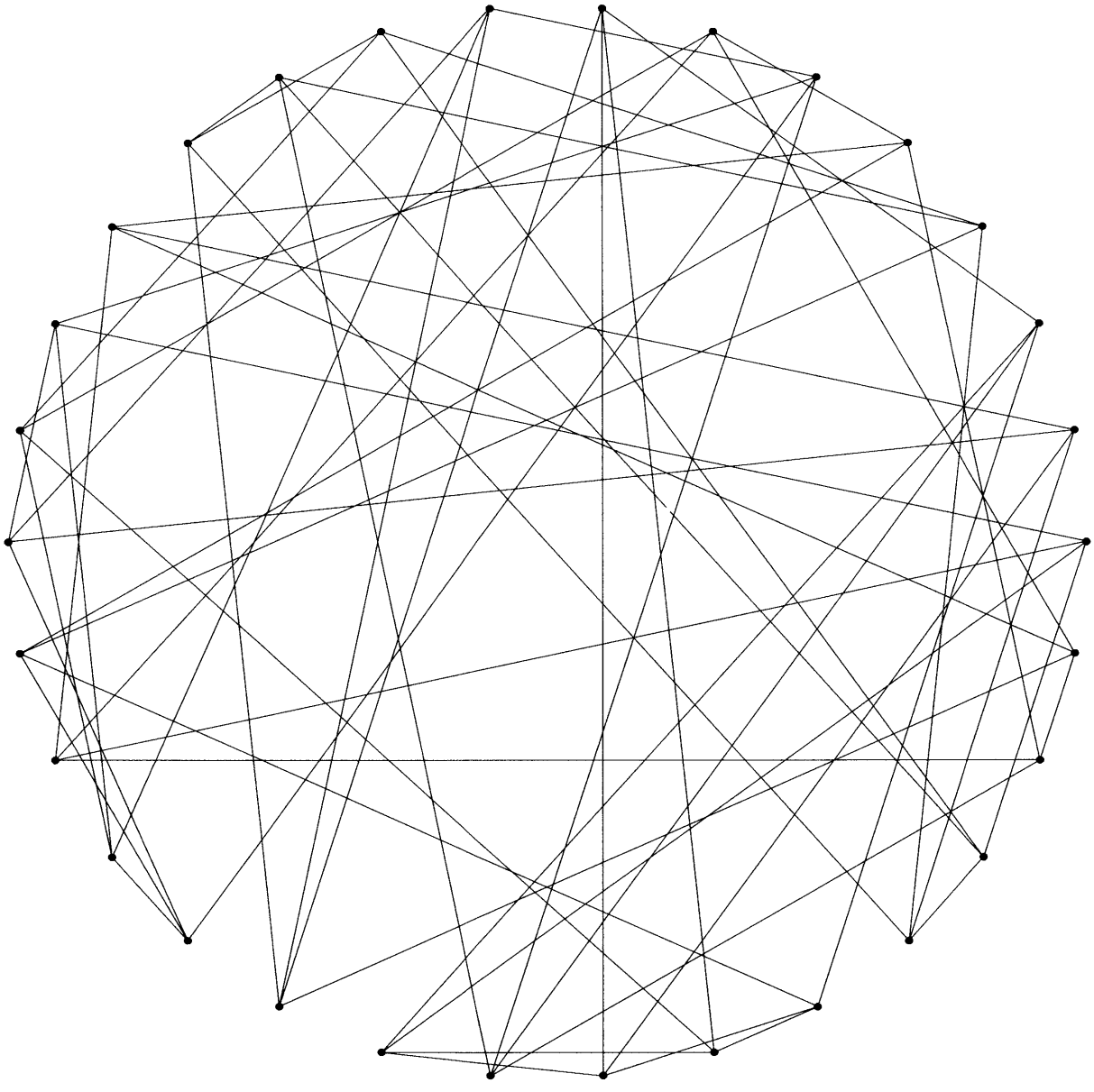
定理 0.0.3 ($Z^{p,q}$ **のトレース公式**). ループがない $Z^{p,q}$ で $|H\backslash V| = n$ とおき，p,q を $p \geq 5$, $p^8 < q$ を満たす奇素数とする．

$$c_V = \begin{cases} q-1 & (\left(\frac{p}{q}\right) = 1 \text{ かつ } p \equiv 1 \pmod 4 \text{ のとき}) \\ q+1 & (\left(\frac{p}{q}\right) = 1 \text{ かつ } p \equiv 3 \pmod 4 \text{ のとき}) \\ 2(q-1) & (\left(\frac{p}{q}\right) = -1 \text{ かつ } p \equiv 1 \pmod 4 \text{ のとき}) \\ 2(q+1) & (\left(\frac{p}{q}\right) = -1 \text{ かつ } p \equiv 3 \pmod 4 \text{ のとき}) \end{cases}$$

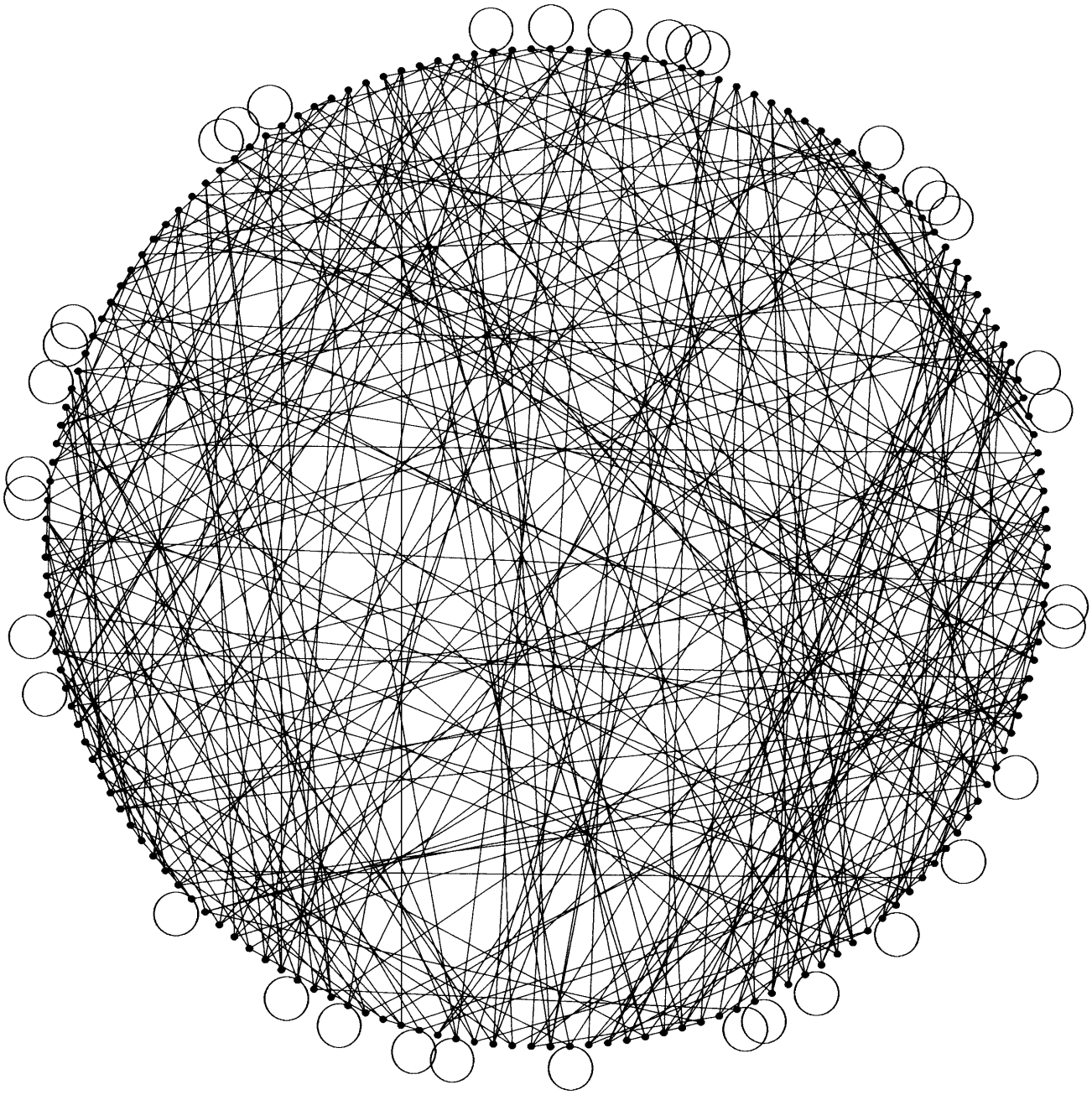
とおく．全ての $m \in \mathbb{N} \cup \{0\}$ に対し

$$\sum_{x \in H\backslash V} \sum_{0 \leq r \leq m/2} \mathfrak{f}_{m-2r,x} = \frac{n}{2} s_{\mathcal{Q}_1}(p^m) + \frac{3}{8} c_V s_{\mathcal{Q}_2}(p^m).$$

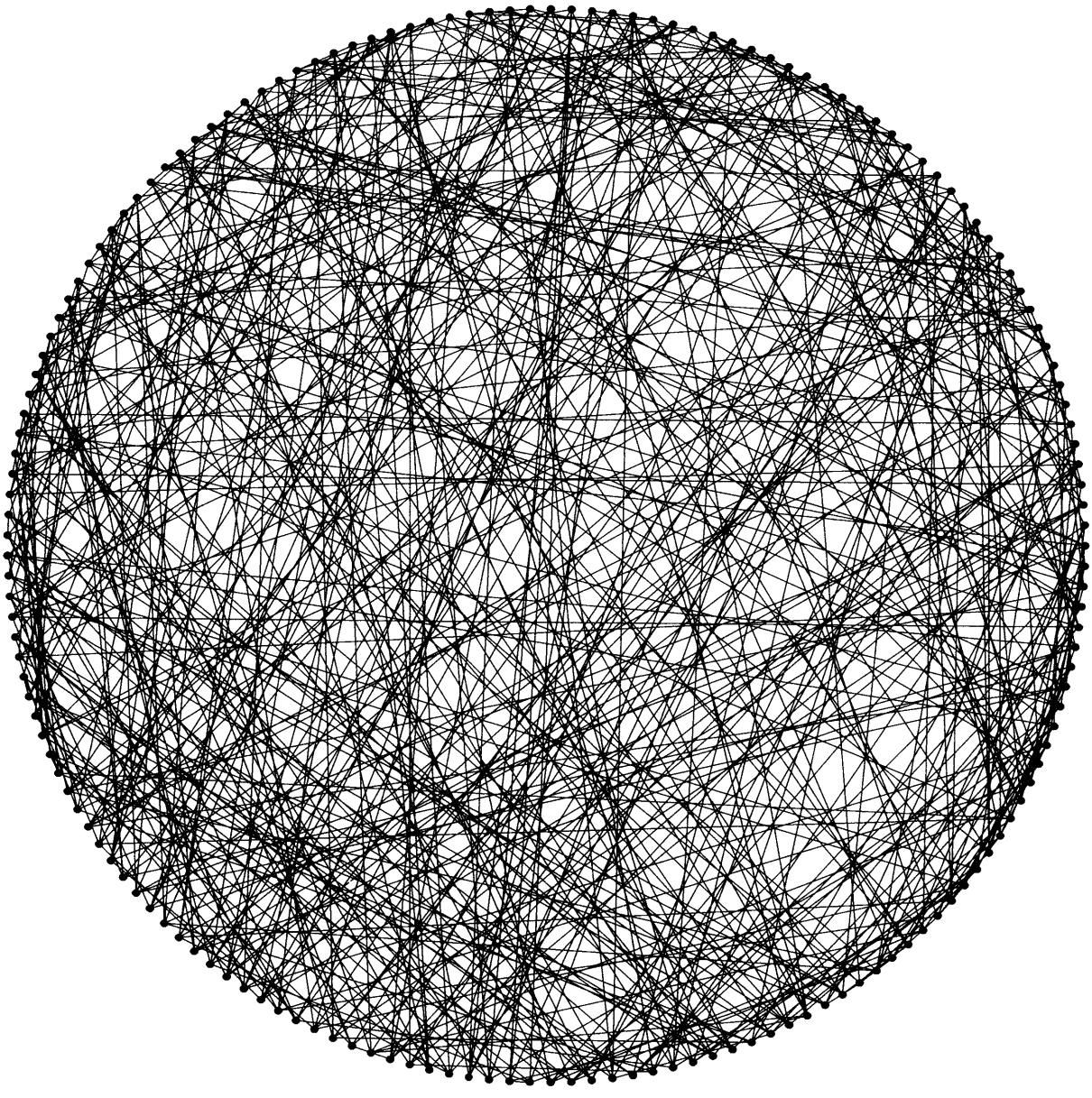
この公式に対して，ラマヌジャン予想を使うことにより，$p \geq 5$, $p^8 < q$ を満たす奇素数 p, q で，ループがない $Z^{p,q}$ がラマヌジャングラフであることを示すことができた．また，ここで仮定になっている $p^8 < q$ は $X^{p,q}$ の連結性と単純性を示すものであり，$X^{p,q}$ が連結で単純あれば，この範囲でなくとも成り立つ．以下に図示した 3 つのグラフ $Z^{3,5}, Z^{3,11}, Z^{5,11}$ は連結グラフであり，ラマヌジャングラフでもある．ただし，$Z^{3,11}$ のグラフはループを持つ．また，このグラフの頂点は，先に紹介した 3 つのグラフの頂点の群を，位数 4 の部分群 H で左から割った集合である．



$Z^{3,5}$ のグラフ：girth は 4



$Z^{3,11}$ のグラフ：ループがある例.



$Z^{5,11}$ のグラフ：girth は 3.

また 2.2 節では，p, q が $p \geq 5$, $p^8 < q$ を満たす奇素数であるとき，ループがない $Z^{p,q}$ は大きな girth を持つことが，3.2 節では同じ条件下で $\left(\frac{p}{q}\right) = 1$ のとき，大きな彩色数を持つことも示せた．特に，頂点数が $1/4$ になっているにもかかわらず，girth の評価は $1/2$ にしかならなかったことと，彩色数の評価は $X^{p,q}$ と同様のものが得られたことは，成果の 1 つである．ここから，ループがない $Z^{p,q}$ は，頂点推移的でないグラフでありながら，$\left(\frac{p}{q}\right) = 1$ かつ $p \geq 5$, $p^8 < q$ のとき，良いグラフであるということを示すことができた．

最後に，この論文を書くにあたりお世話になったたくさんの方に感謝の意を表したい．グラフのサーキットの個数の確認に有用なプログラムを作成してくれた，藤田幸司氏に，

また，授業だけでなく，院生生活全体を支えてくださった三重大学教育学部数学教室の先生方や鈴木事務官に，そして誰より，未熟な私を，このような論文が書けるまでにご指導くださり，すばらしいAppendixを書き添えてくださった指導教官である露峰先生に，この場をお借りして心からの感謝を伝えたい.

1 グラフ $X^{p,q}$

この章では Davidoff, Sarnak, Valette による [1] で述べられていることについてまとめる.

1.1 グラフ

頂点の集合 V と，辺の集合 E からなるグラフ $X = (V, E)$ について考える．$V = \{v_1, v_2, \ldots,\}$ をグラフ X の頂点の集合とする．この時，$A = (A_{ij})$ をグラフ X の隣接行列という．ただし，ここで

$$A_{ij} = (v_i \text{と } v_j \text{をつなぐ辺の数})$$

とする．いくつかの辺がつながったものを道と呼び，X の任意の 2 頂点が道でつながっているとき，その X は連結であるという．全ての隣接点をつなぐ辺が 1 本ずつしかないとき，X は単純であるという．1 本の辺が，ある頂点から同じ頂点に戻るとき，それをループという．また，全ての頂点が，隣接する 2 点を同じ色で塗らないように 2 色で塗り分けられるとき，そのグラフを二部グラフという．全ての $v_i, v_j \in V$ で $\alpha(v_i) = v_j$ となるグラフ X の自己同型写像 α が存在するとき，頂点推移的であるという．

定義 1.1.1. $k \geq 2$ を整数とする．全ての $v_i \in V$ で $\sum_{v_j \in V} A_{ij} = k$ のとき，グラフ X は *k-regular* であるという．

グラフ X を n 個の頂点の有限グラフとする．X の隣接行列 A は，重複を許して n 個の実固有値を持つ．この固有値を小さい方から

$$\mu_0 \leq \mu_1 \leq \cdots \leq \mu_{n-1}$$

とする．A の固有値の集合を X のスペクトルという．また，k-regular のグラフの隣接行列の k となる固有値を自明な固有値という．二部グラフのときは $-k$ も自明な固有値という．ここで $X = (V, E)$ の頂点の集合 V の部分集合 F の境界 ∂F を F の元と $V - F$ の元をつなぐ辺の集合と定義する．

定義 1.1.2. グラフ X の等周定数を

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

と定義する．X が有限で n 個の頂点のとき、これは次のように言い換えられる．

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

この等周定数によって，次の定義をする．

定義 1.1.3. $(X_m)_{m \geq 1}$ を $m \to +\infty$ のとき $|V_m| \to +\infty$ となる有限で連結でループのない $k-$regular のグラフの族とする．ある $\varepsilon > 0$ が存在して，全ての $m \geq 1$ で $h(X_m) \geq \varepsilon$ となるとき，$(X_m)_{m \geq 1}$ を *family of expanders* という．

family of expanders については，次のことが証明されている．

命題 1.1.4. $(X_m)_{m\geq 1}$ を $m \to +\infty$ のとき $|V_m| \to +\infty$ となる有限で連結でループのない $k-$regular のグラフの族とする．$(X_m)_{m\geq 1}$ が family of expanders であることと，ある $\varepsilon > 0$ が存在して，全ての $m \geq 1$ で $k - \mu_1(X_m) \geq \varepsilon$ となることは同値である．

この $k - \mu_1(X_m)$ をスペクトルギャップといい，スペクトルギャップが大きいほど，質の良い family of expanders であるという．

定義 1.1.5. 有限で連結な k-regular グラフ X の，全ての非自明な固有値 μ が $|\mu| \leq 2\sqrt{k-1}$ を満たすとき，X をラマヌジャングラフという．

$(X_m)_{m\geq 1}$ を $m \to +\infty$ のとき $|V_m| \to +\infty$ となる k-regular でループのないラマヌジャングラフの族とする．この族は，スペクトルギャップが大きい，質のよい family of expanders となる．

定義 1.1.6. 連結グラフ X の最小のサーキットの長さを *girth* といい $g(X)$ で表す．サーキットがないときはグラフ X を *tree* といい，$g(X) = +\infty$ とする．

命題 1.1.7. $(X_m)_{m\geq 1}$ を $m \to +\infty$ のとき $|V_m| \to +\infty$ となる有限で連結でループのない $k-$regular のグラフの族とする．$k \geq 5$ のとき，次の式が成り立つ．

$$g(X_m) \leq 2 + 2\log_{k-1}|V_m|.$$

$(X_m)_{m\geq 1}$ を $m \to +\infty$ のとき $|V_m| \to +\infty$ となる有限で連結でループのない k-regular のグラフの族とする．ある定数 $C > 0$ で $g(X_m) \geq (C + o(1))\log_{k-1}|V_m|$ となるとき，$(X_m)_{m\geq 1}$ は**大きな** girth **を持つ**という．ここで $o(1)$ は $m \to +\infty$ のとき，0 になる量を示す．

定義 1.1.8. グラフ X の隣接する 2 点を別の色で塗るとき，すべての頂点を塗り分けるのに必要な最小の数を彩色数といい，$\chi(X)$ で表す．

彩色数について次のことが示されている．

命題 1.1.9. X を有限でループのない k-regular の連結グラフとする．頂点数を n 個とすると，

$$\chi(X) \geq \frac{k}{\max\{|\mu_1|, |\mu_{n-1}|\}}.$$

さらに，X が二部グラフでないラマヌジャングラフのとき，

$$\chi(X) \geq \frac{k}{2\sqrt{k-1}} \sim \frac{\sqrt{k}}{2}.$$

$(X_m)_{m\geq 1}$ を $m \to +\infty$ のとき $|V_m| \to +\infty$ となる有限で連結でループのない k-regular のグラフの族とする．ここでは，任意の $\varepsilon > 0$ に対して定数 C_ε が存在し，$\chi(X_m) > C_\varepsilon(k^{1/6-\varepsilon})$ が成り立つとき，グラフ X は**大きな彩色数を持つ**という．

定義 1.1.10. G を群とする．S を空でない G の部分集合とし，$S = S^{-1}$ が成り立つとする．頂点の集合 $V = G$，辺の集合 $E = \{(x, y) : x, y \in G \text{ で } y = xs \text{ となる } s \in S \text{ が存在する}\}$ でできるグラフ $\mathcal{G}(G, S)$ をケーリーグラフという．

ケーリーグラフについて，次のことが示されている．

命題 1.1.11. G を群とする．$\mathcal{G}(G, S)$ を $|S| = k$ のケーリーグラフとする．
(a) $\mathcal{G}(G, S)$ は単純で k-regular の頂点推移的なグラフである．
(b) $\mathcal{G}(G, S)$ にループがないことと，$1 \notin S$ は同値である．
(c) $\mathcal{G}(G, S)$ が連結であることと，S が G を生成することは同値である．

