AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 7(4): 5305–5313.
DOI: 10.3934/math.2022295
Received: 29 September 2021
Revised: 10 December 2021
Accepted: 22 December 2021
Published: 06 January 2022

Research article

$\mathrm{SL}_n(\mathbb{Z})$-normalizer of a principal congruence subgroup

Guangren Sun and Zhengjun Zhao*

School of Mathematics and Physics, Anqing Normal University, Anqing, Anhui 246133, China

* **Correspondence:** Email: zzj_aqnu@163.com; Tel: +8615222960607.

Abstract: Let $\mathrm{SL}_n(\mathbb{Q})$ be the set of matrices of order n over the rational numbers with determinant equal to 1. We study in this paper a subset Λ of $\mathrm{SL}_n(\mathbb{Q})$, where a matrix B belongs to Λ if and only if the conjugate subgroup $B\Gamma_q(n)B^{-1}$ of principal congruence subgroup $\Gamma_q(n)$ of lever q is contained in modular group $\mathrm{SL}_n(\mathbb{Z})$. The notion of least common denominator (LCD for convenience) of a rational matrix plays a key role in determining whether B belongs to Λ. We show that LCD can be described by the prime decomposition of q. Generally Λ is not a group, and not even a subsemigroup of $\mathrm{SL}_n(\mathbb{Q})$. Nevertheless, for the case $n = 2$, we present two families of subgroups that are maximal in Λ in this paper.

Keywords: principal congruence subgroup; least common denominator; maximal subgroup
Mathematics Subject Classification: 20H05

1. Introduction

Denote by $\mathrm{SL}_n(\mathbb{Q})$ the set

$$\left\{A = (a_{ij})_{n\times n} : \quad a_{ij} \in \mathbb{Q}, i, j = 1, 2, \cdots, n, \text{and} \det(A) = 1\right\},$$

and $\mathrm{SL}_n(\mathbb{Z})$ the set

$$\left\{(a_{ij})_{n\times n} \in \mathrm{SL}_n(\mathbb{Q}) : \quad a_{ij} \in \mathbb{Z}, i, j = 1, 2, \cdots, n\right\}.$$

This set $\mathrm{SL}_n(\mathbb{Z})$ is usually referred to as "modular group". It is well known that $\mathrm{SL}_2(\mathbb{Z})$ is closely related to modular forms, see [3]. Many important subgroups of $\mathrm{SL}_n(\mathbb{Z})$ have been widely studied, such as

Definition 1.1 *Let $n, q \geq 2$ be positive integers. The principal congruence subgroup of level q is defined as*

$$\Gamma_q(n) = \{(a_{ij})_{n\times n} \in \mathrm{SL}_n(\mathbb{Z}) : \quad a_{ii} \equiv 1 (\mathrm{mod}\ \ q); a_{ij} \equiv 0 (\mathrm{mod}\ \ q), i \neq j\}.$$

Remark 1.2 *A different but equivalent definition can refer to [4]. We always denote by I_n the $n \times n$ identity matrix throughout the paper, and use notation $\boldsymbol{E}_{ij}$ to represent the matrix with all entries are 0 but the (i, j) entry is 1. For a matrix A, denoted by A_{ij} its (i, j) entry.*

Naturally, $\Gamma_q(n)$ could be addressed in the larger group $\mathrm{SL}_n(\mathbb{Q})$. In this paper, we concentrate our attention on the the following subset Λ of $\mathrm{SL}_n(\mathbb{Z})$.

Definition 1.3 *Let $n, q \geq 2$ be positive integers. The $\mathrm{SL}_n(\mathbb{Z})$-normalizer of $\Gamma_q(n)$ is defined as*

$$\Lambda = \left\{B \in \mathrm{SL}_n(\mathbb{Q}) : \quad B\Gamma_q(n)B^{-1} \subset \mathrm{SL}_n(\mathbb{Z})\right\},$$

and matrix in Λ is called an $\mathrm{SL}_n(\mathbb{Z})$-normalization element of $\Gamma_q(n)$.

This notion, which ties in nicely with "The congruence subgroup problem" (see [7], or [4]), is inspired by observing subgroup topologies in $\mathrm{SL}_n(\mathbb{Q})$ (see [4]). As well known the normalizer of a congruence subgroup has acquired significance because it is related to some simple group in [2]. It has also played an important role in work on Weierstrass points on the Riemann surfaces in [5].

