

# CONTINUED FRACTIONS

ISHAN LEVY

## 1. THE MAGIC BOX AND CONVERGENTS

Given a ring  $R$ , a **simple continued fraction**  $[a_0, a_1, \dots, a_n]$  is an expression defined via  $[a_0] = a_0$  and  $[a_0, \dots, a_n] = a_0 + \frac{1}{[a_1, \dots, a_n]}$ . In the case that  $R$  has a topology, we can define infinite continued fractions as limits of finite ones. We call the sequence  $r_k = [a_1, \dots, a_k]$  the **convergents** of the continued fraction. Some easily verified identities for continued fractions are:

$$[a_0, \dots, a_k, \dots, a_n] = [a_0, \dots, a_{k-1}, [a_k, \dots, a_n]]$$

$$[0, a_0, \dots, a_n] = \frac{1}{[a_0, \dots, a_n]}$$

The convergents are computable using an algorithm called the **magic box**. The magic box works as follows: let  $\begin{pmatrix} b_{-2} & b_{-1} \\ c_{-2} & c_{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  and define  $b_i = b_{i-2} + b_{i-1}a_i$ ,  $c_i = c_{i-2} + c_{i-1}a_i$ . Then  $\frac{b_k}{c_k}$  is  $r_k$ , the  $k^{th}$  convergent.

This can be proven by inducting on  $k$ . The base case is easy to verify. In general, note that  $[a_0, \dots, a_k] = [a_0, \dots, a_{k-1} + \frac{1}{a_k}]$ . Thus we can apply the result for  $[a_0, \dots, a_{k-1} + \frac{1}{a_k}]$  to get that the  $n^{th}$  convergent is  $\frac{b_{k-1} + \frac{b_{k-2}}{a_k}}{c_{k-1} + \frac{c_{k-2}}{a_k}} = \frac{a_k b_{k-1} + b_{k-2}}{a_k c_{k-1} + c_{k-2}}$ .

The reason it is called the magic box is because the entries  $a_i, b_i, c_i$  can be neatly computed in a box as shown below:

		$a_0$	$a_1$	$\dots$	$a_n$
$0$	$1$	$b_0$	$b_1$	$\dots$	$b_n$
$1$	$0$	$c_0$	$c_1$	$\dots$	$c_n$

It is worth pointing out that the two rows of the magic box have a symmetry, namely that if a 0 is inserted in the beginning of the  $a_i$  sequence, then the values of  $b_n$  and  $c_n$  switch. This corresponds to the second continued fraction identity mentioned at the beginning. Now we will see another symmetry of the magic box, and hence of continued fractions.

The magic box is related to solutions of linear Diophantine equations. Namely, if  $[a_0, \dots, a_n]$  is a continued fraction for  $\frac{b_n}{c_n}$  (the terms in the magic box), then we can find a solution of the equation  $b_n x - c_n y = 1$  in the ring generated by the  $a_i$  using the magic box. Namely, we just reverse the order of the  $a_i$  and compute the magic box for  $d_n, e_n$ , as shown below:

$$\begin{array}{cc|cccc} & & a_n & a_{n-1} & \dots & a_0 \\ \hline 0 & 1 & d_0 & d_1 & \dots & d_n \\ 1 & 0 & e_0 & e_1 & \dots & e_n \end{array}$$

First note that  $d_{n-1}e_n - d_n e_{n-1} = (-1)^n$ . Indeed the determinant of the  $2 \times 2$  matrix on the left hand side is clearly  $-1$  verifying the base case. If we plug in the recurrence relation for the magic box, we will inductively get the result. Now the claim is that  $d_n = b_n, d_{n-1} = c_n$ . By the symmetry property of the  $d_i$  and  $e_i$  it will then follow that  $e_n = b_{n-1}$ , and by the determinant property it will follow that  $e_{n-1} = c_{n-1}$ . These identities along with the fact that the magic box computes the convergents will give the identity:

$$\frac{[a_0, \dots, a_n]}{[a_0, \dots, a_{n-1}]} = \frac{[a_n, \dots, a_0]}{[a_n, \dots, a_1]}$$

To show the claim about  $d_n, d_{n-1}$ , one simply has to note that the recurrence relation for the magic box is essentially the one used to obtain solutions of linear Diophantine equations from the quotients in the Euclidean algorithm. Namely,  $\frac{1}{[a_1, \dots, a_n]} = [a_0, \dots, a_n] - a_0 = \frac{b_n}{c_n} - a_0 = \frac{b_n - c_n a_0}{c_n}$ . If by the induction hypothesis we assume that the result holds for continued fractions of length  $n - 1$ , then the recurrence relation will show that it holds for  $n$ . Indeed the calculation shown here is exactly that done via the Euclidean algorithm if  $a_0$  is the floor of the quotient of  $b_n, c_n$ . Then the magic box is a repackaging of the usual algorithm that constructs the solutions of linear Diophantine equations.