大きな彩色数を持ち，大きな girth を持つグラフを良いグラフということにする．このようなグラフが存在することは，1959 年に Erdös が確率論的な方法で示しているが，具体例までは与えられなかった．1988 年，Phillips，Sarnak によって，頂点を $\mathrm{PGL}_2(q)$ または $\mathrm{PSL}_2(q)$ にしたケーリーグラフを作ることで，ラマヌジャングラフの具体例が構成された．このラマヌジャングラフの一部が，良いグラフであることが示されている．

1.2 四元数

1.3 節で Phillips，Sarnak によって構成されたラマヌジャングラフの具体例について述べるための準備をする．まずルジャンドル記号 $\left(\frac{p}{q}\right)$ を次のように定義する．

$$\left(\frac{p}{q}\right) = \begin{cases} 0 & (p \text{ が } q \text{ で割り切れるとき}) \\ 1 & (p \text{ が } q \text{ で割り切れず } p \text{ が } \bmod q \text{ で平方剰余のとき}) \\ -1 & (p \text{ が } q \text{ で割り切れず } p \text{ が } \bmod q \text{ で平方非剰余のとき}). \end{cases}$$

$k \geq 2, n \in \mathbb{N}$ で

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

とする．

命題 1.2.1. 任意の $\varepsilon > 0$ に対して $r_3(n) = O_\varepsilon(n^{1/2+\varepsilon})$ である．

定理 1.2.2 (Jacobi **の定理**)**.** n を正の奇数とする．このとき，$r_4(n) = 8\sum_{d|n} d$ である．

$\mathbb{H}(\mathbb{Z})$ を整数を係数とする四元数の集合とする．ある四元数 $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ とおく．ノルムを $N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ とし，ノルムが奇数のとき，その四元数は奇数であるといい，ノルムが偶数のときはその四元数を偶数という．また，a_0 が奇数で a_1, a_2, a_3 が偶数，または a_0 が偶数で a_1, a_2, a_3 が奇数であるとき，その四元数は**強奇数**であるという．このとき，$(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ を**強奇数を作る組**という．
$\alpha \in \mathbb{H}(\mathbb{Z})$ で，ノルムが奇素数のべき乗のものを考える．つまり，奇素数を p とし，$\alpha = a_0 + a_1 i + a_2 j + a_3 k$ とおくと，$N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 = p^k$ となる $\alpha \in \mathbb{H}(\mathbb{Z})$ の集合について考える．定理 1.2.2 より，$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$ は $8(p+1)$ 個の整数解を持つ．この整数解の組み合わせは，ノルムが p の整四元数 $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ に対応する．$p \equiv 1 \pmod 4$ のときは，1 つの a_i が奇数で，残りの 3 つは偶数となり，$p \equiv 3 \pmod 4$ のときは，1 つの a_i が偶数で，残りの 3 つは奇数となる．この，唯一の奇数または偶数

となる係数を a_i^0 とする．$\varepsilon\alpha$ で $a_i^0 \neq 0$ のとき，$\varepsilon\alpha$ として 8 個の四元数が考えられるが，a_0 として a_i^0 を持つものだけに絞る．$a_i^0 = 0$ のときは，$p \equiv 3 \pmod 4$ に限られる．このとき，ε を四元数の単数とすると，$a_0 = 0$ になる四元数を作ることができる．このとき，$\overline{\varepsilon\alpha} = -\varepsilon\alpha$ だから，どちらか 1 つに絞る．すると，a_0 に唯一の奇数または偶数がくるもので，$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$ をみたすものは $p+1$ 個あることが分かる．このとき，対応する四元数 α は

$$\alpha \equiv 1 \pmod 2, \text{または } \alpha \equiv i + j + k \pmod 2$$

となる．この対応する四元数の集合を S_p とおくと，S_p には $a_i^0 > 0$ のものはいつも，α と $\overline{\alpha}$ が両方入り，$a_i^0 = 0$ のものはいつも α だけしか入らない．つまり S_p は次のようなノルムが p の強奇数の集合である．

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

$$\text{ただし} \alpha = a_0 + a_1 i + a_2 j + a_3 k\,,\ \beta = b_1 i + b_2 j + b_3 k \in \mathbb{H}(\mathbb{Z}),$$

$$\alpha_i \overline{\alpha_i} = \beta_j^2 = p\ (1 \leq i \leq s, 1 \leq j \leq t)\,,\ 2s + t = p + 1.$$

定義 1.2.3. $\alpha_i\overline{\alpha_i}$, $\overline{\alpha_i}\alpha_i$, β_j^2 $(i = 1, \ldots, s,\ j = 1, \ldots, t)$ を含まない S_p の元の積を S_p 上の既約ワードという．

次のことも分かっている．

定理 1.2.4. $k \in \mathbb{N}, \alpha \in \mathbb{H}(\mathbb{Z})$ が $N(\alpha) = p^k$ を満たすとき，α は一意的な因数分解 $\alpha = \varepsilon p^r w_m$ を持つ．ただしここでは，ε は $\mathbb{H}(\mathbb{Z})$ の単数，w_m は S_p の長さ m の既約ワードのことを指す．

命題 1.2.5. K を標数が 2 ではない体とする．$x^2 + y^2 + 1 = 0$ となる $x, y \in K$ が存在するとき，写像

$$\psi : \mathbb{H}(K) \to M_2(K),$$

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

は同型写像になる．

q 個の元の有限体を $\mathbb{F}_q$ とし，$\mathbb{F}_q$ の 0 でない元でできる乗法群を $\mathbb{F}_q^\times$ とする．これについて，以下のことが分かっている．

命題 1.2.6. $\mathbb{F}_q^\times$ は $\frac{p-1}{2}$ 個の平方剰余を持つ．

定理 1.2.7. $p \in \mathbb{N}$ を奇素数とする．このとき，$p \equiv 1 \pmod 4$ であることと，-1 が $\mathbb{F}_q^\times$ 内で平方剰余であることは同値である．

命題 1.2.8. q を奇素数とすると，$x^2 + y^2 + 1 = 0$ となるような $x, y \in \mathbb{F}_q$ が存在する．

最後に，次のような $\mathbb{H}(\mathbb{Z})$ の部分集合 Λ' を定義しておく．

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha\text{は強奇数}\,,\ N(\alpha)\ \text{は}\ p\ \text{のべき乗}\ \}. \tag{1}$$

明らかに $S_p \subset \Lambda'$ となる．

系 1.2.9. $\alpha \in \Lambda'$ で $N(\alpha) = p^k$ となるものは全て，一意的な因数分解 $\alpha = \pm p^r w_m$ を持つ．ただしここでは，$r \in \mathbb{N}$ で，w_m は S_p の長さ m の既約ワードで $k = 2r + m$ とする．

1.3 グラフ $X^{p,q}$ と $Y^{p,q}$

p, q を異なる奇素数とする．$\mathbb{H}(\mathbb{Z})$ の元の係数を法 q で reduction する写像 $\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$ を作る．命題 1.2.8 より $x^2 + y^2 + 1 \equiv 0 \pmod{q}$ となる $x, y \in \mathbb{Z}$ が存在するので，このような整数を選ぶと，命題 1.2.5 の同型写像 $\psi_q : \mathbb{H}(\mathbb{F}_q) \to M_2(\mathbb{F}_q)$ を作ることができる．この写像は次の 2 つの性質を持つ．
(a) $\alpha \in \mathbb{H}(\mathbb{F}_q)$ で $N(\alpha) = \det \psi_q(\alpha)$ である．
(b) $\alpha \in \mathbb{H}(\mathbb{F}_q)$ が $\alpha = \overline{\alpha}$ を満たすとき，$\psi_q(\alpha)$ はスカラー行列である．
今，$N(\alpha) \not\equiv 0 \pmod{q}$ となる $\alpha \in \mathbb{H}(\mathbb{Z})$ で $\psi_q(\tau_q(\alpha))$ は $\mathrm{GL}_2(q)$ に属するので，次の準同型写像

$$\varphi : \mathrm{GL}_2(q) \to \mathrm{PGL}_2(q)$$

を考えると，その核はスカラー行列からなる部分群になる．ここで

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

とおく．すると，$S_{p,q}$ は $\mathrm{PGL}_2(q)$ の $S_{p,q}^{-1} = S_{p,q}$ となる部分集合である．

命題 1.3.1. $q > 2\sqrt{p}$ のとき，$|S_{p,q}| = p + 1$.

命題 1.3.2. $A \in \mathrm{GL}_2(q)$ とする．$\varphi(A) \in \mathrm{PSL}_2(q)$ と $\left(\frac{\det A}{q}\right) = 1$ は同値である．

以上の 2 つの命題より，次のケーリーグラフを作る．
$\left(\frac{p}{q}\right) = 1$ のとき，$S_{p,q}$ は $\mathrm{PSL}_2(q)$ に含まれる．このとき，$X^{p,q}$ を $S_{p,q}$ に関する $\mathrm{PSL}_2(q)$ のケーリーグラフとする．

$$X^{p,q} = \mathcal{G}(\mathrm{PSL}_2(q), S_{p,q}).$$

$\left(\frac{p}{q}\right) = -1$ のとき，$S_{p,q}$ は $\mathrm{PGL}_2(q) - \mathrm{PSL}_2(\mathrm{q})$ に含まれる．このとき，$X^{p,q}$ を $S_{p,q}$ に関する $\mathrm{PGL}_2(q)$ のケーリーグラフとする．

$$X^{p,q} = \mathcal{G}(\mathrm{PGL}_2(q), S_{p,q}).$$

次に，新たに $Y^{p,q}$ というグラフを作る．式 (1) の集合 Λ' の元 α, β で，次の同値関係 $\alpha \sim \beta$ をつくる．

$$\alpha \sim \beta : p^m\alpha = \pm p^n\beta \text{となる } m, n \in \mathbb{N} \text{が存在する}.$$

$\alpha \in \Lambda'$ の同値類を $[\alpha]$ と書き，同値類の集合を $\Lambda = \Lambda'/\sim$ と書く．このとき，商写像を

$$\mathcal{F} : \Lambda' \to \Lambda$$

$$\mathcal{F}(\alpha) = [\alpha]$$

とする．

命題 1.3.3. (a) Λ は群である．
(b) ケーリーグラフ $\mathcal{G}(\Lambda, \mathcal{F}(S_p))$ は $(p+1)$-regular の tree である．

$\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$ は Λ' を $\mathbb{H}(\mathbb{Z})$ の乗法の逆元がある部分群 $\mathbb{H}(\mathbb{Z})^\times$ に写す．$\mathbb{H}(\mathbb{Z})^\times$ の中心部分群を Z_q とする;

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

$\alpha, \beta \in \Lambda'$ で $\alpha \sim \beta$ のとき，$\tau(\alpha)^{-1}\tau(\beta) \in Z_q$ だから，$\tau : \Lambda' \to \mathbb{H}(\mathbb{F}_q)^\times$ から，群準同型 $\Pi : \Lambda \to \mathbb{H}(\mathbb{F}_q^\times)/Z_q$ が作れる．この写像の核 $\ker \Pi_q$ を $\Lambda(q)$ と書き，Π_q の像を商群 $\Lambda/\Lambda(q)$ と同一視することにする．

補題 1.3.4. $\Lambda(q) = \{[\alpha] \in \Lambda :\ \alpha = a_0 + a_1 i + a_2 j + a_3 k,\ a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod{q}\}$.

また，$T_{p,q} = (\Pi_q \circ \mathcal{F})(S_p)$ とすると，命題 1.3.1 より，$q > 2\sqrt{p}$ のとき，$|T_{p,q}| = p + 1$ が成り立つ．ここで，グラフ $Y^{p,q}$ を $T_{p,q}$ に関する $\Lambda/\Lambda(q)$ のケーリーグラフとする．

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

命題 1.3.3，命題 1.1.11 より，$q > 2\sqrt{p}$ でグラフ $Y^{p,q}$ は $(p+1)$-regular の連結グラフであることが分かる．ここで，$\psi_q : \mathbb{H}(\mathbb{F}_q) \to \mathrm{PGL}_2(q)$ は Z_q を $\mathrm{GL}_2(q)$ のスカラー行列に写す．これは，$\varphi : \mathrm{GL}_2(q) \to \mathrm{PGL}_2(q)$ の核になるので，同型写像

$$\beta : \mathbb{H}(\mathbb{F}_q)^\times/Z_q \to \mathrm{PGL}_2(q)$$

を作ることができる．つまり，次のような可換図式が成り立つ．

$$\begin{array}{ccccc} S_p \subset \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^\times & \xrightarrow{\psi_q} & \mathrm{GL}_2(q) \\ \mathcal{F}\downarrow & & \downarrow & & \downarrow\varphi \\ \Lambda & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^\times/Z_q & \xrightarrow{\beta} & \mathrm{PGL}_2(q) \end{array}$$

この $Y^{p,q}$ について，次のことが成り立つ．

命題 1.3.5. $q > 2\sqrt{p}$ とする．$g(Y^{p,q}) \geq 2\log_p q$ である．特に $\left(\frac{p}{q}\right) = -1$ のときは，$g(Y^{p,q}) \geq 4\log_p q - \log_p 4$ である．

これを使って $X^{p,q}$ と $Y^{p,q}$ の関係について次のことが示されている．ただし，これ以降 $|X|$ はグラフ X の頂点数を表す．

定理 1.3.6. $p \geq 5$ とする．$q > p^8$ のとき，$X^{p,q}$ は連結グラフで，$Y^{p,q}$ と同型である．つまり，グラフ $X^{p,q}$ は連結な $(p+1)$-regular グラフである．また，
$\left(\frac{p}{q}\right) = 1$ のとき，$X^{p,q}$ は二部グラフではなく，

$$g(X^{p,q}) \geq \frac{2}{3}\log_p |X^{p,q}|.$$

$\left(\frac{p}{q}\right) = -1$ のとき，$X^{p,q}$ は二部グラフで，

$$g(X^{p,q}) \geq \frac{4}{3}\log_p |X^{p,q}| - \log_p 4.$$

$x \in V$ で，x から y への，引き返しのない長さ l の道の数を $f_{l,x,y}$ とおく．特に $x = y$ のとき $f_{l,x}$ と書く．U_m を m 次のチェビシェフ多項式，すなわち，$m \in \mathbb{N} \cup \{0\}$ で $U_m(\cos\theta) = \sin(m+1)\theta/\sin\theta$ を満たす式とする．

定理 1.3.7 (トレース公式). k-regular で連結なループがない単純グラフを $X=(V,E)$ とする．全ての $m \in \mathbb{N} \cup \{0\}$ で

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

頂点推移的なグラフでは，どの頂点からの道の数も変わらないので，$x=y$ のときはどの頂点についても f_l で表すことにする．すると，上の定理は次のように書き換えられる．

系 1.3.8. $X=(V,E)$ を頂点推移的で n 個の頂点を持つ，有限で連結なループがない k-regular の単純グラフとする．このとき，全ての $m \in \mathbb{N} \cup \{0\}$ で

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

次に下のような二次形式を導入する．

$$\mathcal{Q}_1(x_0,x_1,x_2,x_3) = x_0^2 + q^2(x_1^2+x_2^2+x_3^2).$$

また，$m \geq 0$ で次のようにおく．

$$s_{\mathcal{Q}_1}(p^m) = |\{(x_0,x_1,x_2,x_3) \in \mathbb{Z}^4 : \mathcal{Q}_1(x_0,x_1,x_2,x_3) = p^m, \\ (x_0,x_1,x_2,x_3) \text{ は強奇数を作る組 }\}|.$$

ここで，m が偶数のとき，または $p \equiv 1 \pmod 4$ のときは，x_0が奇数で x_1,x_2,x_3は偶数に限られるので，次のような二次形式を考えれば良い．

$$\mathcal{Q}_1'(x_0,x_1,x_2,x_3) = x_0^2 + 4q^2(x_1^2+x_2^2+x_3^2).$$

このとき，$s_{\mathcal{Q}_1'}(p^m)$ は二次形式 $\mathcal{Q}_1'$ の p^m を表現する仕方の個数である．
$s_{\mathcal{Q}_1}(p^m)$ と道の数について，次の補題が成り立つ．

補題 1.3.9. p,q を $p \geq 5$, $q > p^8$ を満たす奇素数とする．$m \in \mathbb{N} \cup \{0\}$ で

$$s_{\mathcal{Q}_1}(p^m) = 2 \sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r}.$$

これらを使って，次の $X^{p,q}$ についての定理，系が示される．

定理 1.3.10. p,q を $p \geq 5$, $q > p^8$ を満たす奇素数とする．$0 < \varepsilon < 1/6$ を満たす実数 ε で十分大きな q に対して，$X^{p,q}$ の全ての非自明な固有値 μ は

$$|\mu| \leq p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon}$$

を満たす．このときの $X^{p,q}$ の族は family of expanders である．

系 1.3.11. p,q を $p \geq 5$, $q > p^8$ を満たす奇素数とする．$\left(\frac{p}{q}\right) = 1$ のとき，$0 < \varepsilon < 1/6$ を満たす実数 ε で十分大きな q に対して，

$$\chi(X^{p,q}) \geq \frac{p+1}{p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon}}.$$

よって，$X^{p,q}$ は上の系の仮定を満たすとき，良いグラフであるといえる．ラマヌジャン予想を使うと，$X^{p,q}$ はラマヌジャングラフであることも示すことができる．

2 グラフ $Z^{p,q}$

2.1 グラフ $Z^{p,q}$ と $D^{p,q}$

定義 1.1.10 でケーリーグラフの頂点の集合は群としたが，ここからは頂点の集合を群に限らず，頂点推移的でないグラフを考えていく．G を群とする．S を空でない G の部分集合とし，$S = S^{-1}$ が成り立つとする．頂点の集合 V には G が右から作用しているとする．頂点の集合 V と辺の集合 $E = \{(x, y) : x, y \in V \text{ で } y = xs \text{ となる } s \in S \text{ が存在する}\}$ でできるグラフ $\mathcal{G}(V, S)$ をケーリーグラフということにする．今，K を $\mathbb{H}(\mathbb{Z})$ の単数の集合をする．つまり $K = \{\pm 1, \pm i, \pm j, \pm k\}$ とする．p, q を奇素数とする．1.3 節の写像を使って，

$$H = (\varphi \circ \psi_q \circ \tau_q)(K)$$

とおく．このとき，ケーリーグラフ $Z^{p,q}$ を次のように定義する．
$\left(\frac{p}{q}\right) = 1$ のとき，$Z^{p,q}$ を $S_{p,q}$ に関する $H\backslash \mathrm{PSL}_2(q)$ のケーリーグラフとする．

$$Z^{p,q} = \mathcal{G}(H\backslash \mathrm{PSL}_2(q), S_{p,q}).$$

$\left(\frac{p}{q}\right) = -1$ のとき，$Z^{p,q}$ を $S_{p,q}$ に関する $H\backslash \mathrm{PGL}_2(q)$ のケーリーグラフとする．

$$Z^{p,q} = \mathcal{G}(H\backslash \mathrm{PGL}_2(q), S_{p,q}).$$

次に，グラフ $D^{p,q}$ を考える．p を奇素数とする．

$$\Omega' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \ N(\alpha) = p^m\}$$

とおく．このとき，$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \text{ は強奇数}, N(\alpha) \text{ は } p \text{ のべき乗}\}$ で $\Omega' = \Lambda' \cup i\Lambda' \cup j\Lambda' \cup k\Lambda'$ (直和) と書ける．この Ω' 上で 1.3 節にある同値関係 $\sim$ を定義する．

$$\alpha \sim \beta : p^m\alpha = \pm p^n\beta \text{となる } m, n \in \mathbb{N} \text{が存在する}.$$

$\alpha \in \Omega'$ の同値類を $[\alpha]$，同値類の集合を $\Omega = \Omega'/\sim$ と定義する．その商写像も 1.3 節と同様に

$$\mathcal{F} : \Omega' \to \Omega,$$

$$\mathcal{F}(\alpha) = [\alpha]$$

と定義する．互いに異なる四元数の単数 ε，δ と任意の $[\alpha] \in \Lambda$ で，$[\varepsilon\alpha] \neq [\delta\alpha]$ だから，$\Omega = \Lambda \cup i\Lambda \cup j\Lambda \cup k\Lambda$ (直和) が成り立つ．

命題 2.1.1. (a) Ω は群である．
(b) $\mathcal{G}(\Omega, \mathcal{F}(S_p))$ は 4 つの連結な成分を持つ．その各々は $(p+1)$-regular の tree で同型である．

証明. (a) $\alpha \in \Omega'$ とする．$\alpha\overline{\alpha} = \overline{\alpha}\alpha = p^m \sim 1$ より，$[\alpha]^{-1} = [\overline{\alpha}]$ が成り立つ．
(b) $\beta, \gamma \in S_p$ とする．$\alpha \sim \beta$ のとき，$\alpha = \beta$ を意味するので，$|\mathcal{F}(S_p)| = p + 1$ である．
定理 1.2.4 より，$\alpha \in \Omega$ は $\alpha = \varepsilon p^r w_m$ と書ける．ただしここでは，ε は $\mathbb{H}(\mathbb{Z})$ の単数，w_m

は S_p の長さ m の既約ワードとする．$\varepsilon \neq \pm\varepsilon'$ のとき，$\varepsilon(S_p$の元の積$) \nsim \varepsilon'(S_p$の元の積$)$ だから，式 (1) の集合を使って，

$$\mathcal{F}(\Omega') = \mathcal{F}(\Lambda') \cup \mathcal{F}(i\Lambda') \cup \mathcal{F}(j\Lambda') \cup \mathcal{F}(k\Lambda') \text{ (直和)}$$

