Vortrag 13
Der Cayleygraph von $PGL_2(\mathbb{F}_q)$ bzw $PSL_2(\mathbb{F}_q)$ ist ein zusammenhängender, regulärer Graph

Lara Beßmann

Wir werden die Graphen $Y^{p,q}$ konstruieren und einige Eigenschaften bestimmen, unter anderem werden wir zeigen, dass diese Graphen $Y^{p,q}$ zusammenhängend sind. Im Anschluss werden wir sehen, dass die konstruierten Graphen isomorph zu $X^{p,q}$ sind.

0.1 Erinnerung

$$X^{p,q} = \begin{cases} \Gamma(PSL_2(q), S_{p,q}) & \text{für p Quadrat modulo q} \\ \Gamma(PGL_2(q), S_{p,q}) & \text{für p nicht Quadrat modulo q} \end{cases}$$

Wobei wir diese Graphen über folgende Abbildungen konstruiert haben:

$$\mathbb{H}(\mathbb{Z}) \supseteq S_p \to \mathbb{H}(\mathbb{F}_q)^* \xrightarrow{\cong} GL_2(\mathbb{F}_q) \twoheadrightarrow PGL_2(\mathbb{F}_q) \supseteq S_{p,q}$$

1 Konstruktion von $Y^{p,q}$

Kommen wir nun zur Konstruktion von $Y^{p,q}$. Sei p eine ungerade Primzahl.

1.1 Erinnerung Wir benötigen nun zwei Mengen:

- $\Lambda' = \{\alpha \in \mathbb{H} \mid \ (\alpha \equiv 1 \ mod\ 2)\ oder\ (\alpha \equiv i+j+k \ mod\ 2)\ und\ N(\alpha) = p^l\ für\ ein\ l > 0\}$
- $S_p = \{\alpha_1, \bar{\alpha}_1, \alpha_2, \bar{\alpha}_2, ..., \alpha_s, \bar{\alpha}_s, \beta_1, ..., \beta_t\}$ der $p+1$ Quaternionen mit Norm p. Dabei gilt für alle α_i $\alpha_0^{(i)} > 0$ und für alle β_j $\beta_0^{(j)} = 0$. Es gilt also $\#S_p = p+1$ und $S_p \subseteq \Lambda'$.

1.2 Beispiel Wir wollen nun S_p für $p = 3$ betrachten. Gesucht sind also alle $\alpha_i \in \Lambda'$ mit $N(\alpha_i) = 3$ und $a_0^{(i)} > 0$ und alle $\beta_j \in \Lambda'$ mit $N(\beta_j) = 3$ und $b_0^{(j)} = 0$.
Sei also $\alpha_i = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda'$ mit $a_0^2 + a_1^2 + a_2^2 + a_3^2 = 3$ und $a_0 > 0$. Sei zuerst a_0 ungerade, dann folgt, dass a_1, a_2, a_3 gerade sind. Da $N(\alpha_i) = 3$ muss schon $a_1, a_2, a_3 = 0$ gelten. Damit folgt $a_0^2 = 3$, es gibt aber kein $z \in \mathbb{Z}$ mit $z^2 = 3 \lightning$.
Da $a_0 > 0$ vorausgesetzt ist, kann der Fall, dass a_0 gerade und a_1, a_2, a_3 ungerade sind ebenfalls nicht eintreten, da die Norm $N(\alpha_i) = 3$ sein muss.
Sei nun $\beta_j = b_1 i + b_2 j + b_3 k \in \Lambda'$ mit $b_1^2 + b_2^2 + b_3^2 = 3$. Da $b_0 = 0$, also gerade, müssen b_1, b_2, b_3 ungerade sein. Damit folgt sofort $b_1^2, b_2^2, b_3^2 = 1$, also gilt:

$$\begin{aligned} S_3 = \{&\beta_1 = 0 + 1i + 1j + 1k, \\ &\beta_2 = 0 + 1i + 1j - 1k, \\ &\beta_3 = 0 + 1i - 1j - 1k, \\ &\beta_4 = 1 - 1i + 1j - 1k\} \end{aligned}$$

Dies sind die einzigen Möglichkeiten, da nach der Konstruktion von S_p β mit $\bar{\beta}$ assoziiert wird und deswegen wird wird entweder β oder $\bar{\beta}$ ausgewählt. Außerdem muss nach der Voraussetzung $\#S_p = p+1$ gelten $\#S_3 = 3+1 = 4$ ✓.

