ISRAEL JOURNAL OF MATHEMATICS **133** (2003), 29–44

# THE MINIMUM INDEX OF A NON-CONGRUENCE SUBGROUP OF $\mathrm{SL}_2$ OVER AN ARITHMETIC DOMAIN

BY

A. W. MASON

*Department of Mathematics, University of Glasgow*
*Glasgow G12 8QW, Scotland, U.K.*
*e-mail: awm@maths.gla.ac.uk*

AND

ANDREAS SCHWEIZER

*Korea Institute for Advanced Study (KIAS)*
*207-43 Cheongryangri-dong, Dongdaemun-gu*
*Seoul 130-012, Korea*
*e-mail: schweiz@kias.re.kr*

ABSTRACT

Let $A$ be an arithmetic Dedekind ring with only finitely many units. It is known that (i) $A = \mathbb{Z}$, the ring of rational integers, (ii) $A = \mathcal{O}_d$, the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$, where $d$ is a square-free positive integer, or (iii) $A = \mathcal{C} = \mathcal{C}(C, P, k)$, the coordinate ring of the affine curve obtained by removing a closed point $P$ from a smooth projective curve $C$ over a *finite* field $k$. Serre has shown that, in comparison with other low rank arithmetic groups, the groups $\mathrm{SL}_2(A)$ have "many" non-congruence subgroups.

Let $\mathrm{ncs}(A)$ denote the smallest index of a non-congruence subgroup of $\mathrm{SL}_2(A)$. It is well-known that $\mathrm{ncs}(\mathbb{Z}) = 7$. Grunewald and Schwermer have proved that, with 4 exceptions, $\mathrm{ncs}(\mathcal{O}_d) = 2$. In this paper we prove that $\mathrm{ncs}(\mathcal{C}) = 2$, for "most", but not all, $\mathcal{C}$.

Received June 14, 2001

## Introduction

Let $G$ be an algebraic group over a global field $F$ and let $A$ be an arithmetic Dedekind domain contained in $F$. The problem of determining whether or not the group $G(A)$ has subgroups of finite index which are not congruence subgroups (the celebrated *Congruence Subgroup Problem*) has attracted much attention for many years. It is known that, if the rank of $G$ is "sufficiently high", then every subgroup of finite index is "within bounded index" of a congruence subgroup. For example Bass, Milnor and Serre [1] have proved that, for the cases $G = \mathrm{SL}_n$, where $n \geq 3$, and $G = \mathrm{Sp}_{2n}$, where $n \geq 2$, there exists a constant $c = c(A)$ with the following property. For each subgroup $S$ of finite index in $G(A)$ (for these cases), there exists a congruence subgroup $S'$ containing $S$ such that $|S' : S| \leq c$. (For many $A$, including $A = \mathbb{Z}$, the ring of rational integers, it is known that $c(A) = 1$.) For a result of this type to extend to low rank $G$ it is usually necessary to impose some restrictions on $A$. For example, Liehl [6] and Vaserstein [14] have proved that the above result holds for $\mathrm{SL}_2(A)$, provided $A$ has infinitely many units. It is known that $A$ has only finitely many units if and only if (i) $A = \mathbb{Z}$, (ii) $A = \mathcal{O}_d$, the ring of integers of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$, where $d$ is a square-free positive integer, or (iii) $A = \mathcal{C} = \mathcal{C}(C, P, k)$, the coordinate ring of the affine curve obtained by removing a closed point $P$ from a smooth projective curve $C$ over a *finite* field $k$. Serre [11] uses the theory of profinite groups to show that when $A$ is of type (i), (ii) or (iii) the set of non-congruence subgroups of $\mathrm{SL}_2(A)$ is much more complicated. (In particular no constant $c(A)$ of the above type exists for these cases.)

Let $\mathcal{N}(A)$ denote the set of non-congruence subgroups of $\mathrm{SL}_2(A)$. After [5] we put

$$\mathrm{ncs}(A) := \min\{|\,\mathrm{SL}_2(A) : S| : S \in \mathcal{N}(A)\}.$$

It is clear that $\mathrm{ncs}(A) \geq 2$. It is well-known that $\mathrm{ncs}(\mathbb{Z}) = 7$. Grunewald and Schwermer [5] have proved that $\mathrm{ncs}(\mathcal{O}_d) = 2$, when $d \neq 1, 2, 3$ or 7. (They also evaluate $\mathrm{ncs}(\mathcal{O}_d)$ for the remaining 4 cases. The largest is $\mathrm{ncs}(\mathcal{O}_3) = 22$.) In this paper we prove that a similar situation holds for $\mathrm{SL}_2(\mathcal{C})$. We prove that $\mathrm{ncs}(\mathcal{C}) = 2$, for "most", but not all, $\mathcal{C}$.