が成り立つ．命題 1.3.3 より，ケーリーグラフ $\mathcal{G}(\mathcal{F}(\Lambda'), \mathcal{F}(S_p))$ は連結グラフである．また，$[\varepsilon\alpha] = [\varepsilon w_m]$ だから，$[\varepsilon]$ を始点として，全ての $\mathcal{F}(\varepsilon\Lambda')$ の元は $[\varepsilon]$ と S_p の既約ワードの積で書けるので，$\mathcal{G}(\mathcal{F}(\varepsilon\Lambda'), \mathcal{F}(S_p))$ も連結で $\mathcal{G}(\mathcal{F}(\Lambda'), \mathcal{F}(S_p))$ と同型である．よって，$\mathcal{G}(\mathcal{F}(\varepsilon\Lambda'), \mathcal{F}(S_p))$ は連結ではないが，同型な 4 つの tree からなるグラフである． □

1.3 節の写像 τ_q は Ω' を $\mathbb{H}(\mathbb{Z})^\times$ に写す．$\mathbb{H}(\mathbb{F}_q)$ の中心部分群 Z_q で $\alpha, \beta \in \Omega'$ のとき，$\alpha \sim \beta$ とすると $\tau_q(\alpha)^{-1}\tau_q(\beta) \in Z_q$ が成り立つから，準同型 $\Pi_q : \Omega \to \mathbb{H}(\mathbb{F}_q)^\times / Z_q$ が作れる．このときの核 $\ker \Pi_q$ を $\Omega(q)$ と書くと，像は $\Omega/\Omega(q)$ と同一視できる．

補題 2.1.2. ε を ± 1 以外の四元数の単数とする．x_ε を $\Pi_q([x_\varepsilon]) = \Pi_q([\varepsilon])$ を満たす Λ' の元とする．このとき，次が成り立つ．

$$\Omega(q) = \Lambda(q) \cup [ix_i]\Lambda(q) \cup [jx_j]\Lambda(q) \cup [kx_k]\Lambda(q).$$

証明. $\varepsilon \in \{\pm i, \pm j, \pm k\}$ とする．まず，左辺の集合が右辺の集合を含むことを示す．$[\beta] \in \Omega$ とする．$[\beta] \in \Lambda(q)$ のときは，$[\beta] \in \Omega(q)$ である．$[\beta] \in [\varepsilon x_\varepsilon]\Lambda(q)$ のときは，$\alpha \in \Lambda(q)$ で $[\beta] = [\varepsilon x_\varepsilon \alpha]$ と書ける．

$$\begin{aligned}\Pi_q([\beta]) &= \Pi_q([\varepsilon x_\varepsilon \alpha]) \\ &= \Pi_q([\varepsilon])\Pi_q([\varepsilon])\Pi_q([\alpha]) \\ &= \Pi_q([\alpha])\end{aligned}$$

だから $[\beta] \in \Omega(q)$ である．よって，

$$\Omega(q) \supset \Lambda(q) \cup [ix_i]\Lambda(q) \cup [jx_j]\Lambda(q) \cup [kx_k]\Lambda(q).$$

逆に，$\beta \in \Omega(q)$ とする．このとき，$\tau_q(\beta) \in Z_q$ だから β は $b_1 \equiv b_2 \equiv b_3 \equiv 0 \pmod q, b_0 \equiv 0 \pmod q$ を満たす．$\beta \in \Lambda'$ のときは，明らかに $[\beta] = \Lambda(q)$ が成り立つ．$\beta \in \varepsilon\Lambda'$ のときは，$\alpha \in \Lambda'$ で $\beta = \varepsilon\alpha$ となるものがある．

$$\Pi_q([\beta]) = \Pi_q([\varepsilon\alpha]) = \Pi_q(\varepsilon)\Pi_q(\alpha) = [1]\Omega(q)$$

だから，$\Pi_q([\alpha]) = [\varepsilon]\Omega(q)$ でなければならない．よって，ある $[\alpha'] \in \Lambda(q)$ で $[\alpha] = [x_\varepsilon][\alpha']$ と書ける．すなわち，$[\beta] = [\varepsilon\alpha] = [\varepsilon][x_\varepsilon][\alpha'] \in \Lambda(q)$ がいえるので，

$$\Omega(q) \subset \Lambda(q) \cup [ix_i]\Lambda(q) \cup [jx_j]\Lambda(q) \cup [kx_k]\Lambda(q).$$

□

次に $\Omega/\Omega(q)$ 上の同値関係 $\sim$ を考える．

$[\alpha]\Omega(q) \sim [\beta]\Omega(q) : [\varepsilon][\alpha]\Omega(q) = [\varepsilon'][\beta]\Omega(q)$ となる四元数の単数$\varepsilon, \varepsilon'$が存在する．

$(\Pi_q \circ \mathcal{F})(K) = K'$ とする．このとき，商写像を

$$\rho : \mathbb{H}(\mathbb{F}_q)^\times / Z_q \to K' \backslash \mathbb{H}(\mathbb{F}_q)^\times / Z_q$$

と定義すると，$(\rho \circ \Pi \circ \mathcal{F})(\Lambda') = (\rho \circ \Pi \circ \mathcal{F})(\varepsilon\Lambda')$ が成り立つ．$(\rho \circ \Pi \circ \mathcal{F})(\Lambda') = G_q$ とする．1.3 節と同様に $T_{p,q} = (\Pi \circ \mathcal{F})(S_p)$ とし，グラフ $D^{p,q}$ を $T_{p,q}$ に関する G_q のケーリーグラフとすると，$D^{p,q} = \mathcal{G}(G_q, T_{p,q})$ である．命題 2.1.1 より，G_q の元は $T_{p,q}$ の元の積で書けて，$D^{p,q}$ は $(p+1)$-regular の連結グラフとなる．$(\varphi \circ \psi_q \circ \tau_q)(K) = H$ だから 1.3 節の β より，次の同型写像ができる．

$$\sigma : K' \backslash (\mathbb{H}(\mathbb{F}_q)^\times / Z_q) \to H \backslash \mathrm{PGL}_2(q).$$

よって，次のような可換図式が成立する．

$$\begin{array}{ccccccc}
S_p \subset \Omega' & \xrightarrow{\tau_q} & \mathbb{H}(\mathcal{F}_q)^\times & \xrightarrow{\psi_q} & \mathrm{GL}_2(q) & \xrightarrow{\varphi} & \mathrm{PGL}_2(q) \\
\mathcal{F}\downarrow & & & \overset{\beta}{\searrow} & & & \downarrow \\
\Omega & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^\times / Z_q & \xrightarrow{\rho} & K' \backslash \mathbb{H}(\mathbb{F}_q)^\times / Z_q & \xrightarrow{\sigma} & H \backslash \mathrm{PGL}_2(q)
\end{array}$$

グラフ $Z^{p,q}$ について次のことがいえる．

命題 2.1.3. (a) $q > 2\sqrt{p}$ とする．$Z^{p,q}$ は $X^{p,q}$ に長さ 4 のサーキットがないとき，$(p+1)$-regular の単純グラフである．
(b) $\left(\frac{p}{q}\right) = -1$ であるか，または $\left(\frac{p}{q}\right) = 1$ かつ $S_{p,q}$ の元に H の元と共役な元がないことと，$Z^{p,q}$ にループがないことは同値である．
(c) $Z^{p,q}$ が連結であることと，$V = H\langle S_{p,q} \rangle$ が成り立つことは同値である．
(d) $\left(\frac{p}{q}\right) = -1$ のとき，$Z^{p,q}$ は二部グラフである．

証明. $\left(\frac{p}{q}\right) = 1$ のとき $V = \mathrm{PSL}_2(q)$，$\left(\frac{p}{q}\right) = -1$ のとき $V = \mathrm{PGL}_2(q)$ とする．
(a) $|S_{p,q}| = p+1$ より，$(p+1)$-regular は明らかである．
グラフが単純であることを示すために，$x, y \in V$ をつなぐ多重辺があると仮定する．
$s_1 \neq s_2$ となる $s_1, s_2 \in S_{p,q}$ で，$Hxs_1 = Hy$，$Hxs_2 = Hy$，と書ける．よって，$Hxs_1 = Hxs_2$ が成り立つ．つまり $\varepsilon \in H$ で $xs_1 = \varepsilon x s_2$ となるものがある．$x = \varepsilon x s_2 s_1^{-1}$ となるので，元の式に代入すると $xs_1 = \varepsilon\varepsilon x s_2 s_1^{-1} s_2$ となり，

$$s_1 s_2^{-1} s_1 s_2^{-1} = 1$$

となって，長さ 4 のサーキットがないことに矛盾する．よってグラフ $Z^{p,q}$ は単純グラフである．
(b) 対偶を示す．$Hx \in H\backslash V$ にループがあると仮定すると，$s \in S_{p,q}$ で $Hxs = Hx$ と書ける．よって $\varepsilon \in H$ で $xs = \varepsilon x$ となるものが存在する．
$\left(\frac{p}{q}\right) = -1$ のとき，

$$S_{p,q} \subset \mathrm{PGL}_2(q) - \mathrm{PSL}_2(q) \text{ かつ } H \subset \mathrm{PSL}_2(q)$$

より，矛盾である．
$\left(\frac{p}{q}\right)=1$ のとき，

$$s=x^{-1}\varepsilon x$$

だから，s と ε が共役である．
逆に $S^{p,q}$ の元 s が H の元 ε と共役であるとすると，$x\in V$ で $xs=\varepsilon x$ と書ける．このとき，$Hxs=H\varepsilon x=Hx$ だから，$Z^{p,q}$ にループがあることになる．
(c) $Z^{p,q}$ が連結であることと，任意の $H\backslash V$ の元が，$H\backslash V$ の単位元と道でつながっていることは同値である．今 $Z^{p,q}$ が連結とすると，任意の $x\in V$ に対し $Hx=Hs_1s_2\dots s_n$ となる $s_i\in S_{p,q}$ $(i=1,2,\dots,n)$ が存在する．このとき，$h_1x=h_2s_1s_2\dots s_n$ となる $h_1,h_2\in H$ が存在する．よって，$x=h_1^{-1}h_2s_1s_2\dots s_n\in H\langle S_{p,q}\rangle$ だから，$V\subset H\langle S^{p,q}\rangle$．$V\supset H\langle S_{p,q}\rangle$ は明らかだから，$V=H\langle S_{p,q}\rangle$ である．
逆に，$V=H\langle S_{p,q}\rangle$ とすると，任意の $x\in V$ が $h\in H,(s_1s_2\dots s_n)\in\langle S_{p,q}\rangle$ で $x=h(s_1s_2\dots s_n)$ と書ける．だから，$Hx=H(s_1s_2\dots s_n)$ となる $s_1s_2\dots s_n\in S_{p,q}$ が存在するので，連結となる．
(d) $\left(\frac{p}{q}\right)=-1$ のとき，$S_{p,q}\subset \mathrm{PGL}_2(q)-\mathrm{PSL}_2(q)$ より明らかである． □

次の節で，$Z^{p,q}$ が連結グラフであることを示すために，以下のことを述べておく．

補題 2.1.4. q を奇素数とする．
(a) $q\equiv 1 \pmod 4$ とする．このとき，

$$|\{(a,b)\in\mathbb{F}_q^2 : a^2+b^2=w\}|=\begin{cases} 2q-1 & (w=0)\\ q-1 & (w\neq 0)\end{cases}.$$

(b) $q\equiv 3 \pmod 4$ とする．このとき，

$$|\{(a,b)\in\mathbb{F}_q^2 : a^2+b^2=w\}|=\begin{cases} 1 & (w=0)\\ q+1 & (w\neq 0)\end{cases}.$$

証明. $(a,b)\in\mathbb{F}_q^2$ の組み合わせの総数は q^2 ある．
(a) のとき，$a^2+b^2=0$ とすると，$a^2=-b^2$ だから，このような $(a,b)\in\mathbb{F}_q^2$ の組み合わせの総数は $2(q-1)+1=2q-1$ である．よって，和が 0 にならない $(a,b)\in\mathbb{F}_q^2$ の組み合わせの数は $q^2-(2q-1)=(q-1)^2$ である．つまり，和がある 0 でない数になる組み合わせの数は $(q-1)^2\div(q-1)=q-1$ となり，示せた．
(b) のとき，$a^2+b^2=0$ となるのは $(a,b)=(0,0)$ のときのみである．ここから (a) と同様に分かる． □

系 2.1.5. q を奇素数とする．$w\neq 0$ とする．
(a) $q\equiv 1 \pmod 4$ とする．このとき，

$$|\{(a,b)\in\mathbb{F}_q^2 : a^2+b^2=w\}|=\begin{cases} \frac{(q-1)^2}{2} & (\left(\frac{w}{q}\right)=1)\\ \frac{(q-1)^2}{2} & (\left(\frac{w}{q}\right)=-1)\end{cases}.$$

(b) $q \equiv 3 \pmod 4$ とする．このとき，

$$|\{(a,b) \in \mathbb{F}_q^2 : a^2+b^2=w\}| = \begin{cases} \frac{q^2-1}{2} & (\left(\frac{w}{q}\right)=1) \\ \frac{q^2-1}{2} & (\left(\frac{w}{q}\right)=-1) \end{cases}.$$

証明. $a^2+b^2 \neq 0$ とすれば

$$a^2+b^2 = \begin{cases} \text{平方剰余} & \text{(case 1)} \\ \text{平方非剰余} & \text{(case 2)} \end{cases}$$

である．
補題 2.1.4 から，a^2+b^2 が case 1 の場合と，case 2 の場合の数が等しければ主張は成り立つ．case 1 と case 2 の組み合わせの数が同じであることを背理法で示す．まず，case 2 の場合が 0 通りであるとする．このとき，a^2+1 は平方剰余となる．これは，a の次の数が必ず平方剰余の元であることを示し，繰り返すと，$\mathbb{F}_q$ の元が全て平方剰余であることになるので，命題 1.2.6 に矛盾する．よって，少なくとも 1 つは a^2+b^2 が平方非剰余となる (a,b) の組が存在する．ここで，一般に

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$$

が成り立つので，a^2+b^2 を平方非剰余とすると，平方非剰余の組と，平方剰余の組に 1 対 1 対応が作れる．よって，case 1 と case 2 の組み合わせの数は等しい． □

補題 2.1.6. q を奇素数とする．このとき

$$|\{(a,b,c,d) \in \mathbb{F}_q^4 : a^2+b^2+c^2+d^2=0\}| = q(q^2+q-1).$$

証明.

$$\begin{aligned}
&|\{(a,b,c,d) \in \mathbb{F}_q^4 : a^2+b^2+c^2+d^2=0\}| \\
&= \sum_{\alpha=0}^{q-1} |\{(a,b,c,d) \in \mathbb{F}_q^4 : a^2+b^2=\alpha,\ c^2+d^2=-\alpha\}| \\
&= \sum_{\alpha=0}^{q-1} |\{(a,b,c,d) \in \mathbb{F}_q^4 : a^2+b^2=\alpha\}| \times |\{(a,b,c,d) \in \mathbb{F}_q^4 : c^2+d^2=-\alpha\}| \\
&= \begin{cases} (2q-1)^2+(q-1)^2\times(q-1) & (q \equiv 1 \pmod 4) \\ 1+(q+1)^2\times(q-1) & (q \equiv 3 \pmod 4) \end{cases} \\
&= q^3+q^2-q.
\end{aligned}$$

□

補題 2.1.7. q を奇素数とする．(a) $q \equiv 1 \pmod 4$ とする．このとき，

$$|\{(a,b,c) \in \mathbb{F}_q^3 : a^2+b^2+c^2=w\}| = \begin{cases} q^2 & (w=0) \\ q(q+1) & (\left(\frac{w}{q}\right)=1) \\ q(q-1) & (\left(\frac{w}{q}\right)=-1) \end{cases}.$$

(b) $q \equiv 3 \pmod 4$ とする．このとき，

$$|\{(a,b,c) \in \mathbb{F}_q^3 : a^2+b^2+c^2 = w\}| = \begin{cases} q^2 & (w=0) \\ q(q-1) & (\left(\frac{w}{q}\right)=1) \\ q(q+1) & (\left(\frac{w}{q}\right)=-1) \end{cases}.$$

証明. (a) の場合について考える．まず

$$\begin{aligned} &|\{(a,b,c) \in \mathbb{F}_q^3 : a^2+b^2+c^2 = 0\}| \\ &= \sum_{c=0}^{q-1} |\{(a,b) \in \mathbb{F}_q^2 : a^2+b^2 = -c^2\}| \\ &= (2q-1) + (q-1)\times(q-1) \\ &= q^2 \end{aligned}$$

が成り立つ．すると $\left(\frac{w}{q}\right)=1$ のとき，$-w$ も平方剰余なので，$d_0^2 = -w$ を満たすような $d_0 \in \mathbb{F}_q^\times$ をとる．

$$\begin{aligned} &|\{(a,b,c) \in \mathbb{F}_q^3 : a^2+b^2+c^2 = w\}| \\ &= |\{(a,b,c) \in \mathbb{F}_q^3 : a^2+b^2+c^2+d_0^2 = 0\}| \\ &= \frac{1}{q-1}|\{(a,b,c,d) \in \mathbb{F}_q^4, d \in \mathbb{F}_q^\times : a^2+b^2+c^2+d^2 = 0\}| \\ &= \frac{1}{q-1}\{|\{(a,b,c,d) \in \mathbb{F}_q^4 : a^2+b^2+c^2+d^2 = 0\}| - |\{(a,b,c) \in \mathbb{F}_q^3 : a^2+b^2+c^2 = 0\}|\} \\ &= \frac{1}{q-1}(q^3+q^2-q-q^2) \\ &= q(q+1). \end{aligned}$$

が成り立つ．$\left(\frac{w}{q}\right)=-1$ のとき，平方剰余の数は，$(q-1)/2$ だから，$a^2+b^2+c^2$ が平方非剰余になる組み合わせの数は

$$|\mathbb{F}_q^3| - \frac{1}{q-1}\times q(q+1) - q^2 = q^3 - \frac{1}{2}(q-1)q(q+1) - q^2 = \frac{1}{2}q(q-1)^2$$

である．平方非剰余の数も $(q-1)/2$ だから，

$$\begin{aligned} &|\{(a,b,c) \in \mathbb{F}_q^3 : a^2+b^2+c^2 = w\}| \\ &= \frac{1}{(q-1)/2}\times\frac{1}{2}q(q-1)^2 \\ &= q(q-1) \end{aligned}$$

が成り立つ．

(b) の場合について考える．まず

$$\begin{aligned}
&|\{(a,b,c) \in \mathbb{F}_q^3 : a^2+b^2+c^2 = 0\}| \\
&= \sum_{c=0}^{q-1} |\{(a,b) \in \mathbb{F}_q^2 : a^2+b^2 = -c^2\}| \\
&= (2q-1) + (q+1) \times (q-1) \\
&= q^2
\end{aligned}$$

が成り立つ．この場合も $\left(\frac{w}{q}\right) = -1$ のとき，$-w$ は平方剰余であるので，(a) と同様の計算で

$$|\{(a,b,c) \in \mathbb{F}_q^3 : a^2+b^2+c^2 = w\}| = q(q+1)$$

が示せる．ここから $\left(\frac{w}{q}\right) = 1$ のときも同様に分かる． □

以上のことから，次の命題を示す．

命題 2.1.8. B を $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ と共役な $\mathrm{PSL}_2(q)$ の元とする．$C_V(B) = \{A \in V : AB = BA\}$ とする．このとき次のことがいえる．
$p \equiv 1 \pmod 4$ のとき，$|C_{\mathrm{PSL}_2(q)}(B)| = q-1$.
$p \equiv 3 \pmod 4$ のとき，$|C_{\mathrm{PSL}_2(q)}(B)| = q+1$.
$p \equiv 1 \pmod 4$ のとき，$|C_{\mathrm{PGL}_2(q)}(B)| = 2(q-1)$.
$p \equiv 3 \pmod 4$ のとき，$|C_{\mathrm{PGL}_2(q)}(B)| = 2(q+1)$.