Wir versehen Λ' nun mit folgender Äquivalenzrelation:

$$\alpha,\ \beta \in \Lambda' : \alpha \sim \beta \Leftrightarrow \exists n, m \in \mathbb{N} : p^m \alpha = \pm p^n \beta$$

Und setzen $\Lambda = \Lambda'/\sim$ als die Menge der Äquivalenzklassen und $Q : \Lambda' \to \Lambda, \alpha \mapsto [\alpha]$ als die Quotientenabbildung.
Jetzt können wir zeigen:

1.3 Proposition a) Λ ist eine Gruppe.
b) $\Gamma(\Lambda, Q(S_p))$ ist ein $p+1$-regulärer Baum.

Beweis. a) Verknüpfung: Setze $[\alpha][\beta] := [\alpha\beta]$ für $\alpha, \beta \in \Lambda'$. Diese ist wohldefiniert, denn für $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \Lambda'$ mit $\alpha_1 \sim \beta_1$ und $\alpha_2 \sim \beta_2$ gilt $\alpha_1\alpha_2 \sim \beta_1\beta_2$ und damit $[\alpha_1][\alpha_2] = [\alpha_1\alpha_2]$.
Assoziativität: Seien $\alpha, \beta, \gamma \in \Lambda'$, dann folgt $[\alpha][\beta\gamma] = [\alpha\beta\gamma] = [\alpha\beta][\gamma]$.
Neutralelement: $[p] \in \Lambda$. Sei $\alpha \in \Lambda'$ beliebig, dann gilt $[p][\alpha] = [p\alpha] = [\alpha] = [\alpha p] = [\alpha][p]$, da $\alpha \sim p\alpha$.
Inverse: Für $\alpha \in \Lambda'$ folgt $\bar{\alpha}\alpha = \alpha\bar{\alpha} \sim p$, denn es gilt $\bar{\alpha}\alpha = \alpha\bar{\alpha} = N(\alpha) = p^l$ für ein $l > 0$ und somit $p \cdot \alpha\bar{\alpha} = p \cdot p^l = p^l \cdot p$. Damit gilt außerdem $[\bar{\alpha}][\alpha] = [\bar{\alpha}\alpha] = [p] = [\alpha\bar{\alpha}] = [\alpha][\bar{\alpha}]$ und somit existiert $[\alpha]^{-1} = [\bar{\alpha}] \in \Lambda$.
$\Rightarrow \Lambda$ ist eine Gruppe.
b) Zuerst werden wir nun zeigen, dass $\Gamma(\Lambda, Q(S_p))$ $p+1$-regulär ist. Dazu müssen wir $\#Q(S_p) = p+1$ nach Proposition 4.1.2 zeigen, also dass $Q|_{S_p} : S_p \to \Lambda$ injektiv ist. Für $\alpha, \beta \in S_p$ mit $\alpha \sim \beta$ gilt $\alpha = \beta$ nach Korollar 2.5.14. Denn jedes $\alpha \in \Lambda'$, also insbesondere auch aus S_p, hat eine eindeutige Darstellung als reduziertes Wort über S_p. Da nun $N(\alpha) = N(\beta) = p$ gilt, und es $n, m \in \mathbb{N}$, ohne Einschränkung $m > n$, gibt mit $p^m\alpha = \pm p^n\beta \Leftrightarrow p^{m-n}\alpha = \pm\beta$ folgt schon $\alpha = \pm\beta$. Damit ist $Q|_{S_p}$ injektiv und es gilt $\#Q(S_p) = p+1$. Ebenfalls nach Korollar 2.5.14 gilt, dass $< Q(S_p) >= \Lambda$. Also ist $\Gamma(\Lambda, Q(S_p))$ $p+1$-regulär und zusammenhängend nach Proposition 4.1.2.
Es bleibt zu zeigen, dass $\Gamma(\Lambda, Q(S_p))$ ein Baum ist.
Dazu nehmen wir an, dass es einen Kreis $x_0, ..., x_g = x_0$ mit Länge $g \geq 3$ gibt. Da $\Gamma(\Lambda, Q(S_p))$ nach Proposition 4.1.2 Ecken-transitiv ist, können wir $x_0 = [p]$ annehmen. Nun existieren $\gamma_1, ..., \gamma_g \in S_p$ mit $x_1 = [\gamma_1],\ x_2 = [\gamma_1\gamma_2], ..., x_g = [\gamma_1 \cdots \gamma_g]$ nach Definition des Cayleygraphen. Es gilt $x_{k-1} \neq x_{k+1}$ für alle $1 \leq k \leq g-1$, denn sonst wäre der Kreis kürzer. Damit ist $\gamma_1 \cdots \gamma_g$ ein reduziertes Wort über S_p und es folgt $[p] = x_0 = x_g = [\gamma_1 \cdots \gamma_g]$, also gilt $\gamma_1 \cdots \gamma_g \sim p \Rightarrow \exists m, n \in \mathbb{N} : p^m 1 = \pm p^n \gamma_1 \cdots \gamma_g$ in Λ'. Dies ist aber ein Widerspruch zur Eindeutigkeit aus Korollar 2.5.14. Also gibt es keinen Kreis in $\Gamma(\Lambda, Q(S_p)) \Rightarrow \Gamma(\Lambda, Q(S_p))$ ist ein Baum. □

Jetzt kommen wir zur eigentlichen Konstruktion von $Y^{p,q}$.