Let $K$ be the algebraic function field of $C$. We assume that $k$ is algebraically closed in $K$. Let $q$ be the cardinality of $k$, $g(\geq 0)$ the **genus** of $K$ and $\delta(\geq 1)$ the **degree** of $P$. (Stichtenoth's book [13] provides an excellent account of the algebraic theory of function fields.) Our principal result is the following.

THEOREM: *With the above notation,*

$\mathrm{ncs}(\mathcal{C}) > 2$ *if and only if*

(i) $(g, \delta) = (0,1), (0,2)$ *and* $q \neq 2$

*or*

(ii) $(g, \delta) = (0,3), (1,1)$ *and* $4|q$.

It follows, for example, that $\mathrm{ncs}(\mathcal{C}) = 2$ when $g > 1$, $\delta > 3$ or $q = 2$. Our proof is based on the action of $\mathrm{GL}_2(\mathcal{C})$ on its *Bruhat–Tits building* [12, Chapter II], and makes use of formulae of Gekeler [2] for the genera of various Drinfeld modular curves.

## 1. Unipotent matrices and non-congruence subgroups

From now on we put

$$G := \mathrm{GL}_2(\mathcal{C}) \quad \text{and} \quad \Gamma := \mathrm{SL}_2(\mathcal{C}).$$

The group $G$ acts on a tree $X$, its *Bruhat–Tits building* [12, Chapter II, §1]. For each subgroup $S$ of $G$ and each vertex $v$ of $X$, we denote the **stabilizer** of $v$ in $S$ by $S_v$. We put

$$S_X = \langle S_v : v \in \mathrm{vert}(X) \rangle.$$

Our first lemma is a consequence of the basic theory of groups acting on trees. We denote the free group of (finite) rank $n$ by $F_n$.

LEMMA 1.1: *Let $S$ be a subgroup of finite index in $G$. Then*

$$S/S_X \cong F_r,$$

*where* $r = \mathrm{rk}_{\mathbb{Z}}(S) = \dim_{\mathbb{Q}} H^1(S, \mathbb{Q}) < \infty$.

*Proof:* By [12, Corollary 1, p. 55] it follows that

$$S/S_X \cong \pi_1(S\backslash X),$$

where $\pi_1(S\backslash X)$ is the fundamental group of the (connected) quotient graph $S\backslash X$. This is a free group with a set of free generators in one-one correspondence with a set of edges of $S\backslash X$ *not* on a given spanning tree. By [12, Theorem 9, p. 106], together with [12, Corollary 4, p. 108], the rank, $r$, of this group is finite.

By [12, Proposition 2, p. 76] each stabilizer $S_v$ is finite. The rest of the lemma follows. ∎

Again by [12, Proposition 2, p. 76] it follows that $\mathrm{rk}_{\mathbb{Z}}(S)$ is zero if and only if $S$ is generated by elements of finite order.

We note that Lemma 1.1 applies in particular to $S = \Gamma$, since $|G : \Gamma| = q - 1$. We recall that a **congruence subgroup** of $\Gamma$ is by definition one containing a (normal) subgroup of the type

$$\Gamma(\mathfrak{q}) := \{T \in \Gamma : T \equiv I_2 (\mathrm{mod}\, \mathfrak{q})\},$$

where $\mathfrak{q}$ is a non-zero $\mathcal{C}$-ideal. Since $\mathcal{C}/\mathfrak{q}$ is finite, it follows that congruence subgroups have finite index in $\Gamma$.

A two-by-two matrix $M$ over $\mathcal{C}$ is called **unipotent** if and only if $(M - I_2)^2 = 0$ (equivalently, $\det M = 1$ and $\mathrm{tr}\ M = 2$). Let $U$ denote the subgroup of $\Gamma$ generated by all the unipotent matrices. We now come to the principal result of this section.

THEOREM 1.2: *Suppose that* $\mathrm{rk}_{\mathbb{Z}}(\Gamma) > 0$. *Then*

$$\mathrm{ncs}(\mathcal{C}) = 2.$$

*Proof:* As above let $r = \mathrm{rk}_{\mathbb{Z}}(\Gamma)$. Each unipotent matrix has finite order $p = \mathrm{char}\, k$ and so by Lemma 1.1 there exists an epimorphism

$$\theta \colon \Gamma/U \twoheadrightarrow F_r.$$

It follows that, for each $n > 0$, there exists a (normal) subgroup $S$ of $\Gamma$, containing $U$, such that

$$|\Gamma : S| = n.$$

Now $U$ is a normal subgroup of $\Gamma$ containing all the elementary matrices and so the only *congruence* subgroup of $\Gamma$ containing $U$ is $\Gamma$ itself, by [8, Corollary 1.3]. The result follows. ∎

A similar argument, involving the elementary matrices, is used in the proof of [5, 3.1. Proposition]. (See also the proof of [4, Theorem 1.4].)

