Commun. Korean Math. Soc. **20** (2005), No. 1, pp. 107–116

A PICTURE OF KLEINIAN MODULAR GROUP

HONG CHAN KIM

ABSTRACT. We show an algorithm to draw the famous picture of Kleinian modular group $\mathrm{PSL}(2,\mathbb{Z})$, which appears in describing the moduli space of elliptic curves.

Kleinian modular group $\mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/(\pm\mathbf{1})$ consists of Möbius transformations

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} : z \mapsto \frac{az+b}{cz+d}$$

of the upper half plane $\mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$.

We are interested in the images of the (half) circle

$$S := \{z \in \mathbb{C} \mid |z| = 1,\ \operatorname{im} z > 0\} \subset \mathbb{H}$$

under the action of $\mathrm{PSL}(2,\mathbb{Z})$. Figure 1 is the picture of S.

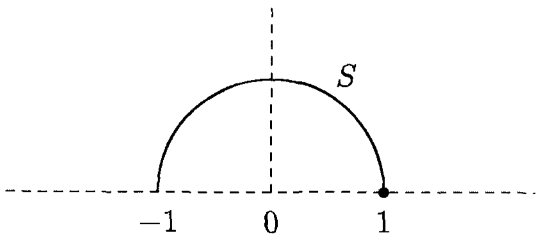

FIGURE 1. The standard half circle S in the upper half plane $\mathbb{H}$.

Note that the transformations which fix the circle S are the identity transformation (if $1 \mapsto 1$ and $-1 \mapsto -1$) and the hyperbolic rotation U

Received January 14, 2004.
2000 Mathematics Subject Classification: 52C45.
Key words and phrases: PSL(2,Z), good divisor, algorithm.
The author gratefully acknowledges the support from a Korea University Grant.

about the point $\sqrt{-1}$ (if $1 \mapsto -1$ and $-1 \mapsto 1$) :

$$U := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} : z \mapsto -\frac{1}{z}.$$

Suppose $c^2 - d^2 = 0$. If $c + d = 0$, then we can compute the transformation A is presented by

$$A = \begin{bmatrix} a & -a-1 \\ 1 & -1 \end{bmatrix} : z \mapsto \frac{az - (a+1)}{z-1}$$

with $A(1) = \infty$, $A(-1) = a + \frac{1}{2}$, and $A(i) = (a + \frac{1}{2}) + \frac{i}{2}$.

If $c - d = 0$, then the transformation B is presented by

$$B = \begin{bmatrix} b+1 & b \\ 1 & 1 \end{bmatrix} : z \mapsto \frac{(b+1)z + b}{z+1}$$

with $B(-1) = \infty$, $B(1) = b + \frac{1}{2}$, and $B(i) = (b + \frac{1}{2}) + \frac{i}{2}$.

Therefore if $c^2 = d^2$, then the image of S is a half line over a half integer. In Figure 2 these half lines are shown.

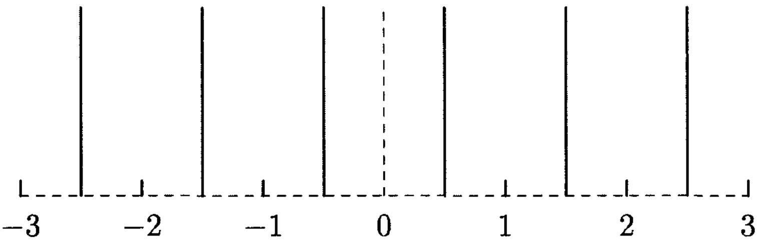

FIGURE 2. Images of S under the maps with $c^2 = d^2$

From now on, we will assume that $c^2 - d^2 \neq 0$ so that the image of S is again a (half) circle, whose radius is

$$\frac{1}{|c^2 - d^2|} \tag{1}$$

and the center is

$$\frac{a\,c - b\,d}{c^2 - d^2} \tag{2}$$

with end points $\frac{a-b}{c-d}$ and $\frac{a+b}{c+d}$. In Figure 3, the typical images of S are shown.

