

Computations in subgroups of finite index in $SL_2(\mathbb{Z})$

Alexander Konovalov,
(joint work with Ann Dooms and Eric Jespers)

Department of Mathematics
Vrije Universiteit Brussel
(Postdoctoral research collaborator by Francqui Stichting grant ADSI107)

Department of Mathematics
Zaporozhye National University, Ukraine

Nikolaus Conference, Aachen, 8-9 December 2006

G - finite group

$\mathbb{Z}G$ - integral group ring of the group G

$\mathcal{U}(\mathbb{Z}G)$ - unit group of $\mathbb{Z}G$

General problem

Describe the unit group $\mathcal{U}(\mathbb{Z}G)$ of $\mathbb{Z}G$

Our goal

Give explicit generators of a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$

Main tool

The method for computation of independent generators of congruence subgroups of $SL_2(\mathbb{Z})$ based on *Farey symbols*

$$\Gamma = SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1 \right\}$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \pmod{N} \right\}$$

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid b \equiv 0 \pmod{N} \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid a - 1 \equiv c \equiv d - 1 \equiv 0 \pmod{N} \right\}$$

$$\Gamma^1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid a - 1 \equiv b \equiv d - 1 \equiv 0 \pmod{N} \right\}$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid a - 1 \equiv b \equiv c \equiv d - 1 \equiv 0 \pmod{N} \right\}$$

$$\Gamma_0(N) = \begin{pmatrix} * & * \\ N & * \end{pmatrix}$$

$$\Gamma^0(N) = \begin{pmatrix} * & N \\ * & * \end{pmatrix}$$

$$\Gamma_1(N) = \begin{pmatrix} 1 + N & * \\ N & 1 + N \end{pmatrix}$$

$$\Gamma^1(N) = \begin{pmatrix} 1 + N & N \\ * & 1 + N \end{pmatrix}$$

$$\Gamma(N) = \begin{pmatrix} 1 + N & N \\ N & 1 + N \end{pmatrix}$$

These subgroups have finite index in Γ :

$$[\Gamma : \Gamma_0(N)] = [\Gamma : \Gamma^0(N)] = N \times \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

$$[\Gamma : \Gamma_1(N)] = [\Gamma : \Gamma^1(N)] = N^2 \times \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

$$[\Gamma : \Gamma(N)] = \begin{cases} 12, & N = 2 \\ N^3 \times \prod_{p|N} \left(1 - \frac{1}{p^2}\right) \end{cases}$$

It is well-known that there are subgroups of finite index in Γ which are not congruence subgroups

Farey symbol :

a compact and useful way to represent a subgroup of finite index in Γ (not necessarily a congruence subgroup). It has two components:

- generalised Farey sequence (g.F.s.)
- labels, giving additional structure to the g.F.s.

generalised Farey sequence :

- ordered list of the form $\{-\infty, x_0, x_1, \dots, x_n, \infty\}$
- $x_i = \frac{a_i}{b_i}$ are rational numbers in the reduced form arranged in increasing order for $i = 0, \dots, n$
- $x_0, x_n \in \mathbb{Z}$, and some $x_i = 0$
- we define $x_{-1} = -\infty = \frac{-1}{0}$ and $x_{n+1} = \infty = \frac{1}{0}$
- $a_{i+1}b_i - a_ib_{i+1} = 1$ for $i = -1, \dots, n$

Labels of Farey symbol :

The ordered list of labels gives an additional structure to the g.F.s. Labels correspond to each consecutive pair of x_i 's and have one of the following types:

- even, denoted by ○
- odd, denoted by ●
- numerical: natural number, which occurs in the list of labels exactly twice or not at all
- note that the actual values of numerical labels are not important: it is the pairing induced on two intervals that matters

Examples of Farey symbols :

Γ :

$$\left\{ \frac{-1}{0} \quad \frown \quad \frac{0}{1} \quad \frown \quad \frac{1}{0} \right\}$$

○ ●

$\Gamma_0(2)$:

$$\left\{ \frac{-1}{0} \quad \frown \quad \frac{0}{1} \quad \frown \quad \frac{1}{1} \quad \frown \quad \frac{1}{0} \right\}$$

1 ○ 1

Another example of Farey symbol :

$\Gamma(3)$:

$$\left\{ \frac{-1}{0} \quad \underbrace{\quad}_{1} \quad \frac{0}{1} \quad \underbrace{\quad}_{2} \quad \frac{1}{1} \quad \underbrace{\quad}_{3} \quad \frac{2}{1} \quad \underbrace{\quad}_{3} \quad \frac{5}{2} \quad \underbrace{\quad}_{2} \quad \frac{3}{1} \quad \underbrace{\quad}_{1} \quad \frac{1}{0} \right\}$$

The development of an algorithm to determine the Farey symbol for a subgroup G of a finite index in Γ was started by Ravi Kulkarni (CUNY) and later it was improved by Mong-Lung Lang, Chong-Hai Lim and Ser-Peow Tan (National University of Singapore).