## 2. Non-zero rank

In this section we use formulae of Gekeler [2], [3] (for the genera of various Drinfeld modular curves) to prove that $\mathrm{rk}_{\mathbb{Z}}(\Gamma)$ is non-zero, for "most" $\mathcal{C}$. We recall the definition [13, p. 165] of the **$L$-polynomial** $P(t)$ of the algebraic function field $K/k$. This is a polynomial of degree $2g$ over $\mathbb{Z}$. It is known [13, V.1.15, p. 166] that

$$P(t) = \prod_{i=1}^{g} (qt^2 - \lambda_i t + 1),$$

for some $\lambda_i \in \mathbb{R}$, where $|\lambda_i| \leq 2\sqrt{q}(1 \leq i \leq g)$. It follows that, if $P(\alpha) = 0$, then $|\alpha| = q^{-1/2}$. This implies that $P(n) > 0$, for all $n \in \mathbb{Z}$.

*Notation:* For each $n \in \mathbb{N}$, let

$$A(n,q) = \frac{(q^n-1)}{(q-1)}P(q) - \frac{nq(q+1)}{2}P(1) - \frac{(1-(-1)^n)q(q-1)}{4}P(-1)$$

and

$$B(n,q) = \frac{2(q^n-1)}{(q-1)}P(q) - \frac{n(q+1)^2}{2}P(1) - \frac{(1-(-1)^n)(q-1)^2}{4}P(-1).$$

It is easily verified that $A(n,q), B(n,q) \in \mathbb{Z}$ and that

$$A(n,q) \equiv B(n,q) \equiv 0(\mathrm{mod}(q^2-1)).$$

We put

$$\mathrm{r}(n,q) = \begin{cases} 1 + (q^2-1)^{-1}A(n,q), & q \text{ even}, \\ 1 + (q^2-1)^{-1}B(n,q), & q \text{ odd}. \end{cases}$$

THEOREM 2.1 (Gekeler):

$$\mathrm{r}(\delta,q) = \dim_{\mathbb{Q}} H^1(\Gamma,\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}(\Gamma).$$

*Proof:* See [2], [3, 5.8 Theorem, p. 73] and Lemma 1.1. ∎

We will prove that $A(\delta,q), B(\delta,q) \geq 0$, for "most" $\mathcal{C}$. We require the following properties of $P(t)$ and $\mathrm{r}(n,q)$.

LEMMA 2.2: *Suppose that $g \neq 0$. Then*

(i) *$P(q) > q^g P(1)$, for all $q$,*

*and*

(ii) *$P(q) > q^g P(-1)$, for all $q > 3$.*

*Proof:* With the above notation, it is clear that, for each $i$,

$$q^3 - \lambda_i q + 1 > q(q - \lambda_i + 1),$$

and that, when $q \geq 4$,

$$q^3 - \lambda_i q + 1 > q(q + \lambda_i + 1). \quad ∎$$

LEMMA 2.3: *Suppose that $m-n=2\alpha$, where $\alpha \in \mathbb{N}$, and that either $(g,m,n) \neq (0,3,1)$ or $q$ is odd. Then*

$$\mathrm{r}(m,q) > \mathrm{r}(n,q).$$

*Proof:* We consider only the case where $q$ is even. For odd $q$ the proof is very similar. It is clearly sufficient to deal with the case $\alpha = 1$ only. Then $\mathrm{r}(m,q) \geq \mathrm{r}(n,q)$ if and only if

$$\frac{(q^m - q^n)}{(q-1)} P(q) - q(q+1)P(1) > 0.$$

We now apply Lemma 2.2(i). ∎

We begin with the simplest case.

LEMMA 2.4: *Suppose that $g=0$. Then*

$$\mathrm{r}(\delta,q) > 0$$

*unless $(g,\delta) = (0,1), (0,2)$ or, when $q$ is even, $(g,\delta) = (0,3)$.*

*Proof:* Follows easily from the above formulae together with Lemma 2.3. ∎

We will treat the cases $q$ odd, $q$ divisible by 4 and $q=2$ separately.