証明. $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ として示す．$A = \begin{pmatrix} a_0 & a_1 \\ a_2 & a_3 \end{pmatrix} \in V$ とおくと，

$$\begin{pmatrix} a_0 & a_1 \\ a_2 & a_3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & a_1 \\ a_2 & a_3 \end{pmatrix}$$

である．これが成り立つためには，

$$-a_1 = \alpha a_2,\ -a_3 = -\alpha a_0,\ a_0 = \alpha a_3,\ a_2 = -\alpha a_1$$

を満たす必要がある．よって $\alpha = \pm 1$ だから，$\alpha = 1$ のとき，$a = \begin{pmatrix} a_0 & a_1 \\ -a_1 & a_0 \end{pmatrix}$ となり，
$\alpha = -1$ のとき，$a = \begin{pmatrix} a_0 & a_1 \\ a_1 & -a_0 \end{pmatrix}$ となる．
まずは $|C_{\mathrm{PSL}_2(q)}(B)|$ について考える．

$$C_{\mathrm{PSL}_2(q)}(B) = \left\{ \begin{pmatrix} a_0 & a_1 \\ -a_1 & a_0 \end{pmatrix} : a_0^2 + a_1^2 = 1 \right\} \cup \left\{ \begin{pmatrix} a_0 & a_1 \\ a_1 & -a_0 \end{pmatrix} : a_0^2 + a_1^2 = -1 \right\} \quad (2)$$

である．$p \equiv 1 \pmod 4$ のときを考える．系 2.1.5 と命題 1.2.6 より，平方剰余は $(p-1)/2$ 個あるので，その内 $a_0^2 + a_1^2 = 1$ になるもの，つまり式 (2) の右辺の前の集合を満たすものの数は，

$$\frac{(q-1)^2}{2} \div \frac{q-1}{2} = q-1$$

だから，$q-1$ 通りである．これは，式 (2) の右辺の後の集合のときも同様である．よって，$a_0^2 + a_1^2 = \pm 1$ となる組み合わせは，$2(p-1)$ 通りあることが分かった．ここで，写像 $\{(a_0, a_1) : a_0^2 + a_1^2 = 1\} \to \mathrm{PSL}_2(q)$ は $2:1$ で写るので，$|C_{\mathrm{PSL}_2(q)}(B)| = p-1$ が成り立つ．

次に $p \equiv 3 \pmod 4$ のときについても．系 2.1.5 と命題 1.2.6 より，上と同様の議論で $|C_{\mathrm{PSL}_2(q)}(B)| = q+1$ が分かる．

$|C_{\mathrm{PGL}_2(q)}(B)|$ について考える．

$$C_{\mathrm{PGL}_2(q)}(B) = \left\{ \begin{pmatrix} a_0 & a_1 \\ -a_1 & a_0 \end{pmatrix} : a_0^2 + a_1^2 \neq 0 \right\} \cup \left\{ \begin{pmatrix} a_0 & a_1 \\ a_1 & -a_0 \end{pmatrix} : a_0^2 + a_1^2 \neq 0 \right\}$$

である．$p \equiv 1 \pmod 4$ のとき，系 2.1.4 より $a_0^2 + a_1^2 \neq 0$ を満たすものは $(q-1)^2$ 通りある．しかし今，$C_{\mathrm{PGL}_2(q)}(B)$ の行列の形は $\begin{pmatrix} a_0 & a_1 \\ -a_1 & a_0 \end{pmatrix}$ と $\begin{pmatrix} a_0 & a_1 \\ a_1 & -a_0 \end{pmatrix}$ の 2 種類の形に書ける．$a^2 + b^2$ が平方剰余と平方非剰余のどちらにもなる可能性がある．また，写像 $\{(a_0, a_1) : a_0^2 + a_1^2 \neq 0\} \to \mathrm{PGL}_2(q)$ は $2:1$ で写る．さらに，$\mathrm{PGL}_2(q)$ 内では，スカラー倍した行列は同じ元とみなせる．以上 4 点のことから，

$$(q-1)^2 \times 2 \times 2 \div 2 \div (q-1) = 2(q-1)$$

となり，$|C_{\mathrm{PGL}_2(q)}(B)| = 2(p-1)$ が成り立つ．

次に $p \equiv 3 \pmod 4$ のとき，系 2.1.4 より $a_0^2 + a_1^2 \neq 0$ を満たすものは $q^2 - 1$ 通りある．よって上と同じ議論で $|C_{\mathrm{PGL}_2(q)}(B)| = 2(p+1)$ が分かる． □

系 2.1.9. 四元数の単数の集合 K に対し $\delta \in K - \{\pm 1\}$ とし，$\varepsilon_\delta \in H$ を δ の像とする．$C_V(\varepsilon_\delta) = \{a \in V \ : \ a\varepsilon_\delta = \varepsilon_\delta a\}$ とする．

$\left(\frac{p}{q}\right) = 1$ かつ $p \equiv 1 \pmod 4$ のとき，$|C_V(\varepsilon_\delta)| = q-1$.

$\left(\frac{p}{q}\right) = 1$ かつ $p \equiv 3 \pmod 4$ のとき，$|C_V(\varepsilon_\delta)| = q+1$.

$\left(\frac{p}{q}\right) = -1$ かつ $p \equiv 1 \pmod 4$ のとき，$|C_V(\varepsilon_\delta)| = 2(q-1)$.

$\left(\frac{p}{q}\right) = -1$ かつ $p \equiv 3 \pmod 4$ のとき，$|C_V(\varepsilon_\delta)| = 2(q+1)$.

次のような集合 W を考える;

$$W = \{(c_1, c_2, c_3) \in \mathbb{F}_q^3 \ : \ \left(\frac{c_1^2 + c_2^2 + c_3^2}{q}\right) = 1\}. \tag{3}$$

補題 2.1.10. 四元数の単数の集合 K に対し $\delta \in K - \{\pm 1\}$ とし，$\varepsilon_\delta \in H$ を δ の像とする．このとき，

$$\{c_1 i + c_2 j + c_3 k \ : \ (c_1, c_2, c_3) \in W\}/Z_q = \{y \in \Omega/\Omega(q) \ : \ y \text{ は } \varepsilon_\delta \text{ と共役な元 }\}$$

である．

証明．四元数の ± 1 でない単数の像は互いに共役なので，どれか1つについて示せば，全ての ± 1 でない単数の像で成り立つ．よって $\delta = j$ として示す．$x \in \Omega/\Omega(q)$ で $y = x^{-1}\Pi_q([j])x$ とする．x', $y' \in \Omega'$ を $\Pi_q([y']) = y, \Pi_q([x']) = x$ を満たす四元数とする．$x' = b_0 + b_1 i + b_2 j + b_3 k$ とおくと，

$$\begin{aligned}\Pi_q([y']) &= \Pi_q([\overline{x'}jx]) \\ &= \Pi_q([(2b_1b_2 + 2b_0b_3)i + (b_0^2 - b_1^2 + b_2^2 + b_3^2)j + (2b_2b_3 - 2b_1b_0)k]) \\ &\in \{c_1 i + c_2 j + c_3 k : (c_1, c_2, c_3) \in W\}/Z_q\end{aligned}$$

が成り立つ．よって，

$$\{c_1 i + c_2 j + c_3 k : (c_1, c_2, c_3) \in W\}/Z_q \supset \{y \in \Omega/\Omega(q) : y \text{ は} \varepsilon_\delta \text{と共役な元}\}$$

がいえる．ここから，集合の元の個数が等しいことが示せれば，集合が一致することが示せる．
系 2.1.9 より，

$$\begin{aligned}&\left(\frac{p}{q}\right) = 1 \text{ かつ } p \equiv 1 \pmod 4 \text{ のとき}, |C_V(\varepsilon_\delta)| = q - 1, \\ &\left(\frac{p}{q}\right) = 1 \text{ かつ } p \equiv 3 \pmod 4 \text{ のとき}, |C_V(\varepsilon_\delta)| = q + 1, \\ &\left(\frac{p}{q}\right) = -1 \text{ かつ } p \equiv 1 \pmod 4 \text{ のとき}, |C_V(\varepsilon_\delta)| = 2(q - 1), \\ &\left(\frac{p}{q}\right) = -1 \text{ かつ } p \equiv 3 \pmod 4 \text{ のとき}, |C_V(\varepsilon_\delta)| = 2(q + 1),\end{aligned}$$

が分かっている．$|V| = \begin{cases} \frac{q(q^2-1)}{2} & (\left(\frac{p}{q}\right) = 1) \\ q(q^2-1) & (\left(\frac{p}{q}\right) = -1) \end{cases}$．ゆえに，

$$|\{y \in \Omega/\Omega(q) : y \text{ は} \varepsilon_\delta \text{と共役な元}\}| = |V|/|C_V(\varepsilon_\delta)|$$

$$|\{y \in \Omega/\Omega(q) : y \text{ は} \varepsilon_\delta \text{と共役な元}\}| = \begin{cases} \frac{q(q+1)}{2} & (q \equiv 1 \pmod 4) \\ \frac{q(q-1)}{2} & (q \equiv 3 \pmod 4) \end{cases}$$

であると分かる．一方，補題 2.1.7(a) より，$q \equiv 1 \pmod 4$ のとき，

$$|\{(a, b, c) \in \mathbb{F}_q^3 : a^2 + b^2 + c^2 = w\}| = q(q + 1) \quad (\left(\frac{w}{q}\right) = 1)$$

である．平方剰余の元の数は $(q-1)/2$ 個，$|Z_q| = q - 1$ だから，

$$|\{c_1 i + c_2 j + c_3 k : (c_1, c_2, c_3) \in W\}/Z_q| = q(q + 1) \times \frac{q - 1}{2} \div (q - 1) = \frac{q(q + 1)}{2}$$

が成り立つ．また補題 2.1.7(b) より，$q \equiv 3 \pmod 4$ のとき，

$$|\{(a, b, c) \in \mathbb{F}_q^3 : a^2 + b^2 + c^2 = w\}| = q(q - 1) \quad (\left(\frac{w}{q}\right) = 1)$$

である．よって，上と同様に

$$|\{c_1 i + c_2 j + c_3 k : (c_1, c_2, c_3) \in W\}/Z_q| = q(q-1) \times \frac{q-1}{2} \div (q-1) = \frac{q(q-1)}{2}$$

が成り立つ．よって，集合の元の個数が同じであることが示せた． □

$D^{p,q}$ について次の命題を示す．

命題 2.1.11. $p^2 < q$ とする．このとき，$D^{p,q}$ は多重辺を持たない．

証明. $x, y \in \Omega/\Omega(q)$ をつなぐ多重辺があると仮定する．
$t_1 \neq t_2$ となる $t_1, t_2 \in T_{p,q}$ で，$K'xt_1 = K'y$，$K'xt_2 = K'y$，と書ける．よって，$K'xt_1 = K'xt_2$ が成り立つ．
$\varepsilon \in K'$ で $xt_1 = \varepsilon xt_2$ となるものがある．$x = \varepsilon xt_2 t_1^{-1}$ となるので，
元の式に代入すると $xt_1 = \varepsilon\varepsilon xt_2 t_1^{-1} t_2$ となり，

$$t_1 t_2^{-1} t_1 t_2^{-1} = 1$$

となって，$Y^{p,q}$ に長さ4のサーキットがあることになる．ところが，命題1.3.5より $g(Y^{p,q}) \geq 2\log_p q$ であるので $p^2 < q$ の範囲では $g(Y^{p,q}) > 4$ であり長さ4のサーキットは持たない．
よって，この範囲では多重辺を持たない． □

命題 2.1.12. $p < 2\sqrt{q}$ とする．$\left(\frac{p}{q}\right) = 1$ かつ $p \not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right) = -1$ ならば，$D^{p,q}$ はループを持たない．

証明. $K'd_0$ に対応する頂点にループがあるとする．$D^{p,q}$ はケーリーグラフだから，$K'd_0 t = K'd_0$ となる $t \in T^{p,q}$ が存在する．このとき，$\delta \in K'$ で $d_0 t = \delta d_0$ と書ける．ある $\alpha \in S_p$ で $t = \Pi([\alpha])$ となるとすると，

$$\begin{aligned} d_0 t &= \delta d_0, \\ d_0 \Pi([\alpha]) &= \delta d_0, \\ \Pi([\alpha]) &= d_0^{-1} \delta d_0 \end{aligned}$$

と変形できる．補題2.1.10より

$$\Pi([\alpha]) \in \{c_1 i + c_2 j + c_3 k \ : \ (c_1, c_2, c_3) \in W\}/Z_q$$

だから，

$$\begin{aligned} \alpha \in \{\beta = b_0 + (b_1 + c_1')i + (b_2 + c_2')j + (b_3 + c_3')k \in \Lambda' \ : \\ b_0 \equiv b_1 \equiv b_2 \equiv b_3 \pmod q\}. \end{aligned} \tag{4}$$

つまり $a_l \equiv 0 \pmod q$ $(l = 0, 1, 2, 3)$ を満たす $a_l \in \mathbb{Z}$ で $\alpha = a_0 + (a_1 + c_1')i + (a_2 + c_2')j + (a_3 + c_3')k$ と書ける．ただしここで，c_1', c_2', c_3' は $0 \leq c_1', c_2', c_3' < q$ の整数で，法 q でreductionすると c_1, c_2, c_3 になるものである．$\alpha \in S_p$ だから $N(\alpha) = p$ となる．しかし，$p < 2\sqrt{q}$ であるから，$a_l \equiv 0 \pmod q$ $(l = 0, 1, 2, 3)$ を満たす a_l は0しかない．よって，

$\alpha = c_1'i + c_2'j + c_3'k$ と書ける．つまり，${c_1'}^2 + {c_2'}^2 + {c_3'}^2 = p$ である．よって，$\left(\frac{p}{q}\right) = 1$ である．α は強奇数だから，c_1', c_2', c_3' は奇数であり，$p \equiv 3 \pmod 4$ であることが分かる．Gauss の定理により，$p \equiv 7 \pmod 8$ の時は，${c_1'}^2 + {c_2'}^2 + {c_3'}^2 = p$ と書ける c_1', c_2', c_3' は存在しないことが分かっている．また同じく，$p \equiv 3 \pmod 8$ の時は ${c_1'}^2 + {c_2'}^2 + {c_3'}^2 = p$ と書ける c_1', c_2', c_3' が存在することが分かっている．つまり，$\left(\frac{p}{q}\right) = 1$ かつ $p \equiv 3 \pmod 8$ の時のみ，この形で書ける． □

命題 2.1.13. $p^2 < q$ を満たし，$\left(\frac{p}{q}\right) = 1$ かつ $p \not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right) = -1$ とする．このとき，$g(D^{p,q}) \geq \log_p q$ である．特に $\left(\frac{p}{q}\right) = -1$ のとき，$g(D^{p,q}) \geq 2\log_p q - \log_p 2$ である．

証明. $g(D^{p,q}) = g$ とおく．$K'y_0, K'y_1, \ldots, K'y_g = K'y_0$ を $D^{p,q}$ の長さ g のサーキットの頂点に対応する元とする．$D^{p,q}$ はケーリーグラフだから，$K'y_i = K'y_0t_1t_2\ldots t_i$ $(1 \leq i \leq g)$ となるような $t_1, t_2, \ldots, t_g \in T^{p,q}$ が存在する．$K'y_0t_1t_2\ldots t_g = K'y_g = K'y_0$ より，$y_0t_1t_2\ldots t_g = \delta y_0$ となる $\delta \in K'$ が存在する．よって $\delta y_0t_1t_2\ldots t_g = y_0$ だから，$y_0t_1t_2\ldots t_gt_1t_2\ldots t_g = y_0$ がなりたつ．ここで y_0 は 1.3 節のグラフ $Y^{p,q}$ の頂点に対応する元だから，この式はグラフ $Y^{p,q}$ 上の長さ $2g$ のサーキットをあらわしている．よって，$2g \geq g(Y^{p,q})$ だから定理 1.3.5 より，$2g \geq 2\log_p q$ が成り立つ．また，同様に $\left(\frac{p}{q}\right) = -1$ のときは，$2g \geq 4\log_p q - \log_p 4$ が成り立つ． □

系 2.1.14. $p^2 < q$ とする．$\left(\frac{p}{q}\right) = 1$ かつ $p \not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right) = -1$ のとき，$|D^{p,q}| \geq \frac{\sqrt{q}}{p}$ である．特に $\left(\frac{p}{q}\right) = -1$ のとき，$|D^{p,q}| \geq \frac{q\sqrt{2}}{2p}$ である．

証明. 命題 1.1.7 より，

$$\begin{aligned} g(D^{p,q}) &\leq 2 + 2\log_p |D^{p,q}|, \\ \log_p q &\leq 2 + 2\log_p |D^{p,q}|, \\ \frac{1}{2}\log_p q - 1 &\leq \log_p |D^{p,q}|, \\ \frac{1}{2}\log_p \frac{q}{p^2} &\leq \log_p |D^{p,q}|. \end{aligned}$$

よって，$|D^{p,q}| \geq \frac{\sqrt{q}}{p}$ である．$\left(\frac{p}{q}\right) = -1$ のとき，

$$\begin{aligned} g(D^{p,q}) &\leq 2 + 2\log_p |D^{p,q}|, \\ 2\log_p q - \log_p 2 &\leq 2 + 2\log_p |D^{p,q}|, \\ \log_p q - \frac{1}{2}\log_p 2 &\leq \log_p |D^{p,q}|, \\ \frac{1}{2}\log_p \frac{q^2}{2p^2} &\leq \log_p |D^{p,q}|. \end{aligned}$$

よって，$|D^{p,q}| \geq \frac{q\sqrt{2}}{2p}$ が成り立つ． □

2.2 グラフ $Z^{p,q}$ の連結性と大きな girth

まず，前節で作ったグラフ $Z^{p,q}$ が連結グラフであることを示す．そのためにいくつかの準備をする．

定義 2.2.1. 群 G がある正規部分群 N を持ち，その N と G/N が両方ともアーベル群であるとき，群 G をメタアーベル群という．

次の命題が [1] で紹介されている．

命題 2.2.2. q を素数とする．H を $\mathrm{PSL}_2(q)$ の $|H| > 60$ を満たす真部分群とする．このとき，H はメタアーベル群である．

命題 2.2.3. 群 G で $g_1, g_2 \in G$ の交換子を $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$ と表すことにする．このとき，G がメタアーベル群であることと，全ての $g_1, g_2, g_3, g_4 \in G$ で $[[g_1, g_2], [g_3, g_4]] = 1$ であることは同値である．

また，Descartes が予想し，Dubouis によって 1911 年に証明された次の定理が，Grosswald[2] に紹介されている．

定理 2.2.4. p を

$$3, 5, 11, 17, 29, 41 \tag{5}$$

以外の奇素数とする．このとき，p は $a, b, c, d \in \mathbb{Z} - \{0\}$ で，$p = a^2 + b^2 + c^2 + d^2$ と書ける．

ここから次の系を導く．

系 2.2.5. p, q を奇素数とし，$p < q$ とする．また p は (5) 以外であるとする．$\delta \in K - \{\pm 1\}$ とし，$\varepsilon_\delta \in H$ を δ の像とする．g' を，S_p の元の中から選び，$g = (\psi \circ \varphi_q \circ \tau_q)(g')$ とすると，$g^{-1} \neq \varepsilon_\delta g \varepsilon_\delta$ が成り立つ．
特に $p \equiv 3 \pmod 4$ のとき，全ての $g \in S_{p,q}$ で $g^{-1} \neq \varepsilon_\delta g \varepsilon_\delta$ が成り立つ．

証明. $p \equiv 1 \pmod 4$ のとき，p が $a, b, c, d \in \mathbb{Z} - \{0\}$ で，$p = a^2 + b^2 + c^2 + d^2$ と書けるとする．係数 $a_l \neq 0$ $(l = 1, 2, 3, 4)$ で $g' = a_0 + a_1 i + a_2 j + a_3 k$ を $(\psi \circ \varphi_q \circ \tau_q)(g') = g$ となる S_p の元とする．$g^{-1} \neq \varepsilon_\delta g \varepsilon_\delta$ と $\tau_q(\overline{g'}) \neq \tau_q(\pm \delta g' \delta)$ は同値であるので，$\tau_q(\overline{g'}) \neq \tau_q(\pm \delta g' \delta)$ を示す．

$$ig'i = i(a_0 + a_1 i + a_2 j + a_3 k)i \quad = (a_0 i - a_1 + a_2 k - a_3 j)i = -a_0 - a_1 i + a_2 j + a_3 k.$$

$\tau_q(\overline{g'}) = \tau_q(\pm \delta g' \delta)$ が成り立つとして矛盾を導く．$\tau_q(\overline{g'}) = \tau_q(\delta g' \delta)$ であるとすると，$p < q$ より，$a_0 = 0$ かつ $a_2 = 0$ かつ $a_3 = 0$ を満たす必要がある．また，$\tau_q(\overline{g'}) \neq \tau_q(-\delta g' \delta)$ であるとすると，$a_1 = 0$ を満たす必要がある．前者の場合は $g' \in S_p$ に矛盾する．後者については，$p \equiv 3 \pmod 4$ のとき，a_0 が偶数で a_1, a_2, a_3 は奇数だから，矛盾する．$p \equiv 1 \pmod 4$ のとき，g' を，係数 $a_l \neq 0$ $(l = 1, 2, 3, 4)$ で $g'_1 = a_0 + a_1 i + a_2 j + a_3 k$ と書ける S_p の元の中から選んでいることに矛盾する． □

これらの命題と定理を用いて，次の定理を証明する．

定理 2.2.6. p, q を $p \geq 5$, $q > p^7$ を満たす奇素数であるとする．ただし，q が $p^7 < q \leq p^8$ のときは，p は (5) 以外であるとする．このとき，$Z^{p,q}$ は連結グラフで $D^{p,q}$ と同型なグラフである．