Konstruktion

Sei q eine ungerade Primzahl, $q \neq p$.
Sei $\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$ die Reduktion modulo q. Sei $\psi_q : \mathbb{H}(\mathbb{F}_q) \to \mathbb{F}^{2\times 2}$ der Isomorphismus aus der Konstruktion von $X^{p,q}$. Also können wir über ψ_q die Einheitengruppe $\mathbb{H}(\mathbb{F}_q)^*$ mit $GL_2(q)$ identifizieren. Daraus folgt, dass Λ' auf $\mathbb{H}(\mathbb{F}_q)^*$ abgebildet wird, denn für $\alpha \in \Lambda'$ gilt nach der Konstruktion von $X^{p,q}$, dass $det(\psi_q(\tau_q(\alpha))) = N(\tau_q(\alpha)) = N(\alpha)\ mod\ q = p^l\ mod\ q$ für ein $l > 0$. Da $p^l\ mod\ q \neq 0$ in $\mathbb{F}_q$, folgt schon $\tau_q(\alpha) \in \mathbb{H}(\mathbb{F}_q)^*$.
Definiere nun $Z_q := \{\alpha \in \mathbb{H}(\mathbb{F}_q)^* \mid \alpha = \bar{\alpha}\} \subseteq \mathbb{H}(\mathbb{F}_q)^*$ Untergruppe.

1.4 Lemma Z_q ist ein Normalteiler in $\mathbb{H}(\mathbb{F}_q)^* \cong GL_2(q)$.

Beweis. Sei $\alpha \in Z_q$ beliebig. Dann existiert ein $\lambda \in \mathbb{F}_q$ mit $\psi_q(\alpha) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Sei nun $\beta \in \mathbb{H}(\mathbb{F}_q)^*$ beliebig, so folgt:

$$\psi_q(\beta\alpha\beta^{-1}) = \psi_q(\beta)\ \psi_q(\alpha)\ \psi_q(\beta^{-1}) = \psi_q(\beta)\lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \psi_q(\beta)^{-1} = \lambda\psi_q(\beta)\ \psi_q(\beta)^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \psi_q(\alpha)$$

Da ψ_q ein Isomorphismus ist, folgt $\beta\alpha\beta^{-1} = \alpha \in Z_q$ und damit ist Z_q ein Normalteiler. □

Setze $\Pi_q : \Lambda \to \mathbb{H}(\mathbb{F}_q)^*/Z_q$.

1.5 Lemma Π_q ist wohldefiniert.

Beweis. Für $\alpha, \beta \in \Lambda'$ mit $\alpha \sim \beta$ gilt $\tau_q(\alpha)^{-1}\tau_q(\beta) \in Z_q$. Seien dazu $n, m \in \mathbb{N} : p^m\alpha = \pm p^n\beta$, ohne Einschränkung $m > n \Rightarrow p^{m-n}\alpha = \pm\beta$. Dann folgt:

$$\begin{aligned}\tau_q(\alpha)^{-1}\tau_q(\beta) &= \tau_q(\alpha)^{-1}\tau_q(\mp p^{m-n}\alpha) \\ &= \tau_q(\alpha)^{-1}\tau_q(\alpha)(\mp p^{m-n}\ mod\ q) \\ &= \mp p^{m-n}\ mod\ q \in Z_q\end{aligned}$$

□

Setze $\Lambda(q) := ker(\Pi_q)$, dann folgt mit dem Homomorphiesatz $\Pi_q(\Lambda) \cong \Lambda/\Lambda(q)$. Also haben wir:

$$\begin{array}{ccc} \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^* \\ {\scriptstyle Q}\downarrow & & \downarrow \\ \Lambda & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^*/Z_q \end{array}$$

Setze nun

$$T_{p,q} := (\Pi_q \circ Q)(S_p) \text{ und } Y^{p,q} = \Gamma(\Lambda/\Lambda(q), T_{p,q}),$$

wobei wir $T_{p,q}$ als das Bild unter dem Isomorphismus $\Pi_q(\Lambda) \cong \Lambda/\Lambda(q)$ in $\Lambda/\Lambda(q)$ auffassen.

2 Eigenschaften von $Y^{p,q}$

Seien p, q weiter ungerade Primzahlen mit $p \neq q$.
Für $q > 2\sqrt(p)$ gilt $\#T_{p,q} = p + 1$ und aus $\Lambda =< Q(S_p) >$ folgt $\Lambda/\Lambda(q) =< T_{p,q} >$, damit ist $Y^{p,q}$ $(p+1)$-regulär und zusammenhängend.
Nun haben wir:

$$\begin{array}{ccccc} \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^* & \xrightarrow[\cong]{\psi_q} & GL_2(q) \\ {\scriptstyle Q}\downarrow & & \downarrow & & {\scriptstyle \varphi}\downarrow \\ \Lambda & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^*/Z_q & & PGL_2(q) \end{array}$$