LEMMA 2.5: *Suppose that $q$ is odd and that $g \neq 0$. Then*

$$\mathrm{r}(\delta,q) > 0.$$

*Proof:* Suppose that $\mathrm{r}(\delta,q) = 0$. Then, by Theorem 2.1, $\mathrm{rk}_{\mathbb{Z}}(\Gamma) = 0$ and so $\mathrm{rk}_{\mathbb{Z}}(G) = 0$. Now Gekeler [2] has proved that

$$\mathrm{rk}_{\mathbb{Z}}(G) = 1 + (q^2-1)^{-1} A(\delta,q).$$

It follows that

$$A(\delta,q) = B(\delta,q) = 1 - q^2,$$

and hence that

$$2\delta P(1) + (1-(-1)^{\delta})P(-1) = 4.$$

When $\delta$ is even we deduce that $\delta = 2$, $P(1) = 1$ and hence that $P(q) = 1$. On the other hand, if $\delta$ is odd, then $\delta = P(1) = P(-1) = 1$, and so $P(q) = 1$. Either conclusion contradicts Lemma 2.2. ∎

LEMMA 2.6: *Suppose that $q = 4$ and that $g \neq 0$. Then*

$$r(\delta, 4) > 0,$$

*unless $(g, \delta) = (1, 1)$.*

*Proof:* By Lemma 2.3 we only have to consider the cases $\delta = 1, 2$. From the above formulae

$$r(2, 4) > 0 \quad \text{if and only if} \quad P(4) \geq 4P(1).$$

We now apply Lemma 2.2(i).

It is clear that

$$r(1, 4) > 0 \quad \text{if and only if} \quad P(4) \geq 10P(1) + 6P(-1).$$

The latter inequality is satisfied when $g \geq 2$, by Lemma 2.2. On the other hand, it is easily verified that

$$r(1, 4) = 0,$$

when $g = 1$. ∎

There remains the (much more complicated) case $q = 2$. We begin with a number of straightforward subcases.

LEMMA 2.7: *Suppose that $g \neq 0$ and that $\delta$ is even. Then*

$$r(\delta, 2) > 0.$$

*Proof:* Follows from Theorem 2.1 and Lemmata 2.2 and 2.3. ∎

LEMMA 2.8: *Suppose that $g = 1$ or 2 and that $\delta$ is odd. Then*

$$r(\delta, 2) = 0 \quad \textit{if and only if} \quad g = \delta = 1.$$

*Proof:* Suppose that $g = 1$. As in the proof of Lemma 2.6 it is easily verified that

$$r(1, 2) = 0.$$

We now apply Lemma 2.3.

Suppose now that $g = 2$. Then

$$P(t) = (2t^2 - \alpha t + 1)(2t^2 - \beta t + 1),$$

for some $\alpha, \beta \in \mathbb{R}$, with $|\alpha|, |\beta| \le 2\sqrt{2}$. Now

$$P(2) - 3P(1) - P(-1) = 45 - 12(\alpha + \beta).$$

But, by [13, V.1.15, (d), (3), p. 166], we have

$$\alpha + \beta \le 3.$$

The result follows by Lemma 2.3. ∎

This leaves one case.

Lemma 2.9: *Suppose that $g > 2$ and that $\delta$ is odd. Then*

$$\mathrm{r}(\delta, 2) > 0.$$

*Proof:* By Lemma 2.3 it suffices to prove that

$$E = P(2) - 3P(1) - P(-1) \ge 0.$$

We recall that

$$P(t) = \prod_{i=1}^{g}(2t^2 - \lambda_i t + 1) = \prod_{i=1}^{g} P_i(t).$$

It follows that

$$(*) \qquad \lambda_1 + \lambda_2 + \cdots + \lambda_g \le 3,$$

by [13, V.1.15, (d), (3), p. 166].

We put

$$Q_i := \frac{P_i(2)}{P_i(-1)} = \frac{15}{3 + \lambda_i} - 2 \quad \text{and} \quad R_i := \frac{P_i(2)}{P_i(1)} = 2 + \frac{3}{3 - \lambda_i}.$$

We recall that $-2\sqrt{2} \le \lambda_i \le 2\sqrt{2}$.