This algorithm works whenever the membership test for G is available. Of course, this is the case for congruence subgroups. Before explaining this algorithm, we will show how to use its output to get independent generators for a finite index subgroup from the corresponding Farey symbol

Let σ be the Farey symbol for a group G with r_1 even labels, r_2 odd labels, and r_3 pairs of intervals.

Then G is generated by $r_1 + r_2 + r_3$ matrices, which form a set of its independent generators.

For each even interval $[x_i, x_{i+1}]$, take the matrix

$$A = \begin{pmatrix} a_{i+1}b_{i+1} + a_i b_i & -a_i^2 - a_{i+1}^2 \\ b_i^2 + b_{i+1}^2 & -a_{i+1}b_{i+1} - a_i b_i \end{pmatrix}$$

For each odd interval $[x_j, x_{j+1}]$, take the matrix

$$B = \begin{pmatrix} a_{j+1}b_{j+1} + a_j b_{j+1} + a_j b_j & -a_j^2 - a_j a_{j+1} - a_{j+1}^2 \\ b_j^2 + b_j b_{j+1} + b_{j+1}^2 & -a_{j+1}b_{j+1} - a_{j+1}b_j - a_j b_j \end{pmatrix}$$

For each pair of free intervals $[x_k, x_{k+1}]$ and $[x_s, x_{s+1}]$, take the matrix

$$C = \begin{pmatrix} a_{s+1}b_{k+1} + a_s b_k & -a_s a_k - a_{s+1} a_{k+1} \\ b_s b_k - b_{s+1} b_{k+1} & -a_{k+1} b_{s+1} - a_k b_s \end{pmatrix}$$

Computation of the Farey symbol :

- The algorithm starts with the g.F.s. $\{-\infty, 0, \infty\}$
- On each step we try to assign labels to unlabeled intervals, computing matrices by rules from the previous slide and checking if they belong to our subgroup:
 - matrices by odd intervals
 - matrices by even intervals
 - matrices by pairs of free intervals
- If after this step we still have unlabeled intervals, we select any unlabeled interval $[x_i = \frac{a_i}{b_i}, x_{i+1} = \frac{a_{i+1}}{b_{i+1}}]$, insert the reduced form of $\frac{a_i + a_{i+1}}{b_i + b_{i+1}}$ between x_i and x_{i+1} (with appropriate shifting of labels) and repeat the previous step.
- The procedure is finished if no unlabeled intervals are left.

The GAP package Congruence:

- creation of congruence subgroups
- intersections of finite number of congruence subgroups
- membership and inclusion tests
- computing Farey symbols for congruence subgroups
- computing generators and indices from Farey symbols
- Contributions by Helena Verrill:
 - factorisation in a product of generators
 - membership test by Farey symbol
- To do:
 - coset representatives of congruence subgroups

Runtime in seconds (Celeron-2.4, WinXP, RAM 512 MB)

Subgroup	Nr gens	GAP 4.4.9	Magma 2.10-14
$\Gamma(8)$	33	0.2	15.6
$\Gamma(16)$	257	14.9	866.6
$\Gamma(32)$	2049	1118.6	test failed

Applications for $\mathbb{Z}G$:

G - finite nilpotent group such that $\mathbb{Q}G$ does not have the following "exceptional" simple components :

- non-commutative division ring D
- $M_2(\mathbb{Q})$
- $M_2(\mathbb{Q}(\sqrt{-d}))$, $d > 0$
- $M_2(D)$, where D is a non-commutative division ring.

Then Jespers and Leal proved that in this case

$\mathcal{B} = \langle \text{Bass cyclic units, bicyclic units} \rangle$ generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.

New result :

By lifting generators of congruence subgroups of $SL_2(\mathbb{Z})$ to $\mathcal{U}(\mathbb{Z}G)$ and adding them to \mathcal{B} , we are able to exclude the exceptional component $M_2(\mathbb{Q})$, and give explicit generators of a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.

References



[MR 1137534: R. Kulkarni](#)

An arithmetic-geometric method in the study of the subgroups of the modular group. Amer. J. Math, Vol.113, No.6, Dec. 1991, 1053–1133



[MR 1206159: E. Jespers, G. Leal](#)

Generators of large subgroups of the unit group of integral group rings. Manuscripta Math. 78 (1993), no. 3, 303–315.



[MR 1332886: M.-L. Lang, C.-H. Lim, S.-P. Tan](#)

An algorithm for determining if a subgroup of the modular group is congruence. J. London Math. Soc. (2) 51 (1995), no. 3, 491–502.



[MR 1363856: M.-L. Lang, C.-H. Lim, S.-P. Tan](#)

Independent generators for congruence subgroups of Hecke groups. Math. Z. 220 (1995), no. 4, 569–594.