Note that if $\begin{pmatrix} a_0 & b_0 \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ and

$$a = a_0 + kc, \quad b = b_0 + kd$$

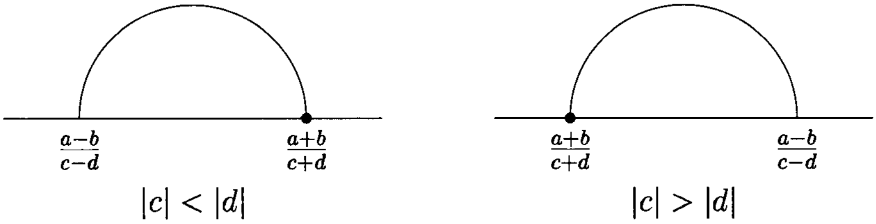

FIGURE 3. Typical images of S

for some integer k, then

$$\frac{ac-bd}{c^2-d^2} = \frac{a_0c-b_0d}{c^2-d^2} + k.$$

Thus the picture of

$$\mathbf{P} := (\mathrm{PSL}(2,\mathbb{Z}))(S)$$

is invariant under the translation $z \mapsto z+1$.

It is easy to show the following theorem.

THEOREM 1. *The center* $\frac{ac-bd}{c^2-d^2}$ *of the image circle is an integer if and only if its radius is equal to* 1.

The circles of radius 1 are shown in Figure 4.

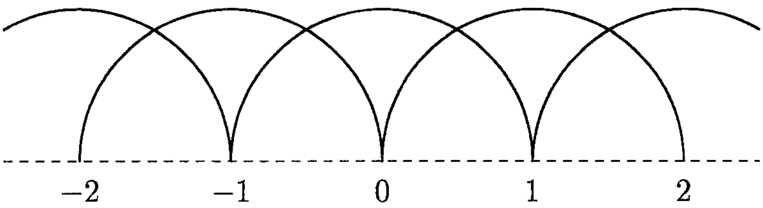

FIGURE 4. Images of S when $|c^2-d^2| = 1$.

We will draw the picture of $\mathbf{P}$ according to the descending order of the radius of each image circle.

Since the reciprocal of the radius of the image circle is $\left|c^2-d^2\right|$, we introduce the following definition.

DEFINITION 2. A positive integer n is said to be *good* if $n = |c^2-d^2|$ for some $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PSL}(2,\mathbb{Z})$.

Thus n is good if and only if $n = \left|c^2 - d^2\right|$ for some relatively prime integers c and d.

THEOREM 3. (1) *Every odd positive integer is good.*
(2) *An even positive integer is good if and only if it is divisible by 8.*

PROOF. (1) Suppose n is odd. Then $\begin{bmatrix} 1 & 1 \\ \frac{n-1}{2} & \frac{n+1}{2} \end{bmatrix} \in \mathrm{PSL}(2,\mathbb{Z})$ and $n = \left|\left(\frac{n-1}{2}\right)^2 - \left(\frac{n+1}{2}\right)^2\right|$.

(2) Suppose n is good and even. Then $n = |c^2 - d^2|$ for relatively prime integers c and d. Since $(c+d) = (c-d) + (2d) = (c-d)+$(even number) and $n = |c+d| \cdot |c-d|$ is even, both $c+d$ and $c-d$ must be even. Hence $n = |c+d| \cdot |c-d|$ is a multiple of 4.

If $n = 8k+4$ for some integer k, then

$$2k+1 = \frac{n}{4} = \left|\frac{c+d}{2}\right| \left|\frac{c-d}{2}\right|.$$

Thus $\frac{c+d}{2}$ and $\frac{c-d}{2}$ are both odd, which implies that c and d are both even. This is absurd, since c and d are relatively prime. Thus we must have $n = 8k$ for some integer k.

Conversely, suppose $n = 8k$ for some integer k. Then

$$c := 2k+1 \quad \text{and} \quad d := 2k-1$$

are relatively prime and $c^2 - d^2 = 8k = n$. This completes the proof. □

Let n_1 be a positive divisor of a positive integer n and $n_2 = n/n_1$. The positive integer n_1 is called a *good divisor* if $\frac{n_1+n_2}{2}$ and $\frac{n_1-n_2}{2}$ are relatively prime integers. A pair (n_1, n_2) of positive integers is called *good* if n_1 is a good divisor of $n = n_1 n_2$. Note that (n_1, n_2) is a good pair if and only if (n_2, n_1) is a good pair.