It is easily verified that

$$\begin{aligned}
\frac{1}{2} < Q_i < 1 &\quad \text{when } 2 < \lambda_i \le 2\sqrt{2},\\
1 < Q_i < 3 &\quad \text{when } 0 < \lambda_i < 2,\\
3 < Q_i < 5 &\quad \text{when } -6/7 < \lambda_i < 0,\\
5 < Q_i &\quad \text{when } -2\sqrt{2} \le \lambda_i < -6/7.
\end{aligned}$$

We assume that

$$\lambda_1 \le \lambda_2 \le \cdots \le \lambda_g.$$

We denote the number of $\lambda_i$ with $\lambda_i > 2$ by $u$, the number with $-\frac{6}{7} \le \lambda_i \le 0$ by $v$ and the number with $\lambda_i < -\frac{6}{7}$ by $w$. It follows that

$$\frac{P(2)}{P(-1)} \ge \frac{5^w 3^v}{2^u}.$$

In addition we have

$$2u - \frac{6}{7}v - 2\sqrt{2}w \le 3, \tag{$**$}$$

by $(*)$.

Suppose now that $u = 0$. Then $\lambda_1 \le 1$, since $g > 2$. It follows that

$$Q_1 \ge \frac{7}{4} \quad \text{and that} \quad Q_i \ge 1 \quad (i \ne 1).$$

Hence

$$\frac{P(2)}{P(-1)} \ge \frac{7}{4}.$$

On the other hand, $R_i > 2$ and so

$$\frac{3}{7}P(2) - 3P(1) > 0,$$

by Lemma 2.2. In this case therefore

$$E = \Big(\frac{3}{7}P(2) - 3P(1)\Big) + \Big(\frac{4}{7}P(2) - P(-1)\Big) > 0.$$

We suppose from now on that $u > 0$. It follows that $\lambda_g > 2$ and hence that

$$R_g > 5.$$

On the other hand, $-2\sqrt{2} \le \lambda_i$ and so

$$R_i \ge 11 - 6\sqrt{2} \quad (i \ne g).$$

Since $g > 2$, it follows that

$$\frac{P(2)}{P(1)} \ge 25$$

and hence that

$$\frac{1}{8}P(2) - 3P(1) > 0.$$

To prove that $E > 0$ it suffices therefore to show that

$$\frac{7}{8}P(2) - P(-1) \ge 0.$$

Suppose then that $P(2) < \frac{8}{7}P(-1)$. Then $5^w 3^v 2^{-u} < \frac{8}{7}$ and so

$$w \log_2(5) + v \log_2(3) < u + 3 - \log_2(7).$$

By the inequality (**) it follows that

$$(\log_2(5) - \sqrt{2})w + \Big(\log_2(3) - \frac{3}{7}\Big)v \leq \frac{9}{2} - \log_2(7).$$

We now make use of the estimates

$$\sqrt{2} < \frac{3}{2} < \log_2(3), \quad \frac{9}{4} < \log_2(5) \quad \text{and} \quad \frac{5}{2} < \log_2(7)$$

to deduce that

$$\frac{3}{4}w + \frac{15}{14}v < 2.$$

Clearly this inequality leaves only finitely many possibilities for $v$ and $w$. There are then only finitely many possibilities for $u$, by (**). We list these.

If $w = v = 1$, it follows that $u \leq 3$ and hence that $P(2)/P(-1) \geq \dfrac{15}{8}$.

If $v = 1$ and $w = 0$, it follows that $u \leq 1$ and hence that $P(2)P(-1) \geq \dfrac{3}{2}$.

If $v = 0$ and $w = 1$, it follows that $u \leq 2$ and hence that $P(2)/P(-1) \geq \dfrac{5}{4}$.

If $v = 0$ and $w = 2$, it follows that $u \leq 4$ and hence that $P(2)/P(-1) \geq \dfrac{25}{16}$.

The remaining case $v = w = 0$ and $u = 1$ is not quite so straightforward. Since $\lambda_g > 2$, it follows that $\lambda_1 < \frac{1}{2}$ (since $g > 2$). If $\lambda_g \leq \frac{5}{2}$, then

$$P(2)/P(-1) \geq Q_1 Q_g \geq \frac{16}{17} \cdot \frac{8}{11} > \frac{8}{7}.$$

If $\lambda_g > \frac{5}{2}$, then $\lambda_1 \leq \frac{1}{4}$ and so

$$P(2)/P(-1) \geq Q_1 Q_g \geq \frac{17}{13} > \frac{8}{7}.$$

This completes the proof. ∎

Combining Lemmata 2.4–2.9 we have the following result.

THEOREM 2.10: *With the above notation,* $\mathrm{r}(\delta, q) = 0$ *if and only if*

(i) $(g, \delta) = (0, 1), (0, 2)$

*or*

(ii) $(g, \delta) = (0, 3), (1, 1)$ *and* $2|q$.