## 2. REAL CONTINUED FRACTIONS AND RATIONAL APPROXIMATIONS

Given a real number  $r$ , there is a unique way to write as a (possibly finite) simple continued fraction  $[a_0, \dots]$  such that each  $a_i$  an integer,  $a_i$  nonnegative for  $i > 0$ , and  $a_i = 0 \implies a_j = 0$  if  $j > i$ . Indeed,  $a_0$  must be  $\lfloor r \rfloor$ . If  $r$  is not an integer,  $[a_1, \dots]$  must be equal to  $\frac{1}{r - \lfloor r \rfloor}$ , which is positive and strictly greater than 1. Thus each of the next  $a_i$  will be nonnegative, and if one of them is zero, the rest are 0 as well, as this happens only when one step gives an integer. The fact that the euclidean algorithm terminates shows that one of them is zero iff  $r$  is a rational number. This particular continued fraction will be called *the* continued fraction of the real number

$r$ . If  $r$  is irrational, the convergents will converge to  $r$ . First observe that by the construction of the  $a_i$  the  $k^{\text{th}}$  partial convergent is an underestimate of  $r$  if  $k$  is even, and an overestimate otherwise. Now by the magic box, if  $r_k = \frac{b_k}{c_k}$  is the  $k^{\text{th}}$  partial convergent, then  $\frac{b_k}{c_k} - \frac{b_{k+1}}{c_{k+1}} = \frac{\pm 1}{c_k c_{k+1}}$ . If the  $a_i$  are eventually 0, then one of the convergents is the rational number, so the convergents converge, and by the remark about over and underestimating  $r$ , they must converge to  $r$ . We see in particular that any sequence  $a_k$  satisfying the conditions will determine a unique real number.

The partial convergents of  $r$  are really good approximations of it. Namely, note that  $|\frac{b_k}{c_k} - r| = |r_k - r| \leq |r_k - r_{k+1}| \leq \frac{1}{c_k c_{k+1}} \leq \frac{1}{c_k^2}$ . This is a surprisingly good approximation, considering that we might expect the best rational approximation of  $r$  with denominator  $c_k$  to have error at most  $\frac{1}{2c_k}$ .

Let  $F_k$  denote the Farey sequence of rational numbers between 0 and 1 with denominator less than or equal to  $k$ . We will write all fractions in their reduced form.

**Lemma 2.1.** *If  $\frac{a}{b}$  is right before  $\frac{c}{d}$  in the  $F_k$ . then  $ad - bc = -1$ . If  $\frac{a}{b}, \frac{c}{d}$  are consecutive, and  $\frac{p}{q}$  is any rational between them, then  $\frac{p}{q} = \frac{k_1 a + k_2 c}{k_1 b + k_2 d}$  for some positive  $k_1, k_2$ . If there is one rational number in  $F_k$  between  $\frac{a}{b}$  and  $\frac{c}{d}$ , then it is given by  $\frac{a+c}{b+d}$ . If the determinant  $ad - bc = \pm 1$ , then  $\frac{a}{b}, \frac{c}{d}$  are neighbors in the Farey sequence  $F_{b+d-1}$  and the rationals between them in reduced form are  $\frac{k_1 a + k_2 c}{k_1 b + k_2 d}$  where  $(k_1, k_2) = 1$ . The determinant is 1 iff the two rationals are consecutive in some  $F_k$ .*

*Proof.* It is clearly negative. Consider the parallelogram generated by  $(a, b), (c, d)$ . The region between the ray generated by  $(a, b)$  and  $(c, d)$  can canonically be tiled with these parallelograms. If  $(a, b)$  are right next to each other, then the triangle between  $(0, 0), (a, b), (c, d)$  can have no interior points so the triangle has area  $\frac{1}{2}$ , and hence the parallelogram has area 1, which proves the first result. We can tile the region between the rays generated by  $(a, b), (c, d)$  with these parallelograms to get the second result. Suppose  $\frac{e}{f}$  is the only thing between  $\frac{a}{b}, \frac{c}{d}$  in the Farey sequence. If  $(a + c, b + d)$  lied strictly in the interior of the region between the rays generated by  $(e, f)$ , and one of  $(a, b), (c, d)$  (WLOG  $(a, b)$ ), we can subtract  $(a, b)$  from it to get that  $(c, d)$  lies in the region between the rays, which is impossible. Thus it must lie on the ray generated by  $(e, f)$ . The next statement follows from the tiling by parallelograms again, and the last statement follows from the second