THEOREM 4. (0) *If $n = c^2 - d^2 > 0$ for some relatively prime positive integers c and d, then*

$$c = \frac{n_1+n_2}{2}, \quad d = \frac{n_1-n_2}{2}$$

for some good pair (n_1, n_2) for n.
(1) *A positive integer n is good if and only if it has a good divisor.*
(2) *If the number of distinct prime factors of a good integer n is k, then there are 2^k good divisors of n.*

(3) *If $n = p_1 \cdots p_k$ is good where $p_1, \dots, p_k$ are powers of distinct odd prime numbers, then*

$$1, \quad p_1, \ \dots, \ p_k, \quad p_1p_2, \ \dots, \ p_{k-1}p_k,$$
$$p_1p_2p_3, \ \dots, \ p_{k-2}p_{k-1}p_k, \quad \dots, \quad p_1 \cdots p_k$$

are all good divisors of n.

(4) *If $n = 2^m p_2 \cdots p_k$ is good where $p_2, \dots, p_k$ are powers of distinct odd prime numbers and $m \geq 3$, then*

$$2, \quad 2p_2, \ \dots, \ 2p_k, \quad 2p_2p_3, \ \dots, \ 2p_{k-1}p_k, \quad \dots, \quad 2p_2 \dots p_k,$$
$$2^{m-1}, \ 2^{m-1}p_2, \ \dots, 2^{m-1}p_k, \ 2^{m-1}p_2p_3,$$
$$\dots, \ 2^{m-1}p_{k-1}p_k, \ \dots, \ 2^{m-1}p_2 \dots p_k$$

are all good divisors of n.

PROOF. (0) Let $n_1 := c+d$ and $n_2 := c-d$. Then $n_1n_2 = c^2-d^2 = n$. Now $n_1+n_2(= 2c)$ and $n_1-n_2(= 2d)$ are even, and $\gcd\left(\frac{n_1+n_2}{2}, \frac{n_1-n_2}{2}\right) = \gcd(c, d) = 1$. Thus (n_1, n_2) is good.

(1) This follows from (0).

(2) This follows from (3) and (4).

(3) Suppose that n_1 is a good divisor of n and $n_2 := n/n_1$. Since n is odd, both n_1 and n_2 are odd. If d is a common divisor of n_1 and n_2, then it is odd and is a common divisor of $(n_1 + n_2)/2$ and $(n_1 - n_2)/2$. Since n_1 is good for n, $d = 1$. Thus n_1 and n_2 are relatively prime. This implies the assertion.

(4) Suppose n_1 is a good divisor of n and $n_2 := n/n_1$. Since n is even and n_1+n_2 is even, n_1 and n_2 are both even. Since $\frac{n_1}{2} + \frac{n_2}{2}$ and $\frac{n_1}{2} - \frac{n_2}{2}$ are relatively prime, so are $\frac{n_1}{2} + \frac{n_2}{2}$ and n_2. Thus $\frac{n_1}{2} + \frac{n_2}{2}$ is odd, and hence $\frac{n_1}{2} + \frac{n_2}{2}$ and $\frac{n_2}{2}$ are relatively prime. Thus $\frac{n_1}{2}$ and $\frac{n_2}{2}$ are relatively prime. The assertion follows from this. □

THEOREM 5. *Let n be a good integer greater than 1.*

(1) *If k is the number of distinct prime factors of n, then, in the picture of $\mathbf{P}$, there are exactly 2^k circles of radius $1/n$ whose centers are in the interval $(0, 1)$.*

(2) *The centers of the above circles are*

$$\frac{2an_1n + n_1^2 - n}{n\left(n + n_1^2\right)}$$

for good divisors n_1 of n, where a is an integer such that

$$0 < a < \frac{n_1 + n_2}{2}, \qquad a\frac{n_1 - n_2}{2} \equiv 1 \pmod{\frac{n_1 + n_2}{2}}$$

and $n_2 = n/n_1$.

PROOF. Let (n_1, n_2) be a good pair for n and let

$$c = \frac{n_1 + n_2}{2} \geq \sqrt{n} \geq \sqrt{2}, \quad d = \frac{n_1 - n_2}{2}.$$

Then there exists a unique pair (a, b) of integers such that

$$ad - bc = 1, \qquad 0 \leq a < c.$$

Note that a must be positive, for otherwise we would have $-bc = 1$ and $c \geq \sqrt{2}$. Now

$$\begin{aligned}(ac - bd)c =& ac^2 - bcd = ac^2 - (ad - 1)d \\ &= a(c^2 - d^2) + d = an + d \geq n + d > 0.\end{aligned}$$

Thus $ac - bd > 0$. Moreover,

$$(c^2 - d^2 - (ac - bd))c = nc - (an + d) = n(c - a) - d \geq n - d > 0$$

and hence $ac - bd < c^2 - d^2$. We have, therefore,

$$0 < \frac{ac - bd}{c^2 - d^2} < 1.$$

Note that the centers

$$\frac{ac - bd}{c^2 - d^2} = \frac{an + d}{nc} = \frac{2an + n_1 - n_2}{n(n_1 + n_2)} = \frac{2an_1n + n_1^2 - n}{n(n + n_1^2)}$$

are distinct for distinct good divisors n_1 of n. Thus, in the picture, there are exactly 2^k circles of radius $1/n$ whose centers lie in the interval $(0, 1)$. This completes the proof. □

Now we introduce an algorithm to draw a picture of **P**.