## 3. Zero rank

In this section we examine the cases where $\mathrm{rk}_{\mathbb{Z}}(\Gamma)$ is zero in more detail. We begin, however, with a result which does not depend on the actual value of the rank.

LEMMA 3.1:
*(i) If* $q = 2$, *then* $\mathrm{ncs}(\mathcal{C}) = 2$.
*(ii) If* $q = 3$, *then* $\mathrm{ncs}(\mathcal{C}) \leq 3$.

*Proof:* For any subring $R$ of $\mathcal{C}$ let

$$E(R) = \left\{ \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} : r \in R \right\}.$$

From Serre's theorem [12, Theorem 10, p. 119] it follows [7, Theorem 1.2] that, when $q = 2$ or 3, there exists a proper subgroup $X$ of $\Gamma$ such that

$$\Gamma = X *_I Y,$$

where $Y = Z \cdot E(\mathcal{C})$ and $I = X \cap Y = Z \cdot E(k)$, with $Z = \{\pm I_2\}$.

We deduce that there exists an epimorphism

$$\phi \colon \Gamma \twoheadrightarrow V^+,$$

where $V^+$ is the additive group of $V$, a complement of the $k$-vector space $k$ in the $k$-vector space $\mathcal{C}$. Since $V$ has countably infinite dimension (over $k$), $V$ has uncountably many hyperplanes. Hence $\Gamma$ has uncountably many (normal) subgroups of index $q$.

Since $\mathcal{C}$ is a Dedekind ring, every $\mathcal{C}$-ideal is 2-generated. There are therefore only countably many $\mathcal{C}$-ideals and hence only countably many congruence subgroups of $\Gamma$. The result follows. ∎

The inequality in part (ii) is best possible. By Theorems 1.2 and 2.10 it is clear, for example, that $\mathrm{ncs}(\mathcal{C}) = 2$, when $q = 3$, if either $g > 1$ or $\delta > 3$. On the other hand, equality here is possible. (See below.)

The group $\Gamma$ acts as a group of linear fractional transformations on $\hat{K} = K \cup \{\infty\}$ in the usual way. For each $s \in \hat{K}$ we denote the stabilizer of $s$ in $\Gamma$ by $F(s)$. Then $F(\infty)$ (resp. $F(0)$) is the set of upper (resp. lower) triangular matrices in $\Gamma$. It is known [9, Theorem 2.1] that, when $s \in K^*$, an element $f \in F(s)$ if and only if

$$f = m_s(\alpha, c) = \begin{bmatrix} \alpha + cs & d \\ c & \alpha^{-1} - cs \end{bmatrix},$$

for some $\alpha \in k^*$, $c, d \in \mathcal{C}$, where $d = (\alpha^{-1} - \alpha)s - cs^2$. For each $\alpha \in k^*$, $c \in \mathcal{C}$ we put

$$m_\infty(\alpha, c) = (m_0(\alpha, c))^T = \begin{bmatrix} \alpha & c \\ 0 & \alpha^{-1} \end{bmatrix}.$$

It is clear that $m_s(\alpha, c)$ has eigenvalues $\alpha, \alpha^{-1}$. When $\alpha \neq \pm 1$ it follows that the order of $m_s(\alpha, c)$ is the (multiplicative) order of $\alpha$. When $\alpha = 1$, $m_s(1, c)$ is **unipotent** and its order is $p =$ char $k$.

The unipotent matrices in $F(s)$ form a (normal) subgroup

$$U(s) = \left\{ m_s(1, c') = \begin{bmatrix} 1 + c's & -c's^2 \\ c' & 1 - c's \end{bmatrix} : c' \in \mathcal{C} \cap \mathcal{C}s^{-2} \right\}.$$

It is clear that, for each $s \in \hat{K}$,

$$\{d \in \mathcal{C} \colon m_s(1, d) \in U(s)\}$$

is a $\mathcal{C}$-ideal. For each $s \in \hat{K}$ there is a map

$$\theta \colon F(s) \to k^*$$

defined by

$$\theta(m_s(\alpha, c)) = \alpha.$$

It is known (see, for example, [9, Corollary 2.2]) that $\theta$ is *surjective.*

We now come to the remaining "zero rank, $q$ even" cases.

LEMMA 3.2: *If* $\mathrm{rk}_{\mathbb{Z}}(\Gamma) = 0$ *and* $4|q$, *then*

$$\mathrm{ncs}(\mathcal{C}) > 2.$$

*Proof:* Suppose, to the contrary, that $\Gamma$ contains a subgroup $\Lambda$ of index 2. To obtain the desired contradiction it is sufficient to prove that every element of finite order lies in $\Lambda$. (See comment after Lemma 1.1.)