In order to figure out Λ, it is a natural approach to transform a matrix in $\mathrm{SL}_n(\mathbb{Q})$ into the set of integral matrices by multiplying a suitable positive integer. The following concept plays a key role in our discussion on the structure of Λ.

Definition 1.4 *Let n, r be positive integers, and $B \in \mathrm{SL}_n(\mathbb{Q})$. We call r the least common denominator (*LCD *for convention) of B, denoted by c_B, if r is the least positive integer such that rB is an integral matrix.*

With above preparation, the remainder of this paper is organized as follows. In Section 2, the fundamental relationship between $\mathrm{SL}_n(\mathbb{Q})$ and Λ is investigated. It is obvious that Λ contains $\mathrm{SL}_n(\mathbb{Z})$, and we will show that this inclusion is proper when q is not square-free. With the aid of Smith normal form of an integral matrix, we first establish a necessary and sufficient condition for determining whether a matrix in $\mathrm{SL}_n(\mathbb{Q})$ belongs to Λ. This statement does not give an explicit relationship between c_B and q in the case $n > 2$ yet. Fortunately one necessary condition is obtained, which enables us to bound the multiplicity of arbitrary prime factor of the LCD of a matrix in Λ by factoring q. Other than that, we also show that Λ is not a group, and not even a semigroup. In spite of this, Λ admits many subgroups distinguished from $\mathrm{SL}_n(\mathbb{Q})$. In section 3, two families of subgroups that are maximal in Λ are presented in the case $n = 2$.

2. LCD and the basic structure of Λ

In this section, we will show that it can be determined whether a matrix in $\mathrm{SL}_n(\mathbb{Q})$ belongs to Λ when its LCD is specified. In order to go on our following discussion, we need a widely understood theorem (see [1,6,8,9]), which arises from basic module theory over a principal ideal domain. The Smith normal form of integral matrices, which will be presented in the following paragraph, is our main tool in this section.

Let n be a positive integer, and A an integral matrix of order n. Then there exists unimodular matrices P, Q such that PAQ is a diagonal matrix

$$PAQ = \mathrm{diag}(d_1, d_2, \cdots, d_l, 0, \cdots, 0), \tag{2.1}$$

where d_i, unique up to the sign, are nonzero integers for all $1 \leq i \leq l$, and $d_i \mid d_{i+1}$. Moreover, d_i is called the i-th invariant factor of A, and (2.1) is the **Smith normal form** of A.

With the aid of this result, we give a characterization for the LCD of matrices in Λ as following theorem states.

Theorem 2.1 *Let $n, q \geq 2$ be positive integers, and $B \in \mathrm{SL}_n(\mathbb{Q})$. Then B is an $\mathrm{SL}_n(\mathbb{Z})$-normalization element of $\Gamma_q(n)$ if and only if the n-th invariant factor d_n of $c_B B$ divides q.*

Proof. Suppose that B is an $\mathrm{SL}_n(\mathbb{Z})$-normalization element of $\Gamma_q(n)$ and $A = c_B B$. Let P, Q be unimodular matrices such that PAQ is the Smith normal form in (2.1). It follows from the fact B is invertible that the number l in (2.1) is equal to the order n of B. It is obvious that $d_i \mid d_{i+1}$, and a positive integer r is the LCD of A if and only if the greatest common divisor of all entries of rA is 1. Thus $d_1 = \pm 1$. Set $C = PBQ$, then C is also an $\mathrm{SL}_n(\mathbb{Z})$-normalization element of $\Gamma_q(n)$. Hence, for any $X = (x_{ij})_{n\times n} \in \Gamma_q(n)$, we have

$$CXC^{-1} = \begin{pmatrix} x_{11} & d_1 d_2^{-1} x_{12} & \dots & d_1 d_n^{-1} x_{1n} \\ d_2 d_1^{-1} x_{21} & x_{22} & \dots & d_2 d_n^{-1} x_{2n} \\ \vdots & \vdots & & \vdots \\ d_n d_1^{-1} x_{n1} & d_n d_2^{-1} x_{n2} & \dots & x_{nn} \end{pmatrix} \in \mathrm{SL}_n(\mathbb{Z})$$

Take $X = I_n + q\mathbf{E}_{1n}$. It follows from above statements that $(1, n)$ entry of CXC^{-1}, which is equal to $\pm q d_n^{-1}$, is an integer, and thus this means that $d_n \mid q$. This completes the proof of necessity.