Algorithm: $\texttt{Pic}[x_0, x_1, y_1, m]$

Step -2: Specify the size of the picture:

$$x_0 \leq x \leq x_1, \quad 0 \leq y \leq y_1.$$

Step -1: Specify the radius $1/m$ of the smallest circle for some good integer m.

Step 0: Draw vertical lines joining the points $(k+\frac{1}{2}, 0)$ and $(k+\frac{1}{2}, y_1)$ for integers k such that $x_0 \leq k + \frac{1}{2} \leq x_1$.

Step 1: Draw half circles of radius 1 centered at $(k, 0)$, where k is an integer such that $x_0 \leq k \leq x_1$.

Step n: For each good integer n with $1 < n \leq m$, draw half circles of radius $1/n$ centered at $\frac{2an_1n+n_1^2-n}{n(n+n_1^2)}$, where n_1 is a good divisor of n and a is as stated in Theorem 5.

This algorithm contains the factorization of integers, and hence it may be slow at the current state. Figure 5 shows the picture of **P** obtained from the algorithm `Pic[-1,1,1.5,200]`.

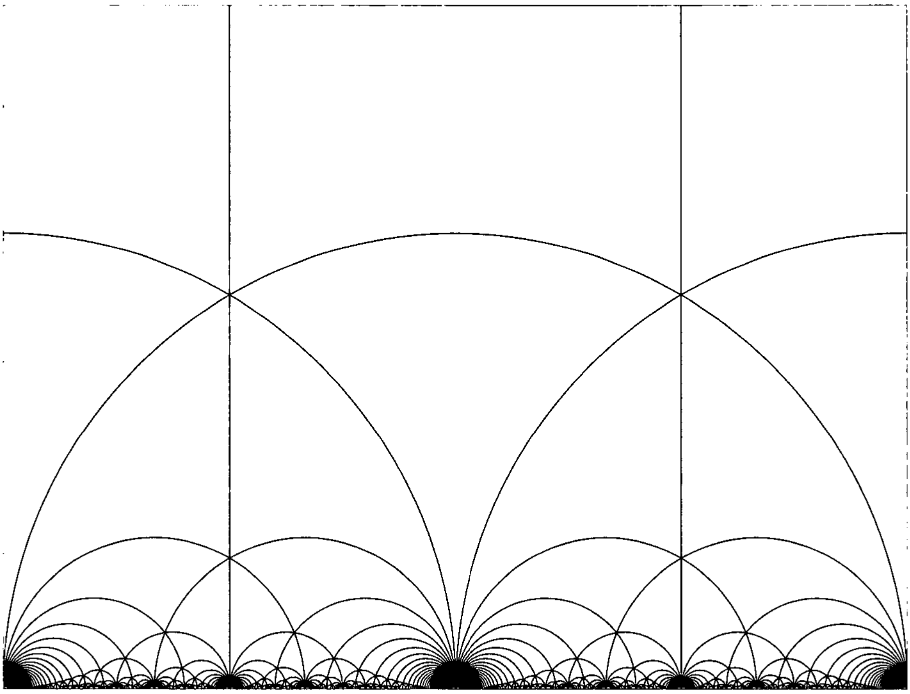

FIGURE 5. `Pic[-1,1,1.5,200]`

REMARK 1. Each rational number is the left and right end point for infinitely many circles. This can be shown as follows.

Suppose we are given a rational number e such that $0 \leq e < 1$. Then there exist relatively prime nonnegative integers p and q such that $e = q/p$. Now take integers b and d satisfying

$$qd - bp = 1. \tag{3}$$

Then

$$a := q - b, \qquad c := p - d$$

implies $q = a + b$, $p = c + d$ and

$$ad - bc = (q - b)d - b(p - d) = qd - bp = 1.$$

Moreover $e = \frac{q}{p} = \frac{a+b}{c+d}$.