Wobei ψ_q und φ aus der Konstruktion von $X^{p,q}$ stammen.
Dort haben wir definiert: $S_{p,q} := (\varphi \circ \psi_q \circ \tau_q)(S_p)$.
Es gilt $\psi_q(Z_q) = ker(\varphi)$, damit ist $GL(q)/\psi_q(Z_q) \to PGL_2(q)$ ein Isomorphismus. Definiere

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

dies ist nun ebenfalls ein Isomorphismus. Das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^* & \xrightarrow[\cong]{\psi_q} & GL_2(q) \\ \downarrow Q & & \downarrow & & \downarrow \varphi \\ \Lambda & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^*/Z_q & \xrightarrow[\cong]{\beta} & PGL_2(q) \end{array}$$

$$\Rightarrow \beta(T_{p,q}) = (\beta \circ \Pi_q \circ Q)(S_p) = (\varphi \circ \psi_q \circ \tau_q)(S_p) = S_{p,q}$$

Also können wir über β jede Ecke in $Y^{p,q}$ mit einer Ecke in $X^{p,q}$ identifizieren, und damit auch jeder Kante in $Y^{p,q}$ eine Kante in $X^{p,q}$ zuordnen. Da außerdem $Y^{p,q}$ zusammenhängend ist, folgt, dass $Y^{p,q}$ eine Zusammenhangskomponente von $X^{p,q}$ ist.

Nun betrachten wir $\Lambda(q)$ etwas genauer.

2.1 Lemma Es gilt $\Lambda(q) = \{[\alpha] \in \Lambda \mid \alpha = a_0 + a_1 i + a_2 j + a_3 k, q \mid a_1, a_2, a_3\}$.

Beweis. Es gilt $\Lambda(q) = ker(\Pi_q) = \{[\alpha] \in \Lambda \mid \Pi_q([\alpha]) = 1\} = \{\alpha \in \Lambda' \mid \tau_q(\alpha) \in Z_q\}$. Daraus folgt:

$$\begin{aligned} [\alpha] \in \Lambda(q) &\Leftrightarrow \tau_q(\alpha) \in Z_q \\ &\Leftrightarrow \tau_q(\alpha) = \overline{\tau_q(\alpha)} \\ &\Leftrightarrow \alpha \ mod\ q \equiv \bar{\alpha} \ mod\ q \\ &\Leftrightarrow q \nmid a_0 \ und\ q \mid a_1, a_2, a_3 \\ &\Leftrightarrow q \mid a_1, a_2, a_3 \end{aligned}$$

Wobei die Rückrichtung der letzten Äquivalenz gilt, da:

$$\begin{aligned} & q \mid a_1, a_2, a_3 \ und\ q \nmid N(\alpha) = p^l \\ \Rightarrow\ & q \mid a_1, a_2, a_3 \ und\ q \nmid a_0^2 + a_1^2 + a_2^2 + a_3^2 \\ \Rightarrow\ & q \mid a_1, a_2, a_3 \ und\ q \nmid a_0^2 \\ \Rightarrow\ & q \mid a_1, a_2, a_3 \ und\ q \nmid a_0 \end{aligned}$$

Also folgt insgesamt $[\alpha] \in \Lambda(q) \Leftrightarrow [\alpha] \in \{[\alpha] \in \Lambda \mid \alpha = a_0 + a_1 i + a_2 j + a_3 k, q \mid a_1, a_2, a_3\}$. □

Für den Beweis der nächsten Proposition benötigen wir noch diese Aussage:

2.2 Lemma Für $a, b \in \mathbb{Z}$ mit $q \nmid a,\ q \nmid b$ und $a^2 \equiv b^2\ mod\ q^2$, gilt $a \equiv \pm\ b\ mod\ q^2$.

Beweis.

$$\begin{aligned} a^2 \equiv b^2 \ mod\ q^2 \Leftrightarrow & q^2 \mid a^2 - b^2 \\ \Leftrightarrow & q^2 \mid (a+b)(a-b) \\ \Leftrightarrow & (q^2 \mid a+b) \vee (q^2 \mid a-b) \vee (q \mid a+b \ und\ q \mid a-b) \\ \Leftrightarrow & q^2 \mid a \pm b \\ \Leftrightarrow & a \equiv \pm\, b \ mod\ q^2 \end{aligned}$$

Der Fall $(q \mid a+b \ und\ q \mid a-b)$ tritt nicht ein, da aus $q \nmid a$ und $q \nmid b$ folgt, dass $q \nmid a+b$ und $q \nmid a-b$. □

Jetzt können wir den Umfang von $Y^{p,q}$ abschätzen:

2.3 Proposition Es gilt $g(Y^{p,q}) \geq 2 \cdot log_p(q)$.
Gilt zusätzlich, dass p nicht Quadrat modulo q ist, so gilt sogar $g(Y^{p,q}) \geq 4 \cdot log_p(q) - log_p(4)$.