Conversely, if $d_n \mid q$, then $d_i \mid q$ for all $1 \leq i \leq n$. We can assert from this fact that all entries in CXC^{-1} are integers, and thus the sufficiency follows. □

It is worth pointing out that in the case $n = 2$, we have $d_1 d_2 = \pm d_2 = c_B^2$, and thus the fact d_2 of $c_B B$ divides q is equivalent to that c_B^2 divides q.

Unfortunately, above theorem does not give an explicit relationship between c_B and q in the case $n > 2$. However, the following proposition can help us to understand the problem stated to some extent.

Theorem 2.2 *Let $n, q \geq 2$ be positive integers, $p_1^{e_1} \cdots p_k^{e_k}$ the prime decomposition of q, and $B = (b_{ij})_{n\times n} \in \mathrm{SL}_n(\mathbb{Q})$. If B is an $\mathrm{SL}_n(\mathbb{Z})$-normalization element of $\Gamma_q(n)$, then $c_B = p_1^{f_1} \cdots p_k^{f_k}$, where $0 \leq f_i \leq e_i - 1$ for all $1 \leq i \leq k$. In particular, if q is square-free, then $\Lambda = \mathrm{SL}_n(\mathbb{Q})$.*

Proof. Let $A = c_B B$, and PAQ be the Smith normal form of A. We claim here that the following conclusion is true. **Claim:** *Suppose that p is a prime number and f a positive integer. Then $p^f \mid c_B$ implies $p^{f+1} \mid d_n$.*

If above assertion was established, then the result follows by Theorem 2.1.

Assume the claim is false, then d_n is divisible by at most f-th power of p, so does d_i, $i = 1, \cdots, n$. Note here that $d_1 = \pm 1$, hence $d_1 \cdots d_n$ is divisible by at most $(n-1)f$-th power of p. On the other hand, the determinants of PBQ and B are both equal to 1. Therefore, $d_1 \cdots d_n = c_B^n$, and this means that $p^{nf} \mid d_1 \cdots d_n = c_B^n$. So, above statements are contrary to the fact $(n-1)f < nf$, and thus the assumption is not correct. □

Corollary 2.3 *Let $q \geq 2$ be a square-free positive integer, then the normalizer of $\Gamma_q(n)$ in $\mathrm{SL}_n(\mathbb{Q})$ is $\mathrm{SL}_n(\mathbb{Z})$.*

The previous conclusions present some description for the elements of Λ. It has to be pointed out that as the subset of the group $\mathrm{SL}_n(\mathbb{Q})$, Λ does not possess a fine structure. In fact, we can show that Λ is not a semigroup of the group $\mathrm{SL}_n(\mathbb{Q})$.

Proposition 2.4 *Let $n \geq 2$ be a positive integer, $q = m^{2s} r$, where $m > 1, r \geq 1, s \geq 1$ are integers with $m^2 \nmid r$. Then $\mathrm{SL}_n(\mathbb{Z})$ is properly contained in Λ, and Λ is also a proper subset of $\mathrm{SL}_n(\mathbb{Q})$, but not* *a subsemigroup. In addition, any subgroup of* $\mathrm{SL}_n(\mathbb{Q})$ *which contains* $\mathrm{SL}_n(\mathbb{Z})$ *must have an element, which does not belong to* Λ.

Proof. It is clear that $B = \mathrm{diag}(\frac{1}{m}, 1, \cdots, 1, m) \notin \mathrm{SL}_n(\mathbb{Z})$. Moreover, m^2 is the n-th invariant factor of $c_B B$ and divides q, hence $B \in \Lambda$, and thus we can get the first proper inclusion. On the other hand, we know that LCD of matrices in $\mathrm{SL}_n(\mathbb{Q})$ is unbounded. However, the fact $B \in \Lambda$ implies $c_B < q$ by Theorem 2.2, then the second inclusion follows.

In what follows, we show that Λ is not a subsemigroup. As a matter of fact, it suffices to verify that there exist two matrices whose product does not belong to Λ. Let $K = \mathrm{diag}(\frac{1}{m^s}, 1, \cdots, 1, m^s)$. Analogously, m^{2s} is the n-th invariant factor of $c_K K$ and divides q, hence $K \in \Lambda$. With B defined as previous paragraph, set $J = BK$. Then the n-th invariant factor of $c_J J$ is m^{2s+2} which does not divide q, the conclusion follows.