証明. $\left(\frac{p}{q}\right) = 1$ のとき $V = \mathrm{PSL}_2(q)$, $\left(\frac{p}{q}\right) = -1$ のとき $V = \mathrm{PGL}_2(q)$ とする．$p^8 < q$ のとき，定理 1.3.6 より $X^{p,q}$ が連結だから $Z^{p,q}$ は連結である．よって $p^7 < q \leq p^8$ のときを示す．$D^{p,q}$ は連結グラフだから，命題 2.1.3 より $\Omega/\Omega(q) = K'\langle T_{p,q}\rangle$ が成り立つ．だから，$\beta(\Omega/\Omega(q)) = \beta(K'\langle T^{p,q}\rangle) = H\langle S_{p,q}\rangle$ である．$Z^{p,q}$ が連結であることを示すために $H\langle S_{p,q}\rangle = V$ を示したい．$B_{p,q} = \mathrm{PSL}_2(q) \cap \beta(\Omega/\Omega(q))$ とおく．$B_{p,q} = \mathrm{PSL}_2(q)$ であることと，$H\langle S_{p,q}\rangle = V$ であることは同値である．よって，$B_{p,q} = \mathrm{PSL}_2(q)$ を示す．命題 2.2.2 より，$|B_{p,q}| > 60$ で $B_{p,q}$ がメタアーベル群でなければ良い．系 2.1.14 より，

$$|G_q| = \frac{1}{4}|\Omega/\Omega(q)| \geq \frac{\sqrt{q}}{p} \geq \frac{\sqrt{p^7}}{p} = p^2\sqrt{p} > 30.$$

つまり，$|\Omega/\Omega(q)| > 120$ だから，$|\beta(\Omega/\Omega(q))| > 120$ となり $|B_{p,q}| > 60$ が分かる．命題 2.2.3 より，$g_1, g_2, g_3, g_4 \in B_{p,q}$ で $[[g_1, g_2], [g_3, g_4]] \neq 1$ となるものがあることを示す．
$\left(\frac{p}{q}\right) = 1$ のとき，$H\langle S_{p,q}\rangle$ の元から次のように g_i $(i = 1, 2, 3, 4)$ を選ぶ．g_1' を，係数 $a_l \neq 0$ $(l = 1, 2, 3, 4)$ で $g_1' = a_0 + a_1 i + a_2 j + a_3 k$ と書ける S_p の元の中から選ぶ．$g_1 = (\psi \circ \varphi_q \circ \tau_q)(g_1')$ とする．$\varepsilon_\delta \in H$ を四元数の単数 δ の像として，g_2, g_3, g_4 を次のようにとる．

$$g_2 = \varepsilon_i g_1,\ g_3 = \varepsilon_j g_1,\ g_4 = g_1.$$

この選び方で，

$$\begin{aligned}[[g_1, g_2], [g_3, g_4]] &= [[g_1, \varepsilon_i g_1], [\varepsilon_j g_1, g_1]] \\ &= g_1\varepsilon_i g_1 g_1^{-1} g_1^{-1}\varepsilon_i\varepsilon_j g_1 g_1 g_1^{-1}\varepsilon_j g_1^{-1}\varepsilon_i g_1 g_1 g_1^{-1}\varepsilon_i g_1^{-1} g_1\varepsilon_j g_1 g_1^{-1} g_1^{-1}\varepsilon_j \\ &= g_1\varepsilon_i g_1^{-1}\varepsilon_i\varepsilon_j g_1\varepsilon_j g_1^{-1}\varepsilon_i g_1\varepsilon_i\varepsilon_j g_1^{-1}\varepsilon_j\end{aligned}$$

ここで，系 2.2.5 より $\varepsilon_i g_1^{-1}\varepsilon_i \in S_{p,q}$, $\varepsilon_j g_1^{-1}\varepsilon_j \in S_{p,q}$ で，$\varepsilon_i g_1^{-1}\varepsilon_i \neq g_1^{-1}$, $\varepsilon_j g_1^{-1}\varepsilon_j \neq g_1^{-1}$ だからこの交換子は $S_{p,q}$ 上の長さ 6 の既約ワードであると分かる．しかし命題 2.1.13 より，$g(D^{p,q}) \geq \log_p(q) > \log_p p^7 = 7$ だから，$D^{p,q}$ のサーキットは 7 より大きい．つまり，$[[g_1, g_2], [g_3, g_4]] \neq 1$.
$\left(\frac{p}{q}\right) = -1$ のとき，h を 0 でない係数 a_i $(i = 1, 2, 3, 4)$ で $h = a_0 + a_1 i + a_2 j + a_3 k$ と書ける S_p の元の中から選ぶ．$\varepsilon_\delta \in H$ を四元数の単数 δ の像として，g_1, g_2, g_3, g_4 を次のようにとる．

$$g_1 = h^2,\ g_2 = g_3 = \varepsilon_i h^2,\ g_4 = \varepsilon_j h^2.$$

この選び方で，

$$\begin{aligned}[[g_1,g_2],[g_3,g_4]] =&[[g_1,\varepsilon_i g_1],[\varepsilon_j g_1,g_1]]\\ =&hh\varepsilon_i hhh^{-1}h^{-1}h^{-1}h^{-1}\varepsilon_i\varepsilon_i hh\varepsilon_j hhh^{-1}h^{-1}\varepsilon_i h^{-1}h^{-1}\varepsilon_j\varepsilon_i\\ &\times hhhhh^{-1}h^{-1}\varepsilon_i h^{-1}h^{-1}\varepsilon_j hh\varepsilon_i hhh^{-1}h^{-1}\varepsilon_j h^{-1}h^{-1}\varepsilon_i\\ =&hh\varepsilon_i\varepsilon_j\varepsilon_i h^{-1}h^{-1}\varepsilon_j\varepsilon_i hh\varepsilon_i h^{-1}h^{-1}\varepsilon_j hh\varepsilon_i\varepsilon_j h^{-1}h^{-1}\varepsilon_i\\ =&hh\varepsilon_j h^{-1}\varepsilon_j\varepsilon_j h^{-1}\varepsilon_j\varepsilon_i h\varepsilon_i\varepsilon_i h\varepsilon_i h^{-1}h^{-1}\varepsilon_j h\varepsilon_j\varepsilon_j h\varepsilon_j\varepsilon_i h^{-1}\varepsilon_i\varepsilon_i h^{-1}\varepsilon_i\end{aligned}$$

ここで，この交換子は $\left(\frac{p}{q}\right)=1$ のときと同様で，$S_{p,q}$ 上の長さ 12 の既約ワードであると分かる．しかし命題 2.1.13 より，$g(D^{p,q})\geq 2\log_p(q)-\log_p 2\geq 14-\log_p 2>13$ だから，$D^{p,q}$ のサーキットは 13 より大きい．つまり，$[[g_1,g_2],[g_3,g_4]]\neq 1$.
よって，$Z^{p,q}$ が連結グラフであることが示せて，$Z^{p,q}$ と $D^{p,q}$ は同型である． □

命題 2.1.3，2.1.11 より，次の系がすぐ分かる．

系 2.2.7. p,q を $p\geq 5$，$q>p^7$ を満たす奇素数であるとする．ただし，q が $p^7<q\leq p^8$ のときは，p は (5) 以外であるとする．このとき，$Z^{p,q}$ は多重辺を持たない．

命題 2.1.12 より次の系が成り立つことも分かる．

系 2.2.8. p,q を $p\geq 5$，$q>p^7$ を満たす奇素数であるとする．ただし，q が $p^7<q\leq p^8$ のときは，p は (5) 以外であるとする．このとき，$\left(\frac{p}{q}\right)=1$ かつ $p\not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right)=-1$ ならば，$Z^{p,q}$ はループを持たない．

これらの系と命題 2.1.13 より，$Z^{p,q}$ の girth について以下の評価ができることがすぐに分かる．

系 2.2.9. p,q を $p\geq 7$，$q>p^7$ を満たす奇素数であるとする．ただし，q が $p^7<q\leq p^8$ のときは，p は (5) 以外であるとする．$\left(\frac{p}{q}\right)=1$ かつ $p\not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right)=-1$ を満たすとする．このとき $g(Z^{p,q})\geq\log_p q$ である．特に $\left(\frac{p}{q}\right)=-1$ のとき，$g(Z^{p,q})\geq 2\log_p q-\log_p 2$ である．

また，これから，次の系も証明できる．

系 2.2.10. p,q を $p\geq 5$，$q>p^7$ を満たす奇素数であるとする．ただし，q が $p^7<q\leq p^8$ のときは，p は (5) 以外であるとする．$\left(\frac{p}{q}\right)=1$ かつ $p\not\equiv 3 \pmod 8$ のとき，$g(Z^{p,q})\geq\frac{1}{3}\log_p 8|Z^{p,q}|$ である．特に $\left(\frac{p}{q}\right)=-1$ のとき，$g(Z^{p,q})\geq\frac{2}{3}\log_p|Z^{p,q}|+\frac{1}{3}\log_p 2$ である．

証明. $\left(\frac{p}{q}\right)=1$ のとき，$|Z^{p,q}|=\frac{|\mathrm{PSL}_2(q)|}{4}=\frac{q(q^2-1)}{8}\leq\frac{q^3}{8}$ だから，$q^3\geq 8|Z^{p,q}|$．系 2.2.9 より，

$$g(Z^{p,q})\geq\log_p q=\frac{1}{3}\log_p q^3\geq\frac{1}{3}\log 8|Z^{p,q}|.$$

$\left(\frac{p}{q}\right) = -1$ のとき，$|Z^{p,q}| = \frac{|\mathrm{PGL}_2(q)|}{4} = \frac{q(q^2-1)}{4} \leq \frac{q^3}{4}$ だから，$q^3 \geq 4|Z^{p,q}|$．系 2.2.9 より，

$$\begin{aligned} g(Z^{p,q}) &\geq 2\log_p q - \log_p 2 \\ &= \frac{2}{3}\log_p q^3 - \log_p 2 \\ &\geq \frac{2}{3}\log_p 4|Z^{p,q}| - \log_p 2 \\ &= \frac{2}{3}\log_p |Z^{p,q}| + \frac{1}{3}\log_p 2. \end{aligned}$$

□

このことから，p, q が上の系の仮定を満たすときは，$Z^{p,q}$ は大きな girth を持つということが分かった．

3 頂点推移的でないラマヌジャングラフ

3.1 頂点推移的でない family of expanders と良いグラフ

この章では奇素数 p を固定して考える．q は奇素数とする．また $\left(\frac{p}{q}\right)=1$ のとき $V=\mathrm{PSL}_2(q)$，$\left(\frac{p}{q}\right)=-1$ のとき $V=\mathrm{PGL}_2(q)$ とする．$Z^{p,q}$ の頂点数を n とする．その隣接行列の固有値を

$$\mu_0=p+1\geq\mu_1\geq\mu_2\geq\ldots\geq\mu_{n-1}$$

とする．$f_{l,x,y}$ を $X^{p,q}$ の頂点 x から y への，引き返しのない長さ l の道の数とする．$X^{p,q}$ は頂点推移的なグラフなので，特に $x=y$ のとき f_l と書くことにする．$\mathfrak{f}_{m,x}$ を $Z^{p,q}$ の頂点 x から始まり，x で終わる引き返しのない長さ m の道の数とする．定理 1.3.7 より，各 $m\in\mathbb{N}\cup\{0\}$ で

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

が成り立つ．

1.3 節にあるようなトレース公式を，$Z^{p,q}$ について考える．そのためにまず，1.3 節の二次形式に加えて，新たに次のような二次形式を導入する．

$(c_1,c_2,c_3)\in W$ に対し

$$\mathcal{Q}_{(c_1,c_2,c_3)}(x_0,x_1,x_2,x_3)=x_0^2+(x_1+c_1')^2+(x_2+c_2')^2+(x_3+c_3')^2.$$

ただしここで，W は式 (3) で定義されたもので，c_1',c_2',c_3' は $0\leq c_1',c_2',c_3'<q$ の整数で，法 q で reduction すると c_1,c_2,c_3 になるものである．さらに次の二次形式も導入する．

$$\mathcal{Q}_2(x_0,x_1,x_2,x_3)=q^2x_0^2+4(x_1^2+x_2^2+x_3^2).$$

また，$m\geq 0$ に対し次のようにおく．

$$\begin{aligned}s_{\mathcal{Q}_{(c_1,c_2,c_3)}}(p^m)=&|\{(x_0,x_1,x_2,x_3)\in\mathbb{Z}^4\ :\mathcal{Q}_{(c_1,c_2,c_3)}(x_0,x_1,x_2,x_3)=p^m,\\&\qquad x_0\equiv x_1\equiv x_2\equiv x_3\equiv 0\pmod q,\\&\qquad (x_0,x_1+c_1',x_2+c_2',x_3+c_3')\text{ は強奇数を作る組 }\}|.\\ s_{\mathcal{Q}_2}(p^m)=&|\{(x_0,x_1,x_2,x_3)\in\mathbb{Z}^4:\ \mathcal{Q}_2(x_0,x_1,x_2,x_3)=p^m\}|.\end{aligned}$$

このとき，次の命題が成り立つ．

命題 3.1.1. m が偶数のとき、$s_{\mathcal{Q}_2}(p^m)=\sum_{(c_1,c_2,c_3)\in W}s_{\mathcal{Q}_{(c_1,c_2,c_3)}}(p^m)$ である．

証明. c_1',c_2',c_3' は $0\leq c_1',c_2',c_3'<q$ の整数で，法 q で reduction すると c_1,c_2,c_3 になるものであるとする．

$$\begin{aligned}\sum_{(c_1,c_2,c_3)\in W}s_{\mathcal{Q}_{(c_1,c_2,c_3)}}(p^m)=\sum_{(c_1,c_2,c_3)\in W}&|\{(x_0,x_1,x_2,x_3)\in\mathbb{Z}^4\ :\mathcal{Q}_{(c_1,c_2,c_3)}(x_0,x_1,x_2,x_3)=p^m,\\&\qquad x_0\equiv x_1\equiv x_2\equiv x_3\equiv 0\pmod q,\\&\qquad (x_0,x_1+c_1',x_2+c_2',x_3+c_3')\text{ は強奇数を作る組 }\}|\end{aligned}$$

の右辺に関して，今，m が偶数であるから，$(c_1,c_2,c_3)\in\mathbb{F}_q^3-W$ でこの集合を満たすものは存在しない．よって，

$$\begin{aligned}\sum_{(c_1,c_2,c_3)\in W} s_{\mathcal{Q}_{(c_1,c_2,c_3)}}(p^m) &= \sum_{(c_1,c_2,c_3)\in\mathbb{F}_q^3} |\{(x_0,x_1,x_2,x_3)\in\mathbb{Z}^4 \ : \mathcal{Q}_{(c_1,c_2,c_3)}(x_0,x_1,x_2,x_3)=p^m,\\ &\qquad x_0\equiv x_1\equiv x_2\equiv x_3\equiv 0 \pmod q,\\ &\qquad (x_0,x_1+c_1',x_2+c_2',x_3+c_3') \text{ は強奇数を作る組 }\}|\\ &= |\{(x_0,x_1,x_2,x_3)\in\mathbb{Z}^4 : x_0^2+4(x_1^2+x_2^2+x_3^2)=p^m,\ x_0\equiv 0 \pmod q\}|\\ &= |\{(x_0,x_1,x_2,x_3)\in\mathbb{Z}^4 : q^2x_0^2+4(x_1^2+x_2^2+x_3^2)=p^m\}|\\ &= s_{\mathcal{Q}_2}(p^m).\end{aligned}$$

□

定理 3.1.2 ($Z^{p,q}$ **のトレース公式**). $|H\backslash V|=n$ とおき，p,q を $p\geq 5$, $p^8<q$ を満たす奇素数とする．$\left(\frac{p}{q}\right)=1$ かつ $p\not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right)=-1$ を満たすとする．

$$c_V=\begin{cases} q-1 & (\left(\frac{p}{q}\right)=1 \text{ かつ } p\equiv 1 \pmod 4 \text{ のとき})\\ q+1 & (\left(\frac{p}{q}\right)=1 \text{ かつ } p\equiv 3 \pmod 4 \text{ のとき})\\ 2(q-1) & (\left(\frac{p}{q}\right)=-1 \text{ かつ } p\equiv 1 \pmod 4 \text{ のとき})\\ 2(q+1) & (\left(\frac{p}{q}\right)=-1 \text{ かつ } p\equiv 3 \pmod 4 \text{ のとき})\end{cases}$$

とおく．全ての $m\in\mathbb{N}\cup\{0\}$ に対し

$$\sum_{x\in H\backslash V}\sum_{0\leq r\leq m/2} \mathfrak{f}_{m-2r,x}=\frac{n}{2}s_{\mathcal{Q}_1}(p^m)+\frac{3}{8}c_V s_{\mathcal{Q}_2}(p^m).$$

証明. 定理 2.2.6 より，$Z^{p,q}$ と $D^{p,q}$ は同型なグラフなので，同一視して考える．
$K'd_0, K'd_1,\dots, K'd_l$ を $D^{p,q}$ の $K'd_0$ から始まり，$K'd_l$ で終わる，引き返しのない長さ l の道の頂点に対応する $K'\backslash\mathbb{H}(\mathbb{F}_q)^\times/Z_q$ の元とする．命題2.1.13より，$K'd_h=K't_0t_1\dots t_h$ $(h=1,2,\dots,l)$ となる $t_1,t_2,\dots,t_l\in T^{p,q}$ が存在する．ある $\alpha_h\in S_p$ $(h=1,2,\dots,l)$ で，$t_h=\Pi_q([\alpha_h])$ となるとすると，引き返しがない道だから，$[\alpha_1][\alpha_2]\dots[\alpha_l]$ は Ω 内の長さ l の既約ワードである．$K'd_0$ から始まり長さ l の道で $K'd_0$ にもどるとする．このとき，$K'd_0t_1t_2\dots t_l=K'd_0$ だから，$\delta\in K'$ で $d_0t_1t_2\dots t_l=\delta d_0$ と書ける．
case 1 : $\delta=(\rho\circ\Pi_q\circ\mathcal{F})(\pm 1)$ のとき．
上の式は $X^{p,q}$ の d_0 に対応する頂点から d_0 に対応する頂点への長さ l の道をあらわす．$X^{p,q}$ 内のある頂点から同じ頂点に戻る，長さ l の道の総数は $4nf_l$ である．$Z^{p,q}$ の 1 つの頂点に対応する $X^{p,q}$ の頂点は 4 つあるので，$Z^{p,q}$ のある頂点から同じ頂点に戻る長さ l の道の数は，nf_l である．
case 2 : $\delta\neq(\rho\circ\Pi_q\circ\mathcal{F})(\pm 1)$ のとき．

$$\begin{aligned} d_0t_1t_2\dots t_l &= \delta d_0,\\ d_0\Pi_q([\alpha_1][\alpha_2]\dots[\alpha_l]) &= \delta d_0,\\ \Pi_q([\alpha_1][\alpha_2]\dots[\alpha_l]) &= d_0^{-1}\delta d_0.\end{aligned}$$

$\gamma \in \Lambda'$ で $\Pi_q([\gamma]) = d_0^{-1}\delta d_0$ とおくと，$[\alpha_1][\alpha_2]\dots[\alpha_l] \in [\gamma]\Lambda(q)$ である．この時，補題 2.1.10 より

$$\Pi([\gamma]) \in \{c_1 i + c_2 j + c_3 k \ : \ (c_1, c_2, c_3) \in W\}/Z_q$$

だから，

$$\gamma \in \{\beta = b_0 + (b_1 + c_1')i + (b_2 + c_2')j + (b_3 + c_3')k \in \Lambda' \ : \\ b_0 \equiv b_1 \equiv b_2 \equiv b_3 \pmod q\}.$$

ただし，ここで，c_1', c_2', c_3' は $0 \le c_1', c_2', c_3' < q$ の整数で，法 q で reduction すると c_1, c_2, c_3 になるものである．ここで，ある $x^{-1}\delta x$ に対して $(c_{1x}, c_{2x}, c_{3x}) \in W$ が決まる．$a_0 \equiv a_1 \equiv a_2 \equiv a_3 \pmod q$ となる a_0, a_1, a_2, a_3 で，$N(\alpha) = p^m$ となる $\alpha = a_0 + (a_1 + c_{1x})i + (a_2 + c_{2x})j + (a_3 + c_{3x})k \in \Lambda'$ を考える．α はある l に対して，S_p の長さ $m - 2r$ の既約ワード w_{m-2r} で $\alpha = \pm p^l w_{m-2r}$ と因数分解できる．このとき，$[\alpha] = [w_{m-2r}] \in [\gamma]\Lambda(q)$ である．逆に $[\gamma]\Lambda(q)$ 内の長さ $m - 2r$ の既約ワード w を考えると，$\alpha = \pm p^l w$ の 2 つの四元数ができる．よって，

$$|\{\alpha \in \Lambda' \ : \ N(\alpha) = p^m \ , \ [\alpha] \in [\gamma]\Lambda(q)\}| = 2 \sum_{0 \le r \le m/2} f_{m-2r,x,\delta x}.$$

次に，ある $(c_1, c_2, c_3) \in W$ に対して，$\mathcal{Q}_{(c_1,c_2,c_3)}(x_0, x_1, x_2, x_3) = p^m$ かつ，$x_0 \equiv x_1 \equiv x_2 \equiv x_3 \pmod q$ を満たすもので，$(x_0, x_1 + c_1', x_2 + c_2', x_3 + c_3')$ が強奇数を作る組になるような $(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$ をとる．ただしここで，c_1', c_2', c_3' は $0 \le c_1', c_2', c_3' < q$ の整数で，法 q で reduction すると c_1, c_2, c_3 になるものである．四元数 α' を $\alpha' = x_0 + (x_1 + c_1')i + (x_2 + c_2')j + (x_3 + c_3')k$ とすると，この α' は Λ' の元で，この同値類は $[\gamma]\Lambda(q)$ に属する．だから，$(c_1, c_2, c_3) \in W$ に対し

$$s_{\mathcal{Q}_{(c_1,c_2,c_3)}}(p^m) = |\{\alpha = x_0 + (x_1 + c_1')i + (x_2 + c_2')j + (x_3 + c_3')k \in \Lambda' \ : \\ N(\alpha) = p^m \ , \ x_0 \equiv x_1 \equiv x_2 \equiv x_3 \pmod q\}|.$$