Thus e is an end point of the circle $\begin{bmatrix} a & b \\ c & d \end{bmatrix} S$. The reciprocal of the radius of this circle is

$$\frac{1}{r} = |c^2 - d^2| = |(p-d)^2 - d^2| = |p^2 - 2pd| = p|p - 2d|.$$

Note that there exists a unique integer $d = d_0$ which satisfies the equation (3) for some $b = b_0$ and $0 \leq d_0 < p$. Then all the other solutions are

$$d = d_0 - kp, \quad b = b_0 - kq$$

for some integers k. Now we have

$$\frac{1}{r} = p\,|(1+2k)p - 2d_0|\,.$$

Therefore if $k \geq 1$, then $|c| > |d|$ and e is the left end point of a circle of radius $1/p((1+2k)p - 2d_0)$. And if $k \leq -1$, then $|c| < |d|$ and e is the right end point of a circle of radius $1/p(2d_0 - (1+2k)p)$.

REMARK 2. The matrices

$$L := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad R := \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

are well known generator of $\mathrm{SL}(2,\mathbb{Z})$ and the local Cayley daigram (cf. Farmer [1]) of $\mathrm{SL}(2,\mathbb{Z})$ is shown in the Figure 6, although the global Cayley diagram is invariant under the right multiplication map and contains loops.

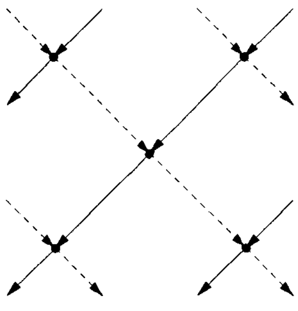

FIGURE 6. Local Cayley diagram of $\mathrm{SL}(2,\mathbb{Z})$

REMARK 3. There is a one-to-one correspondence between the set of chambers (i.e. connected components) of $(\mathbb{H} - \mathbf{P})$ and $\mathrm{PSL}(2,\mathbb{Z})$ in a canonical way. Thus the complement of our picture is a picture of PSL$(2,\mathbb{Z})$. Note that if

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad T = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix},$$

then

$$U^2 = 1 = T^3.$$

T is a hyperbolic rotation of 120 degree with center at $e^{2\pi i/3}$. U and T generate PSL$(2,\mathbb{Z})$. In fact PSL$(2,\mathbb{Z})$ is the free product of the cyclic groups $\langle U \rangle$ and $\langle T \rangle$. (See Jacobson [2], p.90 or Serre [3].) Some of the elements of PSL$(2,\mathbb{Z})$ are shown in Figure 7.

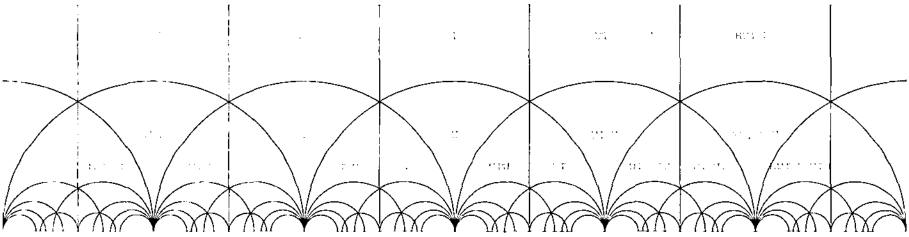

FIGURE 7. PSL(2,$\mathbb{Z}$)

The chambers are hyperbolic triangles and there are six chambers around every finite vertex. The Cayley diagram around any finite vertex looks like the Figure 7, where R_g denotes the right multiplication by g.

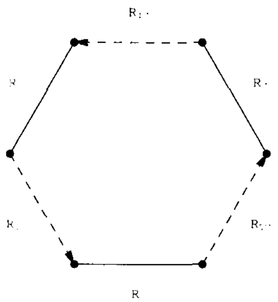

FIGURE 8. The Cayley diagram around a vertex

Thus if we know the names for two adjacent chambers, then the names for the neighboring chambers are determined by the Cayley diagram.

Now we have a complete description of PSL$(2,\mathbb{Z})$.

References

[1] D. Farmer, *Groups and Symmetry. A guide to discovering mathematics*, Amer Math. Soc., 1996.
[2] N. Jacobson, *Basic Algebra II. Second edition*, W. H. Freeman and Company 1989.
[3] J. P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, no. 7 Springer-Verlag, 1973.

Department of Mathematics Education
Korea University
Seoul 136-701, Korea
E-mail: hongchan@korea.ac.kr