The last assertion can be restated as: Let $D \in \Lambda \setminus \mathrm{SL}_n(\mathbb{Z})$, then the subgroup H generated by $\mathrm{SL}_n(\mathbb{Z}) \bigcup \{D\}$ must have an element which does not belong to Λ.

Let $A = c_D D$, and PAQ be the Smith normal form of A. We note that $PDQ \in H$, and thus s-th power of PDQ

$$(PDQ)^s = \left(\frac{1}{c_D} PAQ\right)^s = \mathrm{diag}\left(\frac{d_1^s}{c_D^s}, \cdots, \frac{d_n^s}{c_D^s}\right)$$

is also in the group H. It is easily deduced from $d_1 = \pm 1$ that $c_{(PDQ)^s} = c_D^s$. If $(PDQ)^s \in \Lambda$, then c_D^s divides q by Theorem 2.2. However $c_D > 1$ for $D \notin \mathrm{SL}_n(\mathbb{Z})$, and s can be chose arbitrarily, it is absurd. □

3. Maximal subgroups in Λ

In view of sparsity of set Λ as Proposition 2.4 pointed out, we are led to focus our attention on subgroups of $\mathrm{SL}_n(\mathbb{Q})$ those are maximal in Λ, which is strictly defined as follows.

Definition 3.1 *With n, q defined as Proposition 2.4, we call a subgroup M of* $\mathrm{SL}_n(\mathbb{Q})$ *contained in Λ a maximal* $\mathrm{SL}_n(\mathbb{Z})$*-normalizer or simply maximal normalizer, if the following conditions hold*

1. *M is a subgroup of* $\mathrm{SL}_n(\mathbb{Q})$*;*
2. *If H is a subgroup of* $\mathrm{SL}_n(\mathbb{Q})$ *and properly contains M, then there is a matrix $A \in H \setminus \Lambda$.*

It follows immediately from Proposition 2.4 that $\mathrm{SL}_n(\mathbb{Z})$ satisfies above two conditions, and we call it the trivial maximal normalizer which is not our focus. In fact, we are interested in the following problem.

Problem 3.2 *Find all nontrivial maximal normalizers.*

To our knowledge, the problem we mentioned above is difficult to solve completely. In the rest of this section, two families of nontrivial maximal normalizers will be presented in the case $n = 2$. In what follows, we focus attention on the case $n = 2$. In other words, we will address related problems in $\mathrm{SL}_2(\mathbb{Q})$.

Proposition 3.3 *Let $q = \mu^2\nu > 1$ be a positive integer, where ν is a square-free integer. If τ_1 and τ_2 are two coprime positive integers with product $\tau_1\tau_2$ dividing μ, then*

$$H(\tau_1, \tau_2) = \left\{\frac{1}{\tau_1\tau_2}\begin{pmatrix} a\tau_1\tau_2 & b\tau_1^2 \\ c\tau_2^2 & d\tau_1\tau_2 \end{pmatrix} : \ a, b, c, d \in \mathbb{Z}; ad - bc = 1\right\} \tag{3.1}$$

is a maximal normalizer. And if either τ_1 or τ_2 is greater than 1*, then $H(\tau_1, \tau_2)$ is nontrivial.*

Proof. By Theorem 2.1, we know that the $\mathrm{SL}_2(\mathbb{Z})$-normalizer of $\Gamma_q(2)$ is $\Lambda = \{B \in \mathrm{SL}_2(\mathbb{Q}) : \ c_B \mid \mu\}$.

It is easy to verify that $H(\tau_1, \tau_2)$ is a subset of Λ, and also a subgroup of $\mathrm{SL}_2(\mathbb{Q})$. Therefore, we only need to show $H(\tau_1, \tau_2)$ is maximal in Λ. Namely, we have to prove that for any $K \in \Lambda \setminus H(\tau_1, \tau_2)$, the subgroup L generated by $H(\tau_1, \tau_2) \bigcup \{K\}$ must have an element, which does not belong to Λ.