よって，$s_{\mathcal{Q}_{(c_1,c_2,c_3)}}(p^m) = 2\sum_{0 \le r \le m/2} f_{m-2r,x,\delta x}$ が成り立つ．ゆえに，

$$\begin{aligned}
\sum_{x \in H\backslash V} \sum_{0 \le r \le m/2} \mathfrak{f}_{m-2r,x} &= n \sum_{0 \le r \le m/2} f_{m-2r} + \frac{1}{4} \sum_{\delta \ne (\rho \circ \Pi_q \circ \mathcal{F})(\pm 1)} \sum_{x \in V} \sum_{0 \le r \le m/2} f_{m-2r,x,\delta x} \\
&= \frac{n}{2} s_{\mathcal{Q}_1}(p^m) + \frac{1}{4} \cdot \frac{1}{2} \sum_{\delta \ne (\rho \circ \Pi_q \circ \mathcal{F})(\pm 1)} \sum_{x \in V} s_{\mathcal{Q}_{c_{1x},c_{2x},c_{3x}}}(p^m) \\
&= \frac{n}{2} s_{\mathcal{Q}_1}(p^m) + \frac{1}{8} \sum_{\delta \ne (\rho \circ \Pi_q \circ \mathcal{F})(\pm 1)} c_V \sum_{(c_1,c_2,c_3) \in W} \mathcal{Q}_{c_1,c_2,c_3}(p^m) \\
&= \frac{n}{2} s_{\mathcal{Q}_1}(p^m) + \frac{3}{8} c_V s_{\mathcal{Q}_2}(p^m).
\end{aligned}$$

□

定理 1.3.7 より，U_m を m 次のチェビシェフ多項式とすると，

$$Z^{p,q}\text{のトレース公式の左辺} = p^{m/2} \sum_{j=0}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{p}}\right)$$

となる．ここで，複素数の集合 $\mathbb{C}$ の部分集合 $\Theta_p = [i\log\sqrt{p}, 0] \cup [0, \pi] \cup [\pi, \pi + i\log\sqrt{p}]$ を導入する．Θ_p から $[-(p+1), p+1]$ への写像を $z \to 2\sqrt{p}\cos z$ で定義すると 1 対 1 対応となる．$j = 0, 1, \ldots, n-1$ に対し $\theta_j \in \Theta_p$ を $\mu_j = 2\sqrt{p}\cos\theta_j$ となる唯一の元とする．特に，$\theta_0 = i\log\sqrt{p}$ である．また，$\left(\frac{p}{q}\right) = -1$ のときは，命題 2.1.3(d) より $Z^{p,q}$ は二部グラフだから，$\theta_{n-1} = \pi + i\log\sqrt{p}$ である．
チェビシェフ多項式 U_m の定義より，

$$\begin{aligned}\sum_{x\in H\backslash V}\sum_{0\le r\le m/2} \mathfrak{f}_{m-2r,x} &= p^{m/2}\sum_{j=0}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{p}}\right)\\ &= p^{m/2}\sum_{j=0}^{n-1} U_m(\cos\theta_j)\\ &= p^{m/2}\sum_{j=0}^{n-1}\frac{\sin(m+1)\theta_j}{\sin\theta_j} \qquad (6)\end{aligned}$$

となる．$Z^{p,q}$ がラマヌジャングラフであるためには，全ての非自明な固有値 μ で $|\mu| \le 2\sqrt{p}$ を満たさなくてはならない．つまり，$\left(\frac{p}{q}\right) = 1$ のときは $j \ne 0$，$\left(\frac{p}{q}\right) = -1$ のときは $j \ne 0, n-1$ で θ_j は実数かつ $\theta_j \in [0, \pi]$ を満たすことを示せばよい．しかしラマヌジャングラフであることの証明は次節においておいて，ここではまず，ある条件の p, q に対する $Z^{p,q}$ の族が family of expanders であることを先に示す．

補題 3.1.3. q を奇素数とする．a, b を q で割り切れない整数とする．このとき，$a^2 \equiv b^2 \pmod{q^2}$ ならば，$a \equiv \pm b \pmod{q^2}$ である．

証明. $a \not\equiv \pm b \pmod{q^2}$ として，対偶を示す．
$a = q^2a_1 + a_2$, $b = q^2b_1 + b_2$ とおく．ここで，a_1, b_1 はそれぞれ a, b を q^2 で割った商，a_2, b_2 はそのときの余りである．よって，$0 < a_2, b_2 < q^2$ で，仮定より a_2, b_2 は q の倍数ではなく，$a_2 \ne b_2$ かつ $a_2 \ne q^2 - b_2$ とする．このとき，

$$\begin{aligned}a^2 - b^2 &= (q^2a_1 + a_2)^2 - (q^2b_1 + b_2)^2\\ &= q^4(a_1^2 - b_1^2) + 2q^2(a_1a_2 - b_1b_2) + (a_2^2 - b_2^2)\end{aligned}$$

が成り立つ．ここで，$q^4(a_1^2 - b_1^2) + 2q^2(a_1a_2 - b_1b_2) \equiv 0 \pmod{q^2}$ だから，$k \in \mathbb{N}\cup\{0\}$ で $a_2^2 - b_2^2 = q^2k$ として矛盾を導く．左辺を因数分解すると，$a_2^2 - b_2^2 = (a_2 + b_2)(a_2 - b_2)$ となる．ここで仮定より，$a_2 \not\equiv b_2 \pmod{q^2}$ だから $a_2 - b_2 \ne 0, q^2$ であり $a_2 - b_2 \not\equiv 0 \pmod{q^2}$ である．さらに，$a_2 \ne q^2 - b_2$ だから $a_2 + b_2 \ne q^2$ であり，$a_2 + b_2 \equiv 0 \pmod{q^2}$ である．. q は奇素数なので，$a_2^2 - b_2^2 = q^2x$ になるには，$x_1x_2 = x$ を満たす自然数 x_1, x_2 で $a_2 + b_2 = qx_1$ かつ $a_2 - b_2 = qx_2$ でなければならない．しかし，このとき，a_2, b_2 が q の倍数となるので a, b が q で割り切れないことに矛盾する．よって，$a_2^2 - b_2^2 \ne q^2x$ だから，$a^2 - b^2 \not\equiv 0 \pmod{p^2}$ が成り立つので，対偶が示せた． □

次の命題はよく知られている．

命題 3.1.4. $|\mu|$ を $Z^{p,q}$ の非自明な固有値とする．その重複度を $M(\mu)$ とすると，$M(\mu) \ge (q-1)/2$ である．

今，$p \geq 5$, $p^8 < q$ を満たす奇素数 p, q について考える．有限で連結な，ループのないグラフ $Z^{p,q}$ が無限に存在することを確認する．
命題 2.2.8 より $\left(\frac{p}{q}\right) = 1$ かつ $p \not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right) = -1$ ならばループはないので，上の条件を満たす．つまり，$\left(\frac{p}{q}\right) = -1$ であれば無限に存在することはすぐ分かる．Dirichlet の算術級数定理より，$\left(\frac{p}{q}\right) = 1$ で $p^8 < q$ かつ $p \not\equiv 3 \pmod 8$ を満たす奇素数 q は無限に存在することも分かる．よって，$\left(\frac{p}{q}\right) = 1$ の時も，有限で連結な，ループがないグラフ $Z^{p,q}$ は無限に存在する．

定理 3.1.5. p, q を $p \geq 5, p^8 < q$ を満たす奇素数とする．また，$\left(\frac{p}{q}\right) = 1$ かつ $p \not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right) = -1$ も満たすとする．ε を $0 < \varepsilon < 1/6$ を満たす実数とする．十分大きな q に対して，$Z^{p,q}$ の全ての非自明な固有値 μ は $|\mu| \leq p^{5/6+\varepsilon} + p^{1/6-\varepsilon}$ を満たす．このときの $Z^{p,q}$ の族は family of expanders である．

証明. $\mu_j \in [-2\sqrt{p}, 2\sqrt{p}]$ のときは定理の不等式を満たしているので，$\mu_j \notin [-2\sqrt{p}, 2\sqrt{p}]$ のときについて考えれば良い．
$\mu_j \notin [-2\sqrt{p}, 2\sqrt{p}]$ のとき，$0 < \Psi_j < \log p$ を満たす $\Psi_j \in \mathbb{R}$ で

$$\theta_j = \begin{cases} i\Psi_j & (2\sqrt{p} < \mu_j \leq p+1 : \text{case 1}) \\ \pi + i\Psi_j & (-(p+1) \leq \mu_j < -2\sqrt{p} : \text{case 2}) \end{cases}$$

と表すことができる．
m を偶数とする．$\mu_j \notin [-2\sqrt{p}, 2\sqrt{p}]$ のとき，m が偶数であるから，case 1 のときも case 2 のときも

$$\frac{\sin(m+1)\theta_j}{\sin\theta_j} = \frac{\sinh(m+1)\Psi_j}{\sinh\Psi_j} \geq 0$$

が成り立つ．今，ある非自明な固有値 $\mu_k \notin [-2\sqrt{p}, 2\sqrt{p}]$ を固定する．このとき，$\sin(m+1)\theta_j / \sin\theta_j \geq 0$ より

$$\begin{aligned} &\frac{n}{2} s_{\mathcal{Q}_1}(p^m) + \frac{3}{8} c_V s_{\mathcal{Q}_2}(p^m) \\ &= p^{m/2} M(\mu_k) \frac{\sinh(m+1)\Psi_j}{\sinh\Psi_j} + p^{m/2} \sum_{\mu_j \neq \mu_k} \frac{\sin(m+1)\theta_j}{\sin\theta_j} \\ &\geq p^{m/2} M(\mu_k) \frac{\sinh(m+1)\Psi_j}{\sinh\Psi_j} + p^{m/2} \sum_{|\mu_j| < 2\sqrt{p}} \frac{\sin(m+1)\theta_j}{\sin\theta_j} \end{aligned}$$

が成り立つ．θ が実数のときは $|\sin(m+1)\theta / \sin\theta| \leq m+1$ が成り立つので

$$\begin{aligned} &\frac{n}{2} s_{\mathcal{Q}_1}(p^m) + \frac{3}{8} c_V s_{\mathcal{Q}_2}(p^m) \\ &= p^{m/2} M(\mu_k) \frac{\sinh(m+1)\Psi_j}{\sinh\Psi_j} + p^{m/2} \times n \times (-(m+1)) \\ &\geq p^{m/2} M(\mu_k) \frac{\sinh(m+1)\Psi_j}{\sinh\Psi_j} - np^{m/2}(m+1). \end{aligned} \tag{7}$$

m が偶数だから，$s_{\mathcal{Q}_1}(p^m)$ は

$$x_0^2 + 4q^2(x_1^2 + x_2^2 + x_3^2) = p^m \tag{8}$$

の整数解の個数である．まず，x_0 のとり方から考えると，$|x_0| \leq p^{m/2}$ かつ $x_0^2 \equiv p^m \pmod{q^2}$ を満たす．よって補題 3.1.3 より $x_0 \equiv \pm p^{m/2} \pmod{q^2}$ である．ここで x_0 と p はどちらも奇数だから，$x_0 \equiv \pm p^{m/2} \pmod{2q^2}$ といえる．ここから，x_0 に当てはまるものが，多くて $2(p^{m/2}/q^2 + 1)$ 通りであることが分かる．x_0 を固定して，式 (8) を解くと，

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

となる．命題 1.2.1 より任意の $\varepsilon > 0$ に対して

$$r_3\left(\frac{p^m - x_0^2}{4q^2}\right) = O_\varepsilon\left(\left(\frac{p^m}{q^2}\right)^{1/2+\varepsilon}\right)$$

が成り立つ．よって，

$$\begin{aligned} s_{\mathcal{Q}_1}(p^m) &= O_\varepsilon\left[\frac{p^{m/2+\varepsilon m}}{q^{1+2\varepsilon}}\left(\frac{p^{m/2}}{q^2} + 1\right)\right] \\ &= O_\varepsilon\left[\frac{p^{m+\varepsilon m}}{q^{3+2\varepsilon}} + \frac{p^{m/2+\varepsilon m}}{q^{1+2\varepsilon}}\right] \\ &= O_\varepsilon\left[\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{m/2(1+2\varepsilon)}}{q}\right]. \end{aligned}$$

同様に $s_{\mathcal{Q}_2}(p^m)$ については，$q^q x_0^2 + 4(x_1^2 + x_2^2 + x_3^2) = p^m$ の整数解の個数を考えれば良い．まず，x_0 のとり方から考える．$|x_0| \leq p^{m/2}/q$，$-p^{m/2}/q \leq x_0 \leq p^{m/2}/q$ となり，x_0 になりうる値は $2p^{m/2}/q + 1$ 個以下である．x_0 を固定して，$q^2x_0^2 + 4(x_1^2 + x_2^2 + x_3^2) = p^m$ を解くと，

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

となり，右辺は整数になる．命題 1.2.1 より任意の $\varepsilon > 0$ に対して

$$r_3\left(\frac{p^m - q^2x_0^2}{4}\right) = O_\varepsilon\left(\left(\frac{p^m - q^2x_0^2}{4}\right)^{1/2+\varepsilon}\right)$$

が成り立つ．ε に依存する定数 $C(\varepsilon)$ で

$$\begin{aligned} r_3\left(\frac{p^m - q^2x_0^2}{4}\right) &\leq C(\varepsilon)\left(\frac{p^m - q^2x_0^2}{4}\right)^{1/2+\varepsilon} \\ &\leq C(\varepsilon)(p^m)^{1/2+\varepsilon} \end{aligned}$$

だから，$r_3\left(\frac{p^m - q^2x_0^2}{4}\right) = O_\varepsilon((p^m)^{1/2+\varepsilon})$ といえる．このとき，

$$\begin{aligned} s_{\mathcal{Q}_2}(p^m) &= O_\varepsilon\left[(p^m)^{1/2+\varepsilon} \times \left(\frac{2p^{m/2}}{q} + 1\right)\right] \\ &= O_\varepsilon\left[\frac{p^{m(1+\varepsilon}}{q} + (p^m)^{1/2+\varepsilon}\right] \end{aligned}$$

である．よって，式 (7) は

$$
\begin{aligned}
&p^{m/2}M(\mu_k)\frac{\sinh(m+1)\Psi_k}{\sinh\Psi_k}\\
&\quad\le \frac{n}{2}s_{\mathcal{Q}_1}(p^m)+\frac{3}{8}c_V s_{\mathcal{Q}_2}(p^m)+np^{m/2}(m+1)\\
&\quad\le \frac{n}{2}C^{(1)}(\varepsilon_1)\left[\frac{p^{m(1+\varepsilon_1)}}{q^3}+\frac{p^{m/2(1+2\varepsilon_1)}}{q}\right]\\
&\qquad+\frac{3}{8}c_V C^{(2)}(\varepsilon_2)\left[\frac{p^{m(1+\varepsilon_2)}}{q}+(p^m)^{1/2+\varepsilon_2}\right]+np^{m/2}(m+1)
\end{aligned}
$$

となる．ここで $C^{(1)}(\varepsilon_1)$, $C^{(2)}(\varepsilon_2)$ はそれぞれ，n, ε_1 と c_V, ε_2 によって決まる定数である．$n<q^3/4$ であることと，c_V のもっとも大きな値が $2(q+1)$ であることを使うと，次のような式変形ができる．

$$
\begin{aligned}
p^{m/2}M(\mu_k)\frac{\sinh(m+1)\Psi_k}{\sinh\Psi_k}&\le \frac{q^3}{8}C^{(1)}(\varepsilon_1)\left[\frac{p^{m(1+\varepsilon_1)}}{q^3}+\frac{p^{m/2(1+2\varepsilon_1)}}{q}\right]\\
&\quad+\frac{3}{4}(q+1)C^{(2)}(\varepsilon_2)\left[\frac{p^{m(1+\varepsilon_2)}}{q}+(p^m)^{1/2+\varepsilon_2}\right]+\frac{q^3p^{m/2}}{4}(m+1)\\
&\le C'^{(1)}(\varepsilon_1)[p^{m(1+\varepsilon_1)}+q^2p^{m/2(1+2\varepsilon_1)}]\\
&\quad+C'^{(2)}(\varepsilon_2)\left[\frac{(q+1)p^{m(1+\varepsilon_2)}}{q}+(q+1)p^{m(1/2+\varepsilon_2)}\right]+\frac{q^3p^{m/2}}{4}(m+1).
\end{aligned}
$$

ただし，$C'^{(1)}(\varepsilon_1)$, $C'^{(2)}(\varepsilon_2)$ はそれぞれ，$C^{(1)}(\varepsilon_1)$, q と $C^{(2)}(\varepsilon_2)$, q によって決まる定数である．両辺を $p^{m/2}$ で割ると，

$$
\begin{aligned}
M(\mu_k)\frac{\sinh(m+1)\Psi_k}{\sinh\Psi_k}&\le C'^{(1)}(\varepsilon_1)[p^{m(1/2+\varepsilon_1)}+q^2p^{m\varepsilon_1}]\\
&\quad+C'^{(2)}(\varepsilon_2)\left[\frac{(q+1)p^{m(1/2+\varepsilon_2)}}{q}+(q+1)p^{m\varepsilon_2}\right]+\frac{q^3(m+1)}{4}\\
&\le C(\varepsilon)\left[\frac{2q+1}{q}\cdot p^{m(1/2+\varepsilon)}+(q^2+q+1)p^{m\varepsilon}\right]+\frac{q^3(m+1)}{4}
\end{aligned}
$$

となる．ここで $\varepsilon=\max\{\varepsilon_1,\varepsilon_2\}$, $C(\varepsilon)=\max\{C^{(1)}(\varepsilon_1), C^{(2)}(\varepsilon_2)\}$ である．次に，m を $p^{m/2}\le q^3$ を満たすようにとると，$p^m\le q^6$ だから，

$$
\begin{aligned}
M(\mu_k)\frac{\sinh(m+1)\Psi_k}{\sinh\Psi_k}&\le C(\varepsilon)\left[\frac{2q+1}{q}\cdot q^{3+6\varepsilon}+(q^2+q+1)q^{6\varepsilon}\right]+\frac{q^3(1+6\log_p q)}{4}\\
&\le C(\varepsilon)[(2q+1)\cdot q^{(2+6\varepsilon)}+(q^2+q+1)q^{6\varepsilon}]+\frac{q^3(1+6\log_p q)}{4}\\
&\le C(\varepsilon)[(2q^{(3+6\varepsilon)}+2q^{(2+6\varepsilon)}+q^{(1+6\varepsilon)}+q^{6\varepsilon}]+\frac{q^3(1+6\log_p q)}{4}
\end{aligned}
$$

と変形できるが，$0\le\Psi_j\le\log\sqrt{p}$ より $\sinh\Psi_k<\sinh\log\sqrt{p}$ だから，$\mathfrak{C}(\varepsilon)$ を $C(\varepsilon)$, p によって決まる定数とすると，

$$
M(\mu_k)\sinh(m+1)\Psi_k\le\mathfrak{C}(\varepsilon)q^{3+6\varepsilon} \tag{9}
$$

が成り立つ．ここで，m を $p^{m/2} \leq q^3$ となる最大の偶数とする．

$$\sinh(m+1)\Psi_k = \frac{e^{(m+1)\Psi_k} - e^{-(m+1)\Psi_k}}{2}$$

だから，任意に固定した $x > 0$ に対して $e^{x\Psi_k} > 3$ になるように q を十分大きくとる．このとき，この式は

$$\sinh(m+1)\Psi_k \geq \frac{e^{(m+1)\Psi_k}}{3}$$

となる．m は $m \leq 6\log_p q$ となる最大の偶数だから $m+2 \geq \log_p q$ であるので，

$$\begin{aligned}\sinh(m+1)\Psi_k &\geq \frac{e^{(6\log_p q-1)\Psi_k}}{3} \\ &= \frac{e^{-\Psi_k}}{3} e^{(6\log_p q)\Psi_k}\end{aligned}$$

となり，$\Psi_k \leq \log\sqrt{p}$ より

$$\sinh(m+1)\Psi_k \geq \frac{p^{-1/2}}{3} e^{(6\log_p q)\Psi_k}$$

が成り立つ．よって，式 (9) より，

$$\begin{aligned}M(\mu_k) &\leq \mathfrak{C}(\varepsilon) q^{(3+6\varepsilon)} 3p^{1/2} e^{-(6\log_p q)\Psi_k} \\ &= \mathfrak{C}'(\varepsilon) q^{(3+6\varepsilon)} q^{-6\Psi_k/\log p} \\ &= \mathfrak{C}'(\varepsilon) q^{(3+6\varepsilon-6\Psi_k)/\log p}\end{aligned}$$

となる．ただし，$\mathfrak{C}(\varepsilon)'$ は $\mathfrak{C}(\varepsilon)$, p によって決まる定数である．μ_k は非自明な固有値であるから，命題 3.1.4 より $M(\mu_k) \geq (q-1)/2$ が分かっている．よって，

$$\mathfrak{C}'(\varepsilon) q^{(3+6\varepsilon-6\Psi_k)/\log p} \geq \frac{q-1}{2}$$