Let $h$ be an element of finite order of $\Gamma$ and let $\alpha, \alpha^{-1}$ be its eigenvalues. There are two possibilities. If $\alpha \neq \alpha^{-1}$ then the order of $h$ is the (multiplicative) order of $\alpha$, which is odd (since $q$ is even). We may assume therefore that $\alpha = \alpha^{-1}$ (in which case $\alpha = 1$) and hence that $h$ is unipotent. Then $h \in U(s)$, for some $s \in \hat{K}$. It follows that

$$h = m_s(1, c),$$

for some $c \in \mathcal{C}$. We now make full use of the hypothesis on $q$. Choose $\alpha_0 \in k^*$, such that $\alpha_0^2 \neq 1$, and then $c_0 \in \mathcal{C}$ such that

$$h_0 = m_s(\alpha_0, c_0) \in F(s).$$

Let $h_1 = m_s(1, c')$, where $c' = c(\alpha_0^{-2} - 1)^{-1}$. By the above $h_0 \in \Lambda$ and $h_1 \in U(s)$. It is easily verified that

$$h = h_0 h_1 h_0^{-1} h_1^{-1}.$$

We conclude that $h \in \Lambda$ (since $\Lambda$ is normal in $\Gamma$). ∎

We deal with the remaining two cases separately. We note that, when $g = 0$, it follows from a celebrated result of F. K. Schmidt [13, V.1.11, p. 164] that $K = k(t)$, the rational function field over $k$.

Lemma 3.3: *If $q$ is odd and $(g, \delta) = (0, 1)$, then*

$$\mathrm{ncs}(\mathcal{C}) > 2.$$

*Proof:* When $(g, \delta) = (0, 1)$ it follows that

$$\mathcal{C} \cong k[t].$$

The ring $\mathcal{C}$ is then euclidean and so $\Gamma$ is generated by elementary matrices of the type

$$\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix},$$

both of which have odd order. We deduce that $\Gamma$ does not contain any subgroup of index 2. The result follows. ∎

We now come to the remaining case.

Lemma 3.4: *If $q$ is odd and $(g, \delta) = (0, 2)$, then*

$$\mathrm{ncs}(\mathcal{C}) > 2.$$

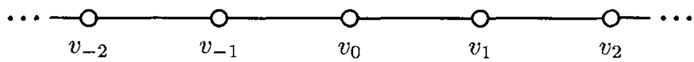
*Proof:* We make use of the results of [10] where the structure of $G\backslash X$ is determined when $K = k(t)$. (Recall that $G = \mathrm{GL}_2(\mathcal{C})$ and that $X$ is its Bruhat–Tits tree.) By Lemmata 2.16–2.20 of [10] it follows that

$$\{\det h \colon h \in G_v\} = k^*,$$

for all $v \in \mathrm{vert}\, X$. By [12, Exercise 1(a), p. 98] we deduce that the natural projection

$$\pi\colon \mathrm{vert}(\Gamma\backslash X) \twoheadrightarrow \mathrm{vert}(G\backslash X)$$

is *injective*. (See also [12, Exercise 4, p. 117].) Combining Theorem 2.22 and Lemmata 2.25, 4.4 of [10], we conclude that $\Gamma\backslash X$ is a *tree* which lifts to a doubly infinite path in $X$




(Serre [12, 2.4.2(a), p.113] states this result for the quotient group $G\backslash X$.)

Let $\Gamma_i$ denote the stabilizer of $v_i$ in $\Gamma$, where $i \in \mathbb{Z}$. It is known [10, Lemmata 2.16–2.20] that

(i) $\Gamma_0 = \mathrm{SL}_2(k)$,

(ii) $\Gamma_1 \cong \mathrm{SL}_2(k)$,

(iii) $\Gamma_n \leq \Gamma_{n+1}$, for all $n \geq 2$.

and

(iv) $\Gamma_n \leq \Gamma_{n-1}$, for all $n \leq -1$.

It is also known [10, Lemmata 2.16, 2.17] that

$$\bigcup_{n\leq -1} \Gamma_n = F(\infty) \quad \text{and that} \quad \bigcup_{n\geq 2} \Gamma_n = F(t).$$

By [12, Theorem 13, p. 55] it follows that $\Gamma$ is generated by

$$\Gamma_0, \Gamma_1, F(\infty) \quad \text{and} \quad F(t)$$

(since $\Gamma\backslash X$ is a tree).