Beweis. Setze $g = g(Y^{p,q})$. Sei $x_0, ..., x_g = x_0$ ein Kreis der Länge g in $Y^{p,q}$. Ohne Einschränkung können wir $x_0 = x_g = 1$ in $\Lambda/\Lambda(q)$ annehmen, da $Y^{p,q}$ Ecken-transitiv ist. Dann existieren $t_1, .., t_g \in T_{p,q}$ mit $x_i = t_1 \cdots t_i$ für $1 \leq i \leq g$. Da $T_{p,q} = \Pi_q(Q(S_p))$ existiert nun für jedes t_i ein $\gamma_i \in S_p \subseteq \Lambda'$ mit $t_i = \Pi_q([\gamma_i])$, γ_i ist eindeutig, da $Q|_{S_p}$ injektiv ist. Schreibe $\alpha = \gamma_1 \cdots \gamma_g \in \Lambda'$ als $\alpha = a_0 + a_1 i + a_2 j + a_3 k$, dann ist α ein reduziertes Wort über S_p und es gilt $[\alpha] = [\gamma_1 \cdots \gamma_g] = [\gamma_1] \cdots [\gamma_g] \neq [p]$ nach Proposition 1.3, also ist mindestens ein $a_l \neq 0$ für $l = 1, 2, 3$.
Außerdem gilt $\Pi_q([\alpha]) = t_1 \cdots t_g = x_g = 1 \Rightarrow [\alpha] \in ker(\Pi_q) = \Lambda(q)$, also mit Lemma 2.1 folgt $q \mid a_1, a_2, a_3 \Rightarrow q \leq a_1, a_2, a_3$. Nach Korollar 2.5.14 gilt $p^g = N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 \geq q^2$ $\Rightarrow g(Y^{p,q}) = g = log_p(p^g) \geq log_p(q^2) = 2 \cdot log_p(q)$.
Angenommen, nun ist p nicht Quadrat modulo q. Aus $p^g = N(\alpha),\ q \nmid a_0,\ q \mid a_1, a_2, a_3$ folgt $p^g \equiv a_0^2 \ mod\ q$, also $1 = (\frac{p^g}{q}) = (\frac{p}{q})^g = (-1)^g \Rightarrow g = 2h$. Es gilt also $p^{2h} \equiv a_0^2 \ mod\ q^2$, da $q^2 \mid a_1^2 + a_2^2 + a_3^2, q^2 \nmid a_0^2$ gilt $\Rightarrow p^h \equiv \pm\, a_0 \ mod\ q^2$ mit Lemma 2.2. Andererseits folgt aus $p^g = N(\alpha) \geq a_0^2 :\ |(a_0)| \leq p^h$.
Angenommen, es gilt $g > 4 \cdot log_p(q) - log_p(4) = log_p(\frac{q^4}{4})$.

$$\begin{aligned} g < log_p(\frac{q^4}{4}) \Leftrightarrow & p^g < \frac{q^4}{4} \\ \Leftrightarrow & (p^h)^2 < (\frac{q^2}{2})^2 \\ \Leftrightarrow & p^h < \frac{q^2}{2} \\ \Leftrightarrow & 2 \cdot p^h < q^2 \\ \Leftrightarrow & p^h + |a_0| < q^2 \end{aligned}$$

Da $|p^h \mp a_0| < p^h + |a_0|$ gilt, folgt $|p^h \mp a_0| < q^2$. Nun existiert ein $l \in \mathbb{Z}$ mit $p^h = l \cdot q^2 \pm a_0$. Damit gilt $p^h \mp a_0 = l \cdot q^2 \Rightarrow l = 0 \Rightarrow p^h = \pm a_0 \Rightarrow a_0^2 + a_1^2 + a_2^2 + a_3^2 = N(\alpha) = p^g = (p^h)^2 = a_0^2 \Rightarrow a_1 = a_2 = a_3 = 0$ ↯

$\Rightarrow g(Y^{p,q}) = g \geq 4 \cdot log_p(q) - log_p(4)$. □

2.4 Lemma Für eine Familie $(X_m)_{m\geq 1}$ von zusammenhängenden, k-regulären Graphen mit $\#V_m \to \infty$ für $m \to \infty$ gilt:

$$g(X_m) \leq (2 + o(1)) \cdot log_{k-1}(\#V_m)$$

wobei $o(1) \to 0$ für $m \to \infty$.
Gilt $k \geq 5$, so gilt:

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

2.5 Bemerkung Für $p \geq 5$ gilt mit Lemma 2.4: $g(Y^{p,q}) \leq 2 + 2 \cdot log_p(\#Y^{p,q})$.
Mit Proposition 2.3 folgt dann $\#Y^{p,q} \geq \frac{q}{p}$ und für p nicht Quadrat modulo q folgt sogar, $\#Y^{p,q} \geq \frac{q^2}{2p}$.
$\Rightarrow \#Y^{p,q} = \#(\Lambda/\Lambda(q))$ wächst mindestens linear mit q

Beweis.