ここで，

$$\begin{aligned}2\mathfrak{C}'(\varepsilon) q^{(3+6\varepsilon-6\Psi_k)/\log p} &\geq q-1 \\ \log_q 2\mathfrak{C}(\varepsilon)' + \left(3 + 6\varepsilon - \frac{6\Psi_k}{\log p}\right) &\geq \log_q(q-1)\end{aligned}$$

だから，十分大きな q をとると，$3 + 6\varepsilon - 6\Psi_k/\log p \geq 1$ になる．ゆえに，

$$\begin{aligned}-\frac{6\Psi_k}{\log p} &\geq -6\varepsilon - 2, \\ -6\Psi_k &\geq (-6\varepsilon - 2)\log p, \\ \Psi_k &\leq (\frac{1}{3} + \varepsilon)\log p\end{aligned}$$

と変形できる．このとき，$\theta_k = i\Psi_k$ または $\theta_k = \pi + i\Psi_k$ で $\mu_k = 2\sqrt{p}\cos\theta_k$ だから

$$\begin{aligned}
|\mu_k| &= 2\sqrt{p}|\cos i\Psi_k| \\
&= 2\sqrt{p}\cosh\Psi_k \\
&\leq 2\sqrt{p}\cosh\left[\left(\frac{1}{3}+\varepsilon\right)\log p\right] \\
&= 2\sqrt{p}\,\frac{e^{(1/3+\varepsilon)\log p}+e^{-(1/3+\varepsilon)\log p}}{2} \\
&= \sqrt{p}(p^{1/3+\varepsilon}+p^{-(1/3+\varepsilon)}) \\
&= p^{5/6+\varepsilon}+p^{1/6-\varepsilon}
\end{aligned}$$

となり，$0 < \varepsilon < 1/6$ で

$$p+1-(p^{5/6+\varepsilon}+p^{1/6-\varepsilon}) > \varepsilon'$$

となる $\varepsilon' > 0$ が存在するので，命題 1.1.4 より，$Z^{p,q}$ の族は family of expanders である．□

この定理と命題 1.1.9 から，次のような彩色数の評価ができる．

系 3.1.6. $\varepsilon \in (0,1/6)$ を固定する．p, q を $p \geq 5$, $p^8 < q$ と $\left(\frac{p}{q}\right) = 1$ かつ $p \not\equiv 3 \pmod 8$ を満たす奇素数とする．q が十分大きいとき，

$$\chi(Z^{p,q}) \geq \frac{p+1}{p^{5/6+\varepsilon}+p^{1/6-\varepsilon}}$$

である．つまり，$Z^{p,q}$ は大きな彩色数を持つ．

すでに 2.2 節で，p, q を $p \geq 5$, $q > p^7$ を満たす奇素数であり，q が $p^7 < q \leq p^8$ のときは，p は (5) 以外であるという仮定を満たし，更に $\left(\frac{p}{q}\right) = 1$ かつ $p \not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right) = -1$ であるという条件下では，$Z^{p,q}$ は大きな girth を持つということが分かっている．よってこの系とあわせると，この系の仮定のもとで $Z^{p,q}$ は良いグラフであることが分かった．

3.2 頂点推移的でないラマヌジャングラフ

最後に，ラマヌジャングラフであることを示す．

定理 3.2.1. $p \geq 5, p^8 < q$ を満たす奇素数 p, q であるとする．$\left(\frac{p}{q}\right) = 1$ かつ $p \not\equiv 3 \pmod 8$，または $\left(\frac{p}{q}\right) = -1$ を満たすとする．$Z^{p,q}$ はラマヌジャングラフである．

証明. 1954 年に Eichler[3] によって示されたラマヌジャン予想を使う．Eicher の結果により，

$$s_{\mathcal{Q}_1}(p^m) = \frac{4}{q(q^2-1)}\frac{p^{m+1}-1}{p-1} + O_{\varepsilon_1}(p^{m(1+\varepsilon)/2})$$

が分かっている．また，Appendix の式 (24)，(26) より，

$$s_{\mathcal{Q}_2}(p^m) = \begin{cases} \frac{2}{q-1}\frac{p^{m+1}-1}{p-1} + O_{\varepsilon_2}(p^{m(1+\varepsilon)/2}) & (q \equiv 1 \pmod 4) \\ \frac{2}{q+1}\frac{p^{m+1}-1}{p-1} + O_{\varepsilon_2}(p^{m(1+\varepsilon)/2}) & (q \equiv 3 \pmod 4) \end{cases}$$

も分かっている．今，$Z^{p,q}$ のトレース公式は式 (6) より全ての $m \in \mathbb{N} \cup \{0\}$ に対し

$$p^{m/2}\sum_{j=0}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{p}}\right) = \frac{n}{2}s_{\mathcal{Q}_1}(p^m) + \frac{3}{8}c_V s_{\mathcal{Q}_2}(p^m) \tag{10}$$

と書けている．ここで，式 (10) の左辺に関して，$Z^{p,q}$ の自明な固有値のときについて考える．
$\left(\frac{p}{q}\right) = 1$ のとき，自明な固有値は μ_0 のみだから，

$$\begin{aligned} \text{左辺} &= p^{m/2}U_m\left(\frac{\mu_0}{s\sqrt{p}}\right) \\ &= p^{m/2}U_m(\cos\theta_0) \\ &= p^{m/2}\frac{\sin(m+1)\theta_0}{\sin\theta_0} \\ &= p^{m/2}\frac{\sin(m+1)(i\log\sqrt{p})}{\sin(i\log\sqrt{p})} \\ &= p^{m/2}\frac{e^{-(m+1)\log\sqrt{p}} - e^{(m+1)\log\sqrt{p}}}{e^{-\log\sqrt{p}} - e^{\log\sqrt{p}}} \\ &= p^{m/2}\frac{p^{-(m+1)/2} - p^{(m+1)/2}}{p^{-1/2} - p^{1/2}} \\ &= p^{m/2}p^{-m/2}\frac{1-p^{m+1}}{1-p} \\ &= \frac{1-p^{m+1}}{1-p} \end{aligned}$$

となる．$\left(\frac{p}{q}\right) = 1$ のときは二部グラフなので，自明な固有値は μ_0, μ_{n-1} の 2 つだから，

$$\begin{aligned} \text{左辺} &= p^{m/2}U_m\left(\frac{\mu_0}{s\sqrt{p}}\right) + p^{m/2}U_m\left(\frac{\mu_{n-1}}{s\sqrt{p}}\right) \\ &= p^{m/2} \times 2U_m\left(\frac{\mu_0}{s\sqrt{p}}\right) \\ &= 2\frac{1-p^{m+1}}{1-p} \end{aligned}$$

となる．次に式 (10) の右辺に関して，二次形式の支配的な項のみ考える．
(a) $\left(\frac{p}{q}\right) = 1$ かつ $q \equiv 1 \pmod 4$ のとき．
$n = q(q^2-1)/8$, $c_V = q-1$ である．よって，

$$\frac{n}{2}\left(\frac{4}{q(q^2-1)}\frac{p^{m+1}-1}{p-1}\right) + \frac{3}{8}c_V\left(\frac{2}{q-1}\frac{p^{m+1}-1}{p-1}\right)$$

$$= \left(\frac{2n}{q(q^2-1)} + \frac{3c_V}{4(q-1)} \right) \frac{p^{m+1}-1}{p-1}$$
$$= \left(\frac{1}{4} + \frac{3}{4} \right) \frac{p^{m+1}-1}{p-1}$$
$$= \frac{p^{m+1}-1}{p-1}$$

となる.

(b) $\left(\frac{p}{q}\right) = 1$ かつ $q \equiv 3 \pmod 4$ のとき.

$n = q(q^2-1)/8$, $c_V = q+1$ である. よって,

$$\frac{n}{2} \left(\frac{4}{q(q^2-1)} \frac{p^{m+1}-1}{p-1} \right) + \frac{3}{8} c_V \left(\frac{2}{q+1} \frac{p^{m+1}-1}{p-1} \right)$$
$$= \left(\frac{2n}{q(q^2-1)} + \frac{3c_V}{4(q+1)} \right) \frac{p^{m+1}-1}{p-1}$$
$$= \left(\frac{1}{4} + \frac{3}{4} \right) \frac{p^{m+1}-1}{p-1}$$
$$= \frac{p^{m+1}-1}{p-1}$$

となる.

(c) $\left(\frac{p}{q}\right) = -1$ かつ $q \equiv 1 \pmod 4$ のとき.

$n = q(q^2-1)/4$, $c_V = 2(q-1)$ である. よって,

$$\frac{n}{2} \left(\frac{4}{q(q^2-1)} \frac{p^{m+1}-1}{p-1} \right) + \frac{3}{8} c_V \left(\frac{2}{q+1} \frac{p^{m+1}-1}{p-1} \right)$$
$$= \left(\frac{2n}{q(q^2-1)} + \frac{3c_V}{4(q-1)} \right) \frac{p^{m+1}-1}{p-1}$$
$$= \left(\frac{1}{2} + \frac{3}{2} \right) \frac{p^{m+1}-1}{p-1}$$
$$= 2\frac{p^{m+1}-1}{p-1}$$

となる.

(d) $\left(\frac{p}{q}\right) = -1$ かつ $q \equiv 3 \pmod 4$ のとき.

$n = q(q^2-1)/4$, $c_V = 2(q+1)$ である. よって,

$$\frac{n}{2} \left(\frac{4}{q(q^2-1)} \frac{p^{m+1}-1}{p-1} \right) + \frac{3}{8} c_V \left(\frac{2}{q+1} \frac{p^{m+1}-1}{p-1} \right)$$
$$= \left(\frac{2n}{q(q^2-1)} + \frac{3c_V}{4(q+1)} \right) \frac{p^{m+1}-1}{p-1}$$
$$= \left(\frac{1}{2} + \frac{3}{2} \right) \frac{p^{m+1}-1}{p-1}$$
$$= 2\frac{p^{m+1}-1}{p-1}$$

となる．
つまり，支配的な項の部分が，$Z^{p,q}$ の自明な固有値と対応することが分かった．ゆえに，(a)，(b) の場合については

$$p^{m/2}\sum_{j=1}^{n-1}\frac{\sin(m+1)\theta_j}{\sin\theta_j}=\frac{n}{2}O_{\varepsilon_1}(p^{m(1+\varepsilon_1)/2})+\frac{3}{8}c_VO_{\varepsilon_2}(p^{m(1+\varepsilon_2)/2}) \tag{11}$$

が成り立ち，(c)，(d) の場合については

$$p^{m/2}\sum_{j=1}^{n-2}\frac{\sin(m+1)\theta_j}{\sin\theta_j}=\frac{n}{2}O_{\varepsilon_1}(p^{m(1+\varepsilon_1)/2})+\frac{3}{8}c_VO_{\varepsilon_2}(p^{m(1+\varepsilon_2)/2}) \tag{12}$$

が成り立つ．
3.1 節で述べたように，全ての非自明な固有値 $\mu=2\sqrt{p}\cos\theta$ に対応する θ が実数であればラマヌジャングラフであるので，非自明な固有値に対応する θ で実数でないものがあるとして矛盾を導く．式 (11) について考える．
θ_j が実数でないとすると，$\Psi_j\in(0,\log\sqrt{p}]$ で $\theta_j=i\Psi_j$ または $\theta_j=\pi+i\Psi_j$ で，m が偶数のとき，対応する区間では

$$\frac{\sin(m+1)\theta_j}{\sin\theta_j}=\frac{\sinh(m+1)\Psi_j}{\sinh\Psi_j}>0$$

である．式 (11)，(12) の左辺を，θ_j が実数の場合とそうでない場合に分けると，$\varepsilon_1,\varepsilon_2$ に対して定数 $C_{\varepsilon_1},C_{\varepsilon_2}$ が存在し，

$$p^{m/2}\sum_{\theta_j\in\mathbb{R}}\frac{\sin(m+1)\theta_j}{\sin\theta_j}+p^{m/2}\sum_{\theta_j\notin\mathbb{R}}\frac{\sin(m+1)\theta_j}{\sin\theta_j}\le\frac{n}{2}C_{\varepsilon_1}(p^{m(1+\varepsilon_1)/2})+\frac{3}{8}c_VC_{\varepsilon_2}(p^{m(1+\varepsilon_2)/2})$$

と書けるので，この式に注目する．左辺の前半部分に関しては θ_j が実数の場合であるので，$|(\sin(m+1)\theta_j)/\sin\theta_j|\le m+1$ より，

$$\left|\sum_{\theta_j\in\mathbb{R}}\frac{\sin(m+1)\theta_j}{\sin\theta_j}\right|<n(m+1)$$

が成り立つ．左辺の後半部分については，$0<\Psi_j\le\log\sqrt{p}$ より

$$\begin{aligned}\frac{\sin(m+1)\theta_j}{\sin\theta_j}&=\frac{e^{(m+1)\Psi_j}-e^{-(m+1)\Psi_j}}{e^{\Psi_j}-e^{-\Psi_j}}\\&=e^{m\Psi_j}\frac{e^{\Psi_j}-e^{-(2m+1)\Psi_l}}{e^{\Psi_j}-e^{-\Psi_j}}\\&=e^{m\Psi_j}\frac{1-e^{-2m\Psi_j}}{1-e^{-2\Psi_j}}\\&\ge e^{m\Psi_j}\frac{1-e^{-2m\Psi_j}}{1-p^{-1}}\\&\ge e^{m\Psi_j}(1-e^{-m\Psi_j})\end{aligned}$$

なので，m を大きくとると，$e^{m\Psi_j}/2$ で抑えられる．今，実数でない θ が存在すると仮定しているので，後半部分の項についても存在し，この式は

$$-n(m+1)+\frac{e^{m\Psi_j}}{2} \leq \frac{n}{2}C_{\varepsilon_1}(p^{m(1+\varepsilon_1)/2})+\frac{3}{8}c_V C_{\varepsilon_2}(p^{m(1+\varepsilon_2)/2}),$$
$$-n(m+1)+\frac{e^{m\Psi_j}}{2} \leq C'_{\varepsilon_1}p^{m\varepsilon_1/2}+C'_{\varepsilon_2}p^{m\varepsilon_2/2} \tag{13}$$

とできる．ただし C'_{ε_1} と C'_{ε_2} はそれぞれ，$C_{\varepsilon_1}, m, n, p$ と $C_{\varepsilon_2}, c_V, m, p$ によって決まる定数である．ここで，$e^{\Psi_j} > p^{\varepsilon/2}$ を満たすような ε よりも小さい $\varepsilon_1, \varepsilon_2 > 0$ をとる．このとき，式 (13) を満たすような定数 $\mathfrak{C}_{\varepsilon_1}, \mathfrak{C}_{\varepsilon_2}$ が ε_1, n と c_V, ε_2 に対してそれぞれ決まる．よって，式 (13) は次のように書き換えられる．

$$-n(m+1)+\frac{e^{m\Psi_j}}{2} \leq \mathfrak{C}_{\varepsilon_1}p^{m\varepsilon_1/2}+\mathfrak{C}_{\varepsilon_2}p^{m\varepsilon_2/2}.$$

ここで，$C_{1,2}=\max\{\mathfrak{C}_{\varepsilon_1}, \mathfrak{C}_{\varepsilon_2}\}$, $\varepsilon_{1,2}=\max\{\varepsilon_1, \varepsilon_2\}$ とおくと，

$$-n(m+1)+\frac{e^{m\Psi_j}}{2} \leq C_{1,2}p^{m\varepsilon_{1,2}/2}+C_{1,2}p^{m\varepsilon_{1,2}/2},$$
$$-n(m+1)+\frac{e^{m\Psi_j}}{2} \leq 2C_{1,2}p^{m\varepsilon_{1,2}/2},$$
$$\frac{-n(m+1)}{2p^{m\varepsilon_{1,2}/2}}+\frac{1}{4}\left(\frac{e^{\Psi_j}}{p^{\varepsilon_{1,2}/2}}\right)^m \leq C_{1,2}$$

となる．しかし，これは $m\to\infty$ のとき，$\frac{-n(m+1)}{2(p^{\varepsilon_{1,2}/2})^m}\to 0$, $\left(\frac{e^{\Psi_j}}{p^{\varepsilon_{1,2}/2}}\right)^m\to\infty$ となるので，矛盾である． □

参考文献

[1] G. Davidoff, P. Sarnak & A. Vallette, *Elementary Number Theory, Group Theory, and Ramnujan Graphs*, London Math. Soc., **55**, Cambridge Univ. Press, 2003

[2] E. Grosswald,*Representations of Integers as sum of square* Springer, 1985

[3] M. Eichler, *Quaternäre quadratischen Formen und die Riemannsche Vermutung für die Kongruentzzeta Funktion*, Archiv. der Math. **5**(1954), 355-366

Appendix

2次形式のテータ級数と Eisenstein 級数

露峰 茂明

Ramanujan 予想

$\mathfrak{H}$ を複素上半平面 $\{z \in \mathbf{C} \mid \Im z > 0\}$ とする，ここで $\Im z$ は z の虚部を表す記号である．Γ を $\mathrm{SL}_2(\mathbf{Z})$ の部分群で，主合同部分群を含むものとする．Γ は分数一次変換により $\mathfrak{H}$ に作用する；

$$z \longrightarrow Mz = \frac{az+b}{cz+d} \quad (z \in \mathfrak{H},\ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma).$$

これ以降，保型関数論の基礎知識を前提にして述べる．

$\mathfrak{H}$ 上の正則関数 f が

$$f(Mz) = (cz+d)^k f(z) \quad (M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma) \tag{14}$$

を満たし，さらに尖点でも正則であるとき，f を重さ k の保型形式であるという．theta 級数は重さ $1/2$ の保型形式であるが，$(cz+d)^{1/2}$ 以外に，自然に決まる乗法系が付随する．保型形式がすべての尖点で 0 となるときは，尖点形式であるという．保型形式はカスプ（尖点） $i\infty$ を中心とした Fourier 展開を持つ；

$$f(z) = \sum_{n=0}^{\infty} a_n \mathbf{e}(nz),$$

ここで $\mathbf{e}(z) = e^{2\pi iz}$ であり，また a_n は複素数である．f が尖点形式であるとき，その Fourier 係数に対する不等式

$$|a_n| \leq O_\varepsilon(n^{(k-1)/2+\varepsilon}) \qquad ({}^\forall\varepsilon > 0)$$

を Ramanujan 予想というが，これは Deligne が Weil 予想を証明したことにより，少なくとも重さ $k \geq 2$ が偶数ならば成立することが示された．なお，本稿で用いる $k = 2$ の場合は，1954 年に Eichler[E] により示された．

自然数 N に対して、群 $\Gamma_0(N)$ を

$$\Gamma_0(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \mid c \equiv 0 \pmod{N}\}$$

で定義する．奇素数 q に対し，群 $\Gamma_0(16q^2)$ についての保型関数論が必要となる．この群のカスプの代表元は

$$\{\frac{1}{2^s q^2}, \frac{1}{2^s} \mid s = 0,1,3,4\} \cup \{\frac{j}{2^s q} \mid s = 1,3,4,\ j \text{ は奇数で } 1 \leq j \leq 2q-1, j \neq q\} \cup \{\frac{j}{q} \mid 1 \leq j \leq q-1\}$$
$$\cup \{\frac{1}{2^2 q^2}, \frac{3}{2^2 q^2}, \frac{1}{2^2}, \frac{3}{2^2}\} \cup \{\frac{j}{2^2 q} \mid j \text{ は奇数で } 1 \leq j \leq 4q-1, j \neq q, 3q\}$$

の $6(q+1)$ 個である．この内の $\frac{1}{16q^2}$ が，無限遠のカスプ $i\infty$ と同値である．保型関数 f のカスプ $r \in \mathbf{Q}$ での値は，$i\infty$ をカスプ r に写す行列 $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}), c > 0$ に対し

$$\lim_{z \to i\infty} (cz+d)^{-k} f(Mz) \tag{15}$$

で定義する．k が半整数であるときは $0 < \arg(cz+d)^{1/2} \leq \pi$ の条件を加える．$f(z)$ が指標付きの保型形式の場合も同じ (15) で，カスプでの値を定める．

Theta 級数

$\mathfrak{H}$ 上の関数の theta 級数は

$$\theta(z) = \sum_{n=0}^{\infty} \mathbf{e}(n^2 z) \qquad (z \in \mathfrak{H})$$

で定義されるものである．$M \in \mathrm{SL}_2(\mathbf{Z})$ に対する変換公式，すなわち $\theta(Mz)$ を Mz でなく直接 z の関数として書く公式はよく知られている（例えば Rademacher[R] 第１０章）．q を奇素数とする．この変換公式を用いて，それぞれ $\theta(2z)$ が $\Gamma_0(4)$ の，$\theta(8z)$ が $\Gamma_0(16)$ の，$\theta(2q^2z)$ が $\Gamma_0(4q^2)$ の，$\theta(8q^2z)$ が $\Gamma_0(16q^2)$ の，重さ $1/2$ の保型形式であることが分かる．これらの群の内で $\Gamma_0(4q^2)$ が最小であり，すべてをこの群についての保型形式とみなすことができる．