To this end, let $A = c_K K$. First, we show there exists $J \in H(\tau_1, \tau_2)$ such that JA is a upper triangular matrix. If $A_{21} = 0$, it is trivial. And when $A_{11} = 0$, we need only take J as $\frac{\tau_1}{\tau_2}\mathbf{E}_{12} - \frac{\tau_1}{\tau_2}\mathbf{E}_{21}$. As a consequence, we can assume that neither of A_{11}, A_{21} is equal to 0. Let $\alpha = \gcd(A_{11}\tau_2, A_{21}\tau_1)$, and $c' = A_{21}\frac{\tau_1}{\alpha}$, $d' = -A_{11}\frac{\tau_2}{\alpha}$. As well known that there exists two integers a', b' such that $a'd' - b'c' = 1$, so we can take

$$J = \frac{1}{\tau_1\tau_2}\begin{pmatrix} a'\tau_1\tau_2 & b'\tau_1^2 \\ c'\tau_2^2 & d'\tau_1\tau_2 \end{pmatrix}.$$

Set $D = JK$, then $D_{11}D_{22} = 1$ as the determinant of JK is 1. We show that the subgroup generated by D is not contained in Λ. The scenarios will be considered for the following two cases:

Case 1. $D_{11}, D_{22} \notin \{\pm 1\}$. Let $D_{11} = \frac{\omega_1}{\theta_1}$ be the reduced fraction with $\theta_1 > 1$. Since $D \in L$ implies $D^m \in L$, we deduce $c_{D^m} \mid \mu$, i.e., $\theta_1^m \mid \mu$ for any positive integer m, but this is in contradiction with $\theta_1 > 1$.

Case 2. $D_{11}, D_{22} \in \{\pm 1\}$. We can assume $D_{11} = D_{22} = 1$ because of $-I_2 \in H(\tau_1, \tau_2)$. Let $D_{12} = \frac{\beta}{\gamma}$ be the reduced fraction. Note that $D \notin H(\tau_1, \tau_2)$, then the ratio $\frac{\beta\tau_2}{\gamma\tau_1}$ of $\frac{\beta}{\gamma}$ and $\frac{\tau_1}{\tau_2}$ is not an integer. For any positive integer m, let

$$P_m = \begin{pmatrix} a_m & b_m \\ c_m & d_m \end{pmatrix} = \left[D\left(-\frac{\tau_1}{\tau_2}\mathbf{E}_{12} + \frac{\tau_2}{\tau_1}\mathbf{E}_{21}\right)\right]^m.$$

By this equality, we can obtain the following recurrence relation

$$a_1 = \frac{\beta\tau_2}{\gamma\tau_1}, a_2 = \left(\frac{\beta\tau_2}{\gamma\tau_1}\right)^2 + 1, a_{m+2} = \frac{\beta\tau_2}{\gamma\tau_1}a_{m+1} - a_m.$$

Hence a_m is a polynomial in $\frac{\beta\tau_2}{\gamma\tau_1}$ with integral coefficients. We note here that $\frac{\beta\tau_2}{\gamma\tau_1}$ is not an integer, so we can take the reduced fraction $\frac{\beta\tau_2}{\gamma\tau_1} = \frac{\omega}{\theta}$ with $\theta > 1$. Suppose now

$$a_m = \frac{\omega^m + s_{m-1}\omega^{m-1}\theta + \cdots + s_1\omega\theta^{m-1} + s_0\theta^m}{\theta^m}, \tag{3.2}$$

where s_i is an integer for $1 \le i \le m$, and m is any positive integer. The right hand side of (3.2) is obviously reduced also, and this implies $\theta^m \mid \mu$. Similar to case 1, it is absurd. □

Remark 3.4 *It is worth pointing out that the group $H(\tau_1, \tau_2)$ in above proposition is a conjugate subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *in* $\mathrm{SL}_2(\mathbb{Q})$*. It is natural to raise a problem here: which conjugate subgroups of* $\mathrm{SL}_2(\mathbb{Z})$ *in* $\mathrm{SL}_2(\mathbb{Q})$ *are maximal normalizers.*

It is not hard to see from above discussion that if the subgroup $\langle A\rangle$, generated by $A \in \Lambda$, is contained in Λ, then there must exist a maximal normalizer in Λ which contains A. In order to go on our story, the following definition is needed.

Definition 3.5 *Let $A \in \mathrm{SL}_n(\mathbb{Q})$. A is called σ−stable if there exists a positive integer σ such that $c_{A^m} \le \sigma$ for any integer m. Otherwise, A is called unbounded.*

When a matrix $A \in \mathrm{SL}_n(\mathbb{Q})$ is $\sigma-$stable, we call A stable instead of $\sigma-$stable for convenience if we do not need to know σ exactly.