$$\begin{aligned} 2 \cdot log_p(q) \leq g(Y^{p,q}) \leq 2 + 2 \cdot log_p(\#Y^{p,q}) &\Leftrightarrow log_p(q^2) \leq log_p(p^2) + log_p((\#Y^{p,q})^2) \\ &\Leftrightarrow log_p(g^2) \leq log_p(p^2 \cdot (\#Y^{p,q})^2) \\ &\Leftrightarrow q^2 \leq p^2 \cdot (\#Y^{p,q})^2 \\ &\Leftrightarrow \frac{q}{p} \leq \#Y^{p,q} \end{aligned}$$

Jetzt der Spezialfall p nicht Quadrat modulo q:

$$\begin{aligned} 4 \cdot log_p(q) - log_p(4) \leq 2 + 2 \cdot log_p(\#Y^{p,q}) &\Leftrightarrow log_p(\frac{q^4}{4}) \leq log_p(p^2 \cdot (\#Y^{p,q})^2) \\ &\Leftrightarrow (\frac{q^2}{2})^2 \leq p^2 \cdot (\#Y^{p,q})^2 \\ &\Leftrightarrow \frac{q^2}{2p} \leq \#Y^{p,q} \end{aligned}$$

□

3 Zusammenhang zwischen $Y^{p,q}$ und $X^{p,q}$

Seien p, q weiter ungerade Primzahlen mit $p \neq q$.

3.1 Erinnerung Wir benötigen nun die folgenden zwei Aussagen:

- Gilt $H \subsetneq PSL_2(q)$ und $\#H > 60$ für eine ungerade Primzahl q, so ist H metabelsch.

- G metabelsch $\Leftrightarrow [[g_1, g_2], [g_3, g_4]] = 1$ für alle $g_1, g_2, g_3, g_4 \in G$.

Jetzt werden wir unsere Ergebnisse auf $X^{p,q}$ übertragen.

3.2 Theorem Sei $p \geq 5$. Für $q > p^8$ ist $X^{p,q}$ zusammenhängend, und da $Y^{p,q}$ eine Zusammenhangskomponente von $X^{p,q}$, sind $X^{p,q}$ und $Y^{p,q}$ isomorph.

Beweis. Da gilt

$$X^{p,q} = \begin{cases} \Gamma(PSL_2(q), S_{p,q}) & \text{für p Quadrat modulo q} \\ \Gamma(PGL_2(q), S_{p,q}) & \text{für p nicht Quadrat modulo q} \end{cases}$$

müssen wir zeigen, dass $S_{p,q} = (\varphi \circ \psi_q \circ \tau_q)(S_p)$ $PSL_2(q)$ bzw. $PGL_2(q)$ erzeugt, denn dann folgt mit Proposition 4.1.2, dass $X^{p,q}$ zusammenhängend ist.
Betrachte dazu den Isomorphismus $\beta : \mathbb{H}(\mathbb{F}_q)^*/Z_q \to PGL_2(q)$. Da $\beta(T_{p,q}) = S_{p,q}$ reicht es

$$\beta(\Lambda/\Lambda(q)) = \begin{cases} PSL_2(q) & \text{für p Quadrat modulo q} \\ PGL_2(q) & \text{für p nicht Quadrat modulo q} \end{cases}$$

zu zeigen.
Wir wissen bereits aus der Konstruktion von $X^{p,q}$, dass $S_{p,q} \subseteq PSL_2(q)$, für p Quadrat modulo q und $S_{p,q} \subseteq PGL_2(q) - PSL_2(q)$, für p nicht Quadrat modulo q gilt, wobei wir mit $PSL_2(q)$ das Bild der Abbildung $SL_2(q) \to GL_2(q) \twoheadrightarrow PGL_2(q)$ in $PGL_2(q)$ meinen.
Setze $H_{p,q} := PSL_2(q) \cap \beta(\Lambda/\Lambda(q))$. Wir werden jetzt $H_{p,q} = PSL_2(q)$ zeigen.

Behauptung 1: $\#H_{p,q} > 60$.
Da $q > p^8$ und $p \geq 5$ folgt mit Bemerkung 2.5 $\#\Lambda/\Lambda(q) \geq \frac{q}{p} > 120 \Rightarrow \#\beta(\Lambda/\Lambda(q)) > 120$, weil β ein Isomorphismus ist.
Seien nun $g, h \in \beta(\Lambda/\Lambda(q)) - PSL_2(q)$, also $g, h \notin H_{p,q}$. Da $PGL_2(q)/PSL_2(q) \cong \{\pm 1\}$ impliziert $g, h \notin PSL_2(q)$, dass $g \equiv h \ mod \ PSL_2(q)$ gilt. Daraus folgt, dass ein $a \in PSL_2(q)$ existiert mit $g = ah \Rightarrow gh^{-1} = a \in \beta(\Lambda/\Lambda(q)) \cap PSL_2(q) = H_{p,q}$.
Gilt nun $\#(\beta(\Lambda/\Lambda(q)) - PSL_2(q)) = n$, so finden wir für alle $g \in \beta(\Lambda/\Lambda(q)) - PSL_2(q)$ und alle $h \in \beta(\Lambda/\Lambda(q)) - PSL_2(q)$ ein $a \in PSL_2(q)$ mit $a = gh^{-1} \in H_{p,q}$, also gibt es in $H_{p,q}$ mindestens genauso viele Elemente wie in $\beta(\Lambda/\Lambda(q)) - PSL_2(q)$.
$\Rightarrow \#H_{p,q} = \#(\beta(\Lambda/\Lambda(q)) \cap PSL_2(q)) \geq n = \#(\beta(\Lambda/\Lambda(q)) - PSL_2(q))$
Also folgt insgesamt