Suppose, to the contrary, that $\Gamma$ contains a subgroup $\Lambda$ of index 2. Since $\mathrm{SL}_2(k)$ has no subgroups of index 2, when $q > 2$, the subgroups $\Gamma_0$ and $\Gamma_1$ are contained in $\Lambda$.

The subgroups $U(\infty)$ and $U(t)$ are generated by (unipotent) elements of odd order ($=$ char $k$) and so each is contained in $\Lambda$. Let $h \in F(s)$, where $s = \infty, t$. Then

$$h = m_s(\alpha, c),$$

for some $\alpha \in k^*$, $c \in \mathcal{C}$. We may assume that $\alpha \neq 1$.

By [10, Lemma 2.16] it follows that

$$h_\infty = m_\infty(\alpha, 0) = (\alpha, \alpha^{-1}) \in \Gamma_0 \cap F(\infty).$$

Now, when $s = \infty$,

$$hh_\infty^{-1} = m_\infty(1, *) \in \Lambda,$$

and so $h \in \Lambda$.

It is shown in the proof of [10, Lemma 2.20], combined with [10, Lemma 2.17], that there exists $c' \in \mathcal{C}$ for which

$$h_t = m_t(\alpha, c') \in \Gamma_1 \cap F(t).$$

It follows that, when $s = t$,

$$hh_t^{-1} = m_t(1, *) \in \Lambda,$$

and so again $h \in \Lambda$. We have therefore proved that $F(\infty), F(t) \leq \Lambda$, which gives the desired contradiction. ∎

We now come to the principal result of this paper.

THEOREM 3.5: *With the above notation,*

$\mathrm{ncs}(\mathcal{C}) > 2$ *if and only if*

(i) $(g, \delta) = (0,1), (0,2)$ *and* $q \neq 2$

*or*

(ii) $(g, \delta) = (0,3), (1,1)$ *and* $4|q$.

By Lemmata 3.1(ii), 3.3 and 3.4 it follows that $\mathrm{ncs}(\mathcal{C}) = 3$, when $q = 3, g = 0$ and $\delta = 1, 2$. With the exception of these cases this leaves open the following question.

PROBLEM: *Determine* $\mathrm{ncs}(\mathcal{C})$, *when* $\mathrm{ncs}(\mathcal{C}) > 2$.

## References


[1] H. Bass, J. Milnor and J-P. Serre, *Solution of the congruence subgroup problem for* $\mathrm{SL}_n (n \geq 3)$ *and* $\mathrm{Sp}_{2n} (n \geq 2)$, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **33** (1967), 59–137.

[2] E.-U. Gekeler, *Le genre des courbes modulaires de Drinfeld*, Comptes Rendus de l'Académie des Sciences, Paris **300** (1985), 647–650.

[3] E.-U. Gekeler, *Drinfeld Modular Curves*, Lecture Notes in Mathematics **1231**, Springer-Verlag, Berlin, 1986.

[4] F. Grunewald, J. Mennicke and L. Vaserstein, *On the groups* $\mathrm{SL}_2(\mathbb{Z}[x])$ *and* $\mathrm{SL}_2(k[x,y])$, Israel Journal of Mathematics **86** (1994), 157–193.

[5] F. Grunewald and J. Schwermer, *On the concept of level for subgroups of* $\mathrm{SL}_2$ *over orders of arithmetic type*, Israel Journal of Mathematics **114** (1999), 205–220.

[6] B. Liehl, *On the groups* $\mathrm{SL}_2$ *over orders of arithmetic type*, Journal für die reine und angewandte Mathematik **323** (1981), 153–171.

[7] A. W. Mason, *Free quotients of congruence subgroups of* $\mathrm{SL}_2$ *over a coordinate ring*, Mathematische Zeitschrift **198** (1988), 39–51.

[8] A. W. Mason, *Congruence hulls in* $\mathrm{SL}_n$, Journal of Pure and Applied Algebra **89** (1993), 255–272.

[9] A. W. Mason, *Groups generated by elements with rational fixed points*, Proceedings of the Edinburgh Mathematical Society **40** (1997), 19–30.

[10] A. W. Mason, *The generalization of Nagao's theorem to other subrings of the rational function field*, Communications in Algebra, to appear.

[11] J-P. Serre, *Le problème des groupes de congruence pour* $\mathrm{SL}_2$, Annals of Mathematics **92** (1970), 489–527.

[12] J-P. Serre, *Trees*, Springer-Verlag, Berlin, 1980.

[13] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

[14] L. N. Vaserstein, *On the group* $\mathrm{SL}_2$ *over Dedekind rings of arithmetic type*, Mathematics of the USSR-Sbornik **18** (1972), 321–332.