Example 3.6 *Let $q = p^2$, where p is a prime number. Then the matrix*

$$B = \frac{1}{p}\begin{pmatrix} p & 1 & & \\ & p & \ddots & \\ & & \ddots & 1 \\ & & & p \end{pmatrix}$$

belongs to the $\mathrm{SL}_n(\mathbb{Z})$-normalizer of $\Gamma_q(n)$, and is $p^{n-1}-$stable. It is not hard to check that B is not $p-$stable when $n > 2$, and thus Λ does not contain the cyclic group generated by B, i.e., no maximal normalizer contains B.

Having taken a short tour to the general case, we now concentrate our attention on the case $n = 2$ again. The following result gives some description for stable matrix in $\mathrm{SL}_2(\mathbb{Q})$.

Lemma 3.7 *Let $A \in \mathrm{SL}_2(\mathbb{Q})$. Then A is stable if and only if the trace $tr(A)$ is an integer. In particular, under assumptions of Proposition 3.3, there exists a maximal normalizer which contains A whenever $tr(A)$ is an integer and $c_A \mid \mu$.*

Proof. Set

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad A^m := \begin{pmatrix} a_m & b_m \\ c_m & d_m \end{pmatrix}$$

It is easy to show the following recurrence relation holds

$$\begin{cases} a_{m+1} = af_m - f_{m-1} \\ b_{m+1} = bf_m \\ c_{m+1} = cf_m \\ d_{m+1} = df_m - f_{m-1} \end{cases} \tag{3.3}$$

where $f_0 = 1, f_1 = tr(A)$ and $f_{m+1} = tr(A)f_m - f_{m-1}$ for any positive integer m. Hence f_m is a polynomial in $tr(A)$ with integral coefficients, and $tr(A)$ is an integer implies in turn f_m is also an integer. Then we can deduce $c_{A^m} \mid c_A$ for $m \geq 1$ by (3.3). When $m \leq -1$, a recurrence relation analogous to (3.3) holds clearly, and thus the sufficiency follows.

Conversely, suppose $tr(A)$ is not an integer, we show that $c_{A^{m+1}}$ is unbounded for $m \geq 1$. Let $tr(A) = \frac{\omega}{\theta}$ be the reduced fraction with $\theta > 1$, we divide proof of the necessity into the following two cases as Proposition 3.3:

Case 1. $b = 0$ and $c = 0$. Proof is the same as ***Case 1*** in Proposition 3.3.

Case 2. $b \neq 0$ or $c \neq 0$. It is sufficient to deal with $b \neq 0$. Let $b = \frac{\alpha}{\beta}$ be the reduced fraction. Set

$$f = \max\left\{f_p : \quad p^{f_p} \mid \theta, p^{f_p+1} \nmid \theta\right\},$$

and $m \geq f + 1$. Let $\frac{\alpha_1}{\theta_m}$ be the reduced fraction of $\frac{\alpha}{\theta^m}$. Then α_1 and θ are coprime numbers, and $p^{m-f} \mid \theta_m$ as long as p is a prime divisor of θ. Hence b_{m+1} can be expressed as

$$\frac{\alpha_1(\omega^m + s_{m-1}\omega^{m-1}\theta + \cdots + s_1\omega\theta^{m-1} + s_0\theta^m)}{\beta\theta_m}, \tag{3.4}$$

where s_i is an integer for $0 \le i \le m-1$. It is easy to check that θ_m and the integer in bracket of (3.4) are coprime, and the proof is the analogy of ***Case 2*** in Proposition 3.3. Then the denominator in the reduced fraction of b_{m+1} is divisible by θ_m, i.e., $\theta_m \mid c_{A^{m+1}}$. This completes the proof of necessity. □

With the help of above lemma, we can give another maximal normalizer in Λ except Proposition 3.3 presented.

Proposition 3.8 *With q, μ defined as Proposition 3.3. Let*

$$A = \frac{1}{\mu}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be a matrix in $\mathrm{SL}_2(\mathbb{Z})$-normalizer Λ of $\Gamma_q(2)$, where a, b, c, d are integers, d, μ are coprime and $a + d \equiv 0 (\mathrm{mod}\ \mu)$. Let $\lambda = d_{-1}b$ where $1 \le d_{-1} \le \mu - 1$ and $dd_{-1} \equiv 1 (\mathrm{mod}\ \mu)$. Then the unique maximal normalizer H which contains A is composed of

$$\frac{1}{\mu}\begin{pmatrix} l\mu + \lambda s & k\mu + \lambda(m\mu - \lambda s) \\ s & m\mu - \lambda s \end{pmatrix}$$

where l, k, m, s are integers satisfy that $l(m\mu - \lambda s) - ks = \mu$ and $la + kc \equiv lb + kd \equiv 0(\mathrm{mod}\ \ \mu)$.