$$\begin{aligned} 2 \cdot \#H_{p,q} &\geq \#H_{p,q} + \#(\beta(\Lambda/\Lambda(q)) - PSL_2(q)) \\ &= \#(\beta(\Lambda/\Lambda(q)) \cap PSL_2(q)) + \#(\beta(\Lambda/\Lambda(q)) - PSL_2(q)) \\ &= \#\beta(\Lambda/\Lambda(q)) \\ &> 120 \end{aligned}$$

und damit $\#H_{p,q} > 60$.

Behauptung 2: $H_{p,q}$ ist nicht metabelsch
1. Fall *p Quadrat modulo q*: Es gilt $S_{p,q} \subseteq PSL_2(q)$ und $S_{p,q} = \beta(T_{p,q}) \subseteq \beta(\Lambda/\Lambda(q)) \Rightarrow S_{p,q} \subseteq H_{p,q}$.
Wähle nun $g_1 \in S_{p,q}, g_2 \in S_{p,q} - \{g_1, g_1^{-1}\}, g_4 \in S_{p,q} - \{g_1, g_1^{-1}, g_2, g_2^{-1}\}$ beliebig und setze $g_3 = g_1$.
Dann folgt das

$$[[g_1, g_2], [g_3, g_4]] = [g_1 g_2 g_1^{-1} g_2^{-1}, g_1 g_4 g_1^{-1} g_4^{-1}] = g_1 g_2 g_1^{-1} g_2^{-1} \ g_1 g_4 g_1^{-1} g_4^{-1} \ g_2 g_1 g_2^{-1} g_1^{-1} \ g_4 g_1 g_4^{-1} g_1^{-1}$$

ein reduziertes Wort der Länge 16 über $S_{p,q}$ ist. Da aber $g(Y^{p,q}) \geq 2 \cdot log_p(q) > 16$ gilt, folgt $[[g_1, g_2], [g_3, g_4]] \neq 1$, denn sonst hätte man einen Kreis mit Länge 16 in $Y^{p,q}$.
2. Fall *p nicht Quadrat modulo q*: Wähle $h_1 \in S_{p,q}$ beliebig, $h_2 \in S_{p,q} - \{h_1, h_1^{-1}\}$ und $h_3 \in S_{p,q} - \{h_1, h_1^{-1}, h_2, h_2^{-1}\}$. Setze nun $g_1 = h_1h_3,\ g_2 = h_2h_3,\ g_3 = h_1h_2,\ g_4 = h_3h_2$, da $S_{p,q} \subseteq PGL_2(q) - PSL_2(q)$, aber $PSL_2(q)$ Index 2 in $PGL_2(q)$ hat und $S_{p,q} \subseteq \beta(\Lambda/\Lambda(q))$ folgt $g_1, g_2, g_3, g_4 \in H_{p,q}$. Damit folgt nun das

$$\begin{aligned}[[g_1, g_2], [g_3, g_4]] &= g_1g_2g_1^{-1}g_2^{-1}\ g_3g_4g_3^{-1}g_4^{-1}\ g_2g_1g_2^{-1}g_1^{-1}\ g_4g_3g_4^{-1}g_3^{-1} \\ &= h_1h_3h_2h_1^{-1}h_3^{-1}h_2^{-1}\ h_1h_2h_3h_1^{-1}h_2^{-1}h_3^{-1}\ h_2h_3h_1h_2^{-1}h_3^{-1}h_1^{-1}\ h_3h_2h_1h_3^{-1}h_2^{-1}h_1^{-1}\end{aligned}$$

ein reduziertes Wort der Länge 24 über $S_{p,q}$ ist. Da außerdem $g(Y^{p,q}) \geq 4 \cdot log_p(q) - log_p(4) > 24$ gilt, folgt analog wie im ersten Fall $[[g_1, g_2], [g_3, g_4]] \neq 1$.
$\Rightarrow H_{p,q}$ ist nicht metabelsch

Jetzt muss aber schon $H_{p,q} = PSL_2(q)$ gelten. Denn angenommen, $H_{p,q} \subsetneq PSL_2(q)$, dann folgt, dass $H_{p,q}$ metabelsch ist $\lightning$.
Damit gilt $PSL_2(q) = H_{p,q} = PSL_2(q) \cap \beta(\Lambda/\Lambda(q))$, also insbesondere $PSL_2(q) \subseteq \beta(\Lambda/\Lambda(q))$.