$\theta(2z), \theta(8z), \theta(2q^2z), \theta(8q^2z)$ の，各カスプでの値を，同じく変換公式を用いて求めることができる．それは，以下のようになる．奇数 j に対し、記号 λ_j を

$$\lambda_j = \begin{cases} 1 & (j \equiv 1 \pmod 4) \\ -i & (j \equiv 3 \pmod 4) \end{cases}$$

で定義する．

表 1:

	$\theta(2z)$	$\theta(8z)$	$\theta(2q^2z)$	$\theta(8q^2z)$
$1/(16q^2)$	1	1	1	1
$1/(8q^2)$	1	0	1	0
$1/(4q^2)$	1	$2^{-1}(1-i)$	1	$2^{-1}(1-i)$
$3/(4q^2)$	$-i$	$2^{-1}(1-i)$	$-i$	$2^{-1}(1-i)$
$1/(2q^2)$	0	$2^{-3/2}(1-i)$	0	$2^{-3/2}(1-i)$
$1/q^2$	$2^{-1}(1-i)$	$2^{-2}(1-i)$	$2^{-1}(1-i)$	$2^{-2}(1-i)$
$j/(16q)$, $^{1 \leq j \leq 2q-1,}_{(2q,j)=1}$	$\left(\frac{q}{j}\right)\lambda_j$	$\left(\frac{q}{j}\right)\lambda_j$	$\lambda_{jq}q^{-1/2}$	$\lambda_{jq}q^{-1/2}$
$j/(8q)$, $^{1 \leq j \leq 2q-1,}_{(2q,j)=1}$	$\left(\frac{2q}{j}\right)\lambda_j$	0	$\left(\frac{2}{qj}\right)\lambda_{jq}q^{-1/2}$	0
$j/(4q)$, $^{1 \leq j \leq 4q-1,}_{j \neq q, 3q}$	$\left(\frac{q}{j}\right)\lambda_j$	$\left(\frac{j}{q}\right)2^{-1}(1-i)\lambda_q^{-1}$	$\lambda_{jq}q^{-1/2}$	$2^{-1}(1-i)q^{-1/2}$

$j/(2q)$, $1 \leq j \leq 2q-1$, $(2q,j)=1$	0	$\left(\frac{2j}{q}\right) 2^{-3/2}(1-i)\lambda_q$	0	$2^{-3/2}(1-i)q^{-1/2}$
j/q, $1 \leq j \leq q-1$	$\left(\frac{j}{q}\right) 2^{-1}(1-i)\lambda_q^{-1}$	$\left(\frac{j}{q}\right) 2^{-2}(1-i)\lambda_q^{-1}$	$2^{-1}(1-i)q^{-1/2}$	$2^{-2}(1-i)q^{-1/2}$
$1/16$	1	1	q^{-1}	q^{-1}
$1/8$	1	0	q^{-1}	0
$1/4$	1	$2^{-1}(1-i)$	q^{-1}	$2^{-1}(1-i)q^{-1}$
$3/4$	$-i$	$2^{-1}(1-i)$	$-iq^{-1}$	$2^{-1}(1-i)q^{-1}$
$1/2$	0	$2^{-3/2}(1-i)$	0	$2^{-3/2}(1-i)q^{-1}$
1	$2^{-1}(1-i)$	$2^{-2}(1-i)$	$2^{-1}(1-i)q^{-1}$	$2^{-2}(1-i)q^{-1}$

Q を 4 次の正値 2 次形式とする.

$$\theta_Q(z) := \sum_{\mathbf{x}\in\mathbf{Z}^4} \mathbf{e}(Q(\mathbf{x}))$$

を 2 次形式の theta 級数という. Q が整係数であるとき, $\theta_Q(z)$ は Q について決まる $\mathrm{SL}_2(\mathbf{Z})$ の部分群についての, 重さ 2 の保型形式となる. この Fourier 展開を

$$\theta_Q(z) = \sum_{n=0}^{\infty} s_Q(n)\mathbf{e}(nz)$$

とおく. このとき $s_Q(n)$ は 2 次形式 Q による n の表現数となる, すなわち

$$s_Q(n) = \sharp\{\mathbf{x}\in\mathbf{Z}^4 \mid Q(\mathbf{x}) = n\}$$

となる. q を奇素数とし, $\mathbf{x} = {}^t(x_1, x_1, x_2, x_3)$ とする. 論文に表れる $\mathbf{x}$ の 2 次形式

$$\begin{aligned} Q_1(\mathbf{x}) &= x_0^2 + 4q^2x_1^2 + 4q^2x_2^2 + 4q^2x_3^2, \\ Q_2(\mathbf{x}) &= q^2x_0^2 + 4x_1^2 + 4x_2^2 + 4x_3^2 \end{aligned} \tag{16}$$

についての theta 級数を考察する. 容易に分かるように

$$\begin{aligned} \theta_{Q_1}(z) &= \theta(2z)\theta(8q^2z)^3, \\ \theta_{Q_2}(z) &= \theta(2q^2z)\theta(8z)^3 \end{aligned}$$

である. よって $\theta_{Q_1}(z), \theta_{Q_2}(z)$ は群 $\Gamma_0(8q^2)$ についての重さ 2 の保型形式である. 表 1 より, $\theta_{Q_1}(z), \theta_{Q_2}(z)$ の, 各カスプでの値が求められる.

表 2:

	$\theta_{Q_1}(z)$	$\theta_{Q_2}(z)$
$1/(16q^2)$	1	1
$1/(8q^2)$	0	0
$1/(4q^2)$	$-2^{-2}(1+i)$	$-2^{-2}(1+i)$
$3/(4q^2)$	$-2^{-2}(1-i)$	$-2^{-2}(1-i)$

$1/(2q^2)$	0	0
$1/q^2$	-2^{-5}	-2^{-5}
$j/(16q)_{,(2q,j)=1}^{1\le j\le 2q-1,}$	$\left(\frac{j}{q}\right)\lambda_q^{-1}q^{-3/2}$	$\left(\frac{j}{q}\right)\lambda_q q^{-1/2}$
$j/(8q)_{,(2q,j)=1}^{1\le j\le 2q-1,}$	0	0
$j/(4q)_{,j\neq q,3q}^{1\le j\le 4q-1,}$	$-\left(\frac{j}{q}\right)2^{-2}q^{-3/2}(\lambda_q^{-1}+(-1)^{(j-1)/2}i\lambda_q)$	$-\left(\frac{j}{q}\right)2^{-2}q^{-1/2}(\lambda_q+(-1)^{(j-1)/2}i\lambda_q^{-1})$
$j/(2q)_{(2q,j)=1}^{1\le j\le 2q-1,}$	0	0
$j/q,_{1\le j\le q-1}$	$-\left(\frac{j}{q}\right)\lambda_q^{-1}2^{-5}q^{-3/2}$	$-\left(\frac{j}{q}\right)\lambda_q 2^{-5}q^{-1/2}$
$1/16$	q^{-3}	q^{-1}
$1/8$	0	0
$1/4$	$-2^{-2}(1+i)q^{-3}$	$-2^{-2}(1+i)q^{-1}$
$3/4$	$-2^{-2}(1-i)q^{-3}$	$-2^{-2}(1-i)q^{-1}$
$1/2$	0	0
1	$-2^{-5}q^{-3}$	$-2^{-5}q^{-3}$

よって $q\theta_{Q_1}(z)-\theta_{Q_2}(z)$ の各カスプでの値は

表 3:

	$q\theta_{Q_1}(z)-\theta_{Q_2}(z)$
$1/(16q^2)$	$q-1$
$1/(4q^2)$	$-2^{-2}(1+i)(q-1)$
$3/(4q^2)$	$-2^{-2}(1-i)(q-1)$
$1/q^2$	$-2^{-5}(q-1)$
$j/(16q)$	$0 \quad (q\equiv 1 \pmod 4)$ $i\left(\frac{j}{q}\right)2q^{-1/2} \quad (q\equiv 3 \pmod 4)$
$j/(4q)$	$0 \quad (q\equiv 1 \pmod 4)$ $-(-1)^{(j-1)/2}\left(\frac{j}{q}\right)2^{-1}q^{-1/2} \quad (q\equiv 3 \pmod 4)$
j/q	$0 \quad (q\equiv 1 \pmod 4)$ $-i\left(\frac{j}{q}\right)2^{-4}q^{-1/2} \quad (q\equiv 3 \pmod 4)$
$1/16$	$-q^{-2}(q-1)$
$1/4$	$2^{-2}(1+i)q^{-2}(q-1)$
$3/4$	$2^{-2}(1-i)q^{-2}(q-1)$
1	$2^{-5}q^{-2}(q-1)$

となる，ただし表にないカスプでの値は，すべて 0 である．

Eisenstein 級数

N を自然数とする．$k>0$ を偶数とし c_0, d_0 を整数とするときとき，Hecke[H] に従って，Eisenstein 級数を

$$G_k(z; c_0, d_0; N) = \sum_{\substack{c \equiv c_0(N) \\ d \equiv d_0(N)}}{}' \frac{1}{(cz+d)^k |cz+d|^s}\Big|_{s=0} \tag{17}$$

により定義する．ここで $\sum'$ は，もし和で $(c,d)=(0,0)$ となる場合があったらその項を無視することを意味し，また $|_{s=0}$ は，s の解析関数として解析接続したものに $s=0$ を代入することを意味する．Eisenstein 級数 (17) の一次結合も，Eisenstein 級数と言われる．(17) は，c_0, d_0 については法 N で決まるものである．

$N=1$ とする．このときは $c_0=d_0=0$ としてよい．

$$G_k(z) := \frac{(k-1)!}{(-2\pi i)^k} G_k(z; 0, 0; 1)$$

とおく．この Fourier 展開は

$$G_k(z) = \zeta(1-k) - \delta_{k,2}\frac{\pi i}{\Im z} + 2\sum_{n=1}^{\infty} \sigma_{k-1}(n)\mathbf{e}(nz)$$

で与えられる．ここで $\zeta(s)$ は Riemann zeta 関数を表し，また σ_{k-1} は

$$\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$$

で定義される数論的関数である．この関数は n が整数でないときは値は 0 と定義する．また $\delta_{k,2}$ は Kronecker のデルタを表している．すなわち $k=2$ のときだけ $-\pi i/\Im z$ という項が現れ，そのため $k=2$ のときは正則関数とならない．$G_k(z)$ は (14) の変換公式を群 $\mathrm{SL}_2(\mathbf{Z})$ に対し満たしている．特に $k \geq 4$ のときは保型形式となる．

自然数 N に対し $G_k(Nz)$ は変換公式 (14) を群 $\Gamma_0(N)$ に対し満たす．$k \geq 4$ ならば $G_k(Nz)$ は $\Gamma_0(N)$ に対する重さ k の保型形式である．$k=2$ のときも，例えば

$$G_2(z) - NG_2(Nz)$$

では $1/\Im z$ を持つ項が消えるため，これは $\Gamma_0(N)$ に対する重さ 2 の保型形式である．

重さ 2 の Eisenstein 級数で，カスプで取る値が表 3 となるものを構成したい．まず，表 3 の値の実部と一致するものを構成する．$G_2(z), G_2(2z), G_2(4z), G_2(8z), G_2(16z)$ の $\Gamma_0(16)$ のカスプ $1/16, 1/8, 1/4, 3/4, 1/2, 1$ での値は次の通りである．

表 4:

	$G_2(z)$	$G_2(2z)$	$G_2(4z)$	$G_2(8z)$	$G_2(16z)$
1/16	−1/12	−1/12	−1/12	−1/12	−1/12
1/8	−1/12	−1/12	−1/12	−1/12	−1/48
1/4	−1/12	−1/12	−1/12	−1/48	−1/192
3/4	−1/12	−1/12	−1/12	−1/48	−1/192
1/2	−1/12	−1/12	−1/48	−1/192	−1/768
1	−1/12	−1/48	−1/192	−1/768	−1/3072

この表より

$$F(z) := (1/2)G_1(z) - (3/2)G_2(2z) + 5G_2(4z) - 16G_2(16z)$$

はカスプ $1/16, 1/8, 1/4, 3/4, 1/2, 1$ で，それぞれ $1, 0, -2^{-2}, -2^{-2}, 0, -2^{-5}$ の値を取ることが分かる．更に $F(z)$ は $1/\Im z$ の項が消えており，正則でもある．よって $F(z)$ は保型形式である．

$F(z), F(q^z)$ は群 $\Gamma_0(16q^2)$ についての保型形式である．各カスプでの値は，

表 5:

	$F(z)$	$F(q^2z)$
$1/(16q^2)$	1	1
$1/(4q^2)$	-2^{-2}	-2^{-2}
$3/(4q^2)$	-2^{-2}	-2^{-2}
$1/q^2$	-2^{-5}	-2^{-5}
$j/(16q)$	1	q^{-2}
$j/(4q)$	-2^{-2}	$-2^{-2}q^{-2}$
$3j/(4q)$	-2^{-2}	$-2^{-2}q^{-2}$
j/q	-2^{-5}	$-2^{-5}q^{-2}$
$1/16$	1	q^{-4}
$1/4$	-2^{-2}	$-2^{-2}q^{-4}$
$3/4$	-2^{-2}	$-2^{-2}q^{-4}$
1	-2^{-5}	$-2^{-5}q^{-4}$

となる，ただし表にないカスプでの値は，すべて 0 である．よって，

$$-\frac{1}{q+1}\{F(z) - q^2F(q^2z)\} \tag{18}$$

はカスプでの値が，$q \equiv 3 \pmod 4$ のときの $j/(4q)$ を除いて，表 3 の実数部分と一致する Eisenstein 級数である．

表 3 の虚数部分をカスプでの値とする Eisenstein 級数を構成する．2 種類の Eisenstein 級数が必要となる．Eisenstein 級数

$$\widetilde{G}_2(z) := \frac{2i}{\pi^2} \sum_{\substack{c_0 = 1,3 \\ d_0 = 1,3}} (-1)^{(c_0-1)/2+(d_0-1)/2} \sum_{0 \le l \le 3} G_2(z; 4c_0, 4c_0l + d_0; 16) \tag{19}$$

$$= 2 \sum_{\substack{n \equiv 1 (N) \\ n > 0}} (-1)^{(n-1)/2} \sigma_1(n) \mathbf{e}(nz) \tag{20}$$

は群 $\Gamma_0(16)$ に対する保型形式である．(19) は $\Gamma_0(16)$ のカスプの $1/4$ で値 $-i/2$ を，カスプの $3/4$ で値 $i/2$ を，そして他では 0 を取る．$\widetilde{G}_2(z), \widetilde{G}_2(q^2z)$ は群 $\Gamma_0(16q^2)$ に対する保型形式である．各カスプでの値は

表 6:

	$\widetilde{G}_2(z)$	$\widetilde{G}_2(q^2z)$
$1/(4q^2)$	$-i/2$	$-i/2$
$3/(4q^2)$	$i/2$	$i/2$
$j/(4q)$	$-i/2$	$-i/2q^{-2}$
$3j/(4q)$	$i/2$	$i/2q^{-2}$
$1/4$	$-i/2$	$-i/2q^{-4}$
$3/4$	$i/2$	$i/2q^{-4}$

となる，ただし表にないカスプでの値は，すべて 0 である．よって

$$-\frac{1}{2(q+1)}\{\widetilde{G}_2(z)-q^2\widetilde{G}_2(q^2z)\}$$

はカスプでの値が，$q\equiv 3 \pmod 4$ のときの $j/(16q), j/q$ を除いて，表 3 の虚数数部分と一致する Eisenstein 級数である．

$q\equiv 3 \pmod 4$ とする．q によって決まる Eisenstein 級数

$$\widehat{G}_2(z):=2\sum_{\substack{n\not\equiv 0(q)\\ n>0}}\left(\frac{n}{q}\right)\sigma_1(n)\mathbf{e}(nz)$$

は群 $\Gamma_0(q^2)$ に対する保型形式である．これは，$\Gamma_0(q^2)$ のカスプ j/q $(1\le j<q)$ で値 $\frac{-i}{12}\left(\frac{j}{q}\right)q^{-1/2}(q^2-1)$ を取り，他では 0 を取る．よって

$$\frac{1}{q^2-1}\{\widehat{G}_2(z)-\widehat{G}_2(2z)+8\widehat{G}_2(8z)-32\widehat{G}_2(16z)\} \tag{21}$$

は群 $\Gamma_0(16q^2)$ に対する保型形式で，カスプ $j/(16q)$ および j/q で表 3 のものと同じ値を取り，また他のカスプでは 0 を取る．

最後に，$q\equiv 3 \pmod 4$ のとき，$j/(4q)$ において表 3 の値を取る Eisenstein 級数を構成する．

$$\check{G}_2(z):=2\sum_{\substack{(n,2q)=1\\ n>0}}(-1)^{(n-1)/2}\left(\frac{n}{q}\right)\sigma_1(n)\mathbf{e}(nz)$$

これは $\Gamma_0(q^2)$ に対する保型形式で，カスプ $j/(4q)$ において $-\frac{1}{2}(-1)^{(j-1)/2}\left(\frac{j}{q}\right)q^{-1/2}(q^2-1)$ の値をとり，他のカスプでは 0 となる．よって $\frac{1}{q^2-1}\check{G}_2(z)$ が $j/(4q)$ において表 3 の値を取る Eisenstein 級数である．

表現数の近似式

2次形式 (16) の theta 級数 $\theta_{Q_1}(z), \theta_{Q_2}(z)$ の Fourier 展開を

$$\theta_{Q_1}(z) = \sum_{n=0}^{\infty} s_{Q_1}(n)\mathbf{e}(nz),$$

$$\theta_{Q_2}(z) = \sum_{n=0}^{\infty} s_{Q_2}(n)\mathbf{e}(nz)$$

とおく．Sarnak[S] により $\theta_{Q_1}(z)$ は Eisenstein 級数と尖点形式の和に書かれており，それを用いて，q と互いに素な奇素数 p と正の偶数 m に対して

$$s_{Q_1}(p^m) = \frac{4}{q(q^2-1)}\frac{p^{m+1}-1}{p-1} + O_\varepsilon(p^{\frac{m}{2}(1+\varepsilon)}) \tag{22}$$

が示されている．ここでは同様な近似式を Q_2 に対して求める．

$q \equiv 1 \pmod 4$ の場合を考える．今までの議論により，ある尖点形式 $g(z)$ があって

$$q\theta_{Q_1}(z) - \theta_{Q_2}(z) = -\frac{1}{2(q+1)}\{2F(z) - 2q^2F(q^2z) + \widetilde{G}_2(z) - q^2F(q^2z)\} + g(z)$$

となる．Sarnak[S] による $\theta_{Q_1}(z)$ の Eisenstein 級数 $E_2(z)$ と尖点形式 $g'(z)$ の和への分解を

$$\theta_{Q_1}(z) = E_2(z) + g'(z)$$

とすると

$$\theta_{Q_2}(z) = qE_2(z) + \frac{1}{2(q+1)}\{2F(z) - 2q^2F(q^2z) + \widetilde{G}_2(z) - q^2F(q^2z)\} + g(z) + qg'(z) \tag{23}$$

である．

ここで p を q と素な奇素数とし，m を正の偶数とする．(23) の左辺の Eisenstein 級数の p^m 番目の Fourier 係数は容易に求めることができる．これには $F(z)$ の項の $G_2(z)$ および $\widetilde{G}_2(z)$ しか関与しない．これより

$$s_{Q_2}(p^m) = \frac{2}{q-1}\frac{p^{m+1}-1}{p-1} + O_\varepsilon(p^{\frac{m}{2}(1+\varepsilon)}) \qquad (q \equiv 1 \pmod 4) \tag{24}$$

となる．

次に $q \equiv 3 \pmod 4$ の場合を考える．同様な考察で，

$$\begin{aligned}\theta_{Q_2}(z) =& qE_2(z) + \frac{1}{(q^2-1)}\left\{(q-1)F(z) - q^2(q-1)F(q^2z) + \frac{1}{2}(q-1)\widetilde{G}_2(z)\right.\\ &\left.-\frac{1}{2}q^2(q-1)F(q^2z) - \widehat{G}_2(z) + \widehat{G}_2(2z) - 8\widehat{G}_2(8z) + 32\widehat{G}_2(16z) - \check{G}_2(z)\right\} + g(z) + qg'(z)\end{aligned} \tag{25}$$

となる．(25) の Eisenstein 級数の部分の p^m 番目の Fourier 係数には，$G_2(z), \widetilde{G}_2(z), \widehat{G}_2(z), \check{G}_2(z)$ しか関与しない．これより

$$s_{Q_2}(p^m) = \frac{2}{q+1}\frac{p^{m+1}-1}{p-1} + O_\varepsilon(p^{\frac{m}{2}(1+\varepsilon)}) \qquad (q \equiv 3 \pmod 4) \tag{26}$$

となる．

参考文献

[E] M. EICHLER, *Quaternäre quadratischen Formen und die Riemannsche Vermutung für die Kongruentzzeta Funktion*, Archiv. der Math. **5**(1954), 355-366

[H] E. HECKE, *Theorie der Eisensteinschen Reihen Höherer Stufe und ihre Anwndung auf Funktionentheorie und Arithmetik*, Math. Werke. Vandenok und Ruprecht, Göttingen 1959, 461–486

[R] H. RADEMACHER, *Topics in Analytic Number Theory*, Springer, Grundlehren **169**, 1973

[S] P. SARNAK, *Some Applications of Modular Forms*, Cambridge Tract in Math. **99**, Cambridge Univ. Press, 1990