Proof. It is not hard to verify that $c_A = \mu$ and $A \in H \subseteq \Lambda$. The product of any two matrices in H can be expressed as

$$P = \frac{1}{\mu}\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \frac{1}{\mu^2}\begin{pmatrix} l_1\mu + \lambda s_1 & k_1\mu + \lambda t_1 \\ s_1 & t_1 \end{pmatrix}\begin{pmatrix} l_2\mu + \lambda s_2 & k_2\mu + \lambda t_2 \\ s_2 & t_2 \end{pmatrix},$$

where $t_i = m_i\mu - \lambda s_i$ for $i = 1, 2$, and

$$\begin{cases} a_1 = (l_1 l_2 + s_2\frac{\lambda l_1 + k_1}{\mu})\mu + \lambda(s_1 l_2 + s_2 m_1) \\ b_1 = [l_1 k_2 + (m_2\mu - \lambda s_2)\frac{\lambda l_1 + k_1}{\mu}]\mu + \lambda[(m_1 m_2 + s_2\frac{\lambda l_2 + k_2}{\mu})\mu - \lambda(s_1 l_2 + s_2 m_1)] \\ c_1 = s_1 l_2 + s_2 m_1 \\ d_1 = (m_1 m_2 + s_2\frac{\lambda l_2 + k_2}{\mu})\mu - \lambda(s_1 l_2 + s_2 m_1) \end{cases}.$$

Note here that $d(\lambda l_i + k_i) = (dd_{-1})l_i b + k_i d \equiv 0(\mathrm{mod}\ \mu)$ for $i = 1, 2$, so $\lambda l_i + k_i \equiv 0(\mathrm{mod}\ \mu)$. Let

$$\begin{cases} s = s_1 l_2 + s_2 m_1 \\ l = l_1 l_2 + s_2\frac{\lambda l_1 + k_1}{\mu} \\ k = l_1 k_2 + (m_2\mu - \lambda s_2)\frac{\lambda l_1 + k_1}{\mu} \\ m = m_1 m_2 + s_2\frac{\lambda l_2 + k_2}{\mu} \end{cases}.$$

It is easy to see $l(m\mu - \lambda s) - ks = \mu$ for $\det P = 1$. Since

$$la + kc = l_1(l_2 a + k_2 c) + [m_2 c\mu + s_2(a - \lambda c)]\,\frac{\lambda l_1 + k_1}{\mu},$$

we deduce $la + kc \equiv 0(\mathrm{mod}\ \mu)$ from the congruence $l_2 a + k_2 c \equiv 0(\mathrm{mod}\ \mu)$ and $a - \lambda c = a(1 - dd_1) + d_1\mu^2 \equiv 0(\mathrm{mod}\ \mu)$. Similarly, we can get $lb + kd \equiv 0(\mathrm{mod}\ \mu)$, and this implies in turn $P \in H$. On the other hand, the inverse of arbitrary matrix in H is

$$\frac{1}{\mu}\begin{pmatrix} m\mu - \lambda s & -k\mu - \lambda(m\mu - \lambda s) \\ -s & l\mu + \lambda s \end{pmatrix}$$

$$= \frac{1}{\mu}\begin{pmatrix} m\mu + \lambda(-s) & (-k - \lambda m - \lambda l)\mu + \lambda[l\mu - \lambda(-s)] \\ -s & l\mu - \lambda(-s) \end{pmatrix},$$

where

$$ma + (-k - \lambda m - \lambda l)c = m(a - \lambda c) + c(\lambda l + k) \equiv 0(\mathrm{mod}\, \mu)$$

and

$$mb + (-k - \lambda m - \lambda l)d \equiv 0(\mathrm{mod}\, \mu),$$

and thus H is a subgroup of $\mathrm{SL}_2(\mathbb{Q})$.

In what follows, we show that H is the maximal and the unique normalizer. In fact, we will prove that any $B \in \Lambda$ contained in the same maximal normalizer with A must be in H.