Dann folgt für die beiden Fälle:
1. Fall *p Quadrat modulo q*: Es gilt $S_{p,q} \subseteq PSL_2(q)$, daraus folgt $< S_{p,q} > \subseteq PSL_2(q)$. Da $< S_{p,q} > = \beta(\Lambda/\Lambda(q))$, folgt $\beta(\Lambda/\Lambda(q)) \subseteq PSL_2(q)$, also $PSL_2(q) = \beta(\Lambda/\Lambda(q))$.
2. Fall *p nicht Quadrat modulo q*: Es gilt

$$\beta(\Lambda/\Lambda(q)) \subseteq PGL_2(q),\ S_{p,q} \subseteq PGL_2(q) - PSL_2(q) \Rightarrow < S_{p,q} > \not\subseteq PSL_2(q).$$

Dann existiert $g \in \beta(\Lambda/\Lambda(q)) - PSL_2(q) \Leftrightarrow g \not\equiv 1\ mod\ PSL_2(q)$.
Sei nun $h \in PGL_2(q)$ beliebig. Da $PGL_2(q)/PSL_2(q) \cong \{\pm 1\}$ gilt entweder

$$h \equiv 1\ mod\ PSL_2(q) \Rightarrow h \in PSL_2(q) \subseteq \beta(\Lambda/\Lambda(q))$$

oder

$$h \equiv g\ mod\ PSL_2(q) \Rightarrow \exists\ a \in PSL_2(q) : h = g \cdot a \in \beta(\Lambda/\Lambda(q)).$$

Also folgt $h \in \beta(\Lambda/\Lambda(q))$ und damit $PGL_2(q) \subseteq \beta(\Lambda/\Lambda(q)) \Rightarrow \beta(\Lambda/\Lambda(q)) = PGL_2(q)$.
Somit ist $X^{p,q}$ zusammenhängend und damit isomorph zu $Y^{p,q}$. □

Nun als Zusammenfassung folgendes Korollar:

3.3 Korollar Angenommen, es gilt $q > p^8$. Dann sind die Graphen $X^{p,q}$ $p+1$-regulär und zusammenhängend. Außerdem gilt

(i) für p Quadrat modulo q: $X^{p,q}$ ist nicht bipartit und $g(X^{p,q}) \geq \frac{2}{3} \cdot log_p(\#X^{p,q})$

(ii) für p nicht Quadrat modulo q: $X^{p,q}$ ist bipartit und $g(X^{p,q}) \geq \frac{4}{3} \cdot log_p(\#X^{p,q}) - log_p(4)$

Beweis. $X^{p,q}$ $p+1$-regulär und zusammenhängend folgt direkt aus Theorem 3.2. Außerdem gilt

$$\#X^{p,q} = \begin{cases} \#PSL_2(q) & \text{für p Quadrat modulo q} \\ \#PGL_2(q) & \text{für p nicht Quadrat modulo q} \end{cases} \leq q(q^2-1) \leq q^3$$

(i) Es gilt $g(X^{p,q}) \geq 2 \cdot log_p(q) = \frac{2}{3} \cdot log_p(q^3) \geq \frac{2}{3} \cdot log_p(\#X^{p,q})$.
Angenommen, $X^{p,q}$ wäre bipatit, dann existiert nach Proposition 4.1.2 ein Homomorphismus $\mathcal{X} : PSL_2(q) \to \{\pm 1\}$ mit $\mathcal{X}(S_{p,q}) = \{-1\}$. Da $PSL_2(q)$ einfach ist, ist jeder Homomorphismus $PSL_2(q) \to \{\pm 1\}$ konstant oder injektiv. Damit ist $\mathcal{X}$ konstant, also $\mathcal{X}(PSL_2(q)) = \{1\} \Rightarrow \mathcal{X}(S_{p,q}) = \{1\}\lightning$ dazu, dass $\mathcal{X}(S_{p,q}) = \{-1\}$ gilt. Damit ist $X^{p,q}$ nicht bipartit.

(ii) Es gilt $g(X^{p,q}) \geq 4 \cdot log_p(q) - log_p(4) = \frac{4}{3} \cdot log_p(q^3) - log_p(4) \geq \frac{4}{3} \cdot log_p(\#X^{p,q}) - log_p(4)$.
Sei $\mathcal{X} : PGL_2(q) \to PGL_2(q)/PSL_2(q) \cong \{\pm 1\}$ kanonisch. Da $S_{p,q} \subseteq PGL_2(q) - PSL_2(q)$ folgt schon $\mathcal{X}(S_{p,q}) = \{-1\}$, also ist $X^{p,q}$ nach Proposition 4.1.2 bipartit.

□