Set

$$B = \frac{1}{\mu}\begin{pmatrix} u & v \\ s & t \end{pmatrix},$$

and compute AB and BA respectively. It follows from the fact c_{AB} and c_{BA} divide μ that $au + bs \equiv av + bt \equiv bs + dt \equiv 0(\mathrm{mod}\, \mu)$. As d and μ are coprime, we can find integers l, k, m such that $u = l\mu + \lambda s$, $v = k\mu + \lambda t, t = m\mu - \lambda s$. On the other hand, we get by Lemma 3.7 that

$$au + bs + cv + dt \equiv 0(\mathrm{mod}\, \mu^2) \tag{3.5}$$

Substitute u, v, t in (3.5), we have

$$(la + kc)\mu + (1 - dd_1)(1 + ad_1) \equiv 0(\mathrm{mod}\, \mu^2)$$

By Lemma 3.7 again, we obtain that $a + d \equiv 0(\mathrm{mod}\, \mu)$, so $1 + ad_1 \equiv (a + d)d_1 \equiv 0(\mathrm{mod}\, \mu)$, and thus $la + kc \equiv 0(\mathrm{mod}\, \mu)$.

Finally, let $D = \mu^3 ABA$, then

$$D_{12} = a(lb + kd)\mu + b^2 s(1 - dd_1)(1 + ad_1) + dbm(1 + ad_1)\mu$$

The fact $ABA \in \Lambda$ implies $D_{12} \equiv 0(\mathrm{mod}\, \mu^2)$, and then $a(lb+kd) \equiv 0(\mathrm{mod}\, \mu)$, that is $lb+kd \equiv 0(\mathrm{mod}\, \mu)$. Our proof of necessity is completed. □

Remark 3.9 *For coprime numbers d, μ, the maximal normalizer H in Proposition 3.8 is clearly different from $H(\tau_1, \tau_2)$ in Proposition 3.3.*

4. Conclusions

We give some remarks about our results obtained above to conclude our paper. In this paper, we study a subset Λ of $\mathrm{SL}_n(\mathbb{Q})$, where a matrix B belongs to Λ if and only if the conjugate subgroup $B\Gamma_q(n)B^{-1}$ of principal congruence subgroup $\Gamma_q(n)$ is contained in modular group $\mathrm{SL}_2(\mathbb{Z})$. We demonstrated that this subset Λ is fairly loose, and even not a semigroup. However, we presented in previous two sections two families of nontrivial maximal normalizers, i.e., two families of subgroups that are maximal in Λ. It is worth being pointed out that the maximal normalizers we provided are only one part of solutions to Problem 3.2 when $n = 2$. In the light of Proposition 3.3 and 3.8, we need to consider matrices whose diagonals are not invertible or 0 modulo μ. As for the case $n > 2$, Example 3.6 indicates that it is not enough to consider $tr(A)$ only. However, it seems difficult to our knowledge to get a simple formula which is analogous to (3.3).

Acknowledgments

We thank the referees for careful reading of the manuscript and the suggestions on the writing of the paper. This work was supported by National Nature Science Foundation of China(No. 11971382).

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. W. A. Adkins, S. H. Weintraub, *Algebra: An approach via module theory*, Springer-Verlag, New York, Grad. Texts in Math., **136**, 1992. https://dx.doi.org/10.1007/978-1-4612-0923-2
2. C. Conway, S. Norton, Monstrous moonshine, *Bull. London Math. Soc.,* **11** (1979), 308–339. https://dx.doi.org/10.1112/blms/11.3.308
3. F. Diamond, J. Shurman, *A first course in modular forms*, Springer-Verlag, New York, Grad. Texts in Math., **228**, 2005. https://dx.doi.org/10.1007/978-0-387-27226-9
4. J. E. Humphreys, *Arithmetic groups*, Springer-Verlag, Berlin, Lecture Notes in Mathematics.**789**, 1980. https://dx.doi.org/10.1007/BFb0094567
5. J. Lehner, M. Newman, Weierstrass points on $\Gamma_0(N)$, *Ann. Math.,* **79** (1964), 360–368. https://dx.doi.org/10.2307/1970550
6. M. Newman, *Integral matrices*, Academic Press, New York and London, 1972. https://dx.doi.org/10.2307/2005847
7. M. S. Raghunathan, The congruence subgroup problem, *Proc. Indian Acad. Sci. (Math. Sci.,)* **114** (2004), 299–308. https://dx.doi.org/10.1007/BF02829437
8. J. J. Rotman, *Advanced modern algebra*, revised 2nd printing, Prentice Hall, 2003. http://dx.doi.org/10.1090/gsm/114
9. H. J. S. Smith, On systems of linear indeterminate equations and congruences, *Philos. Trans.,* **151** (1861), 293–326. https://dx.doi.org/10.1080/03081081003709819

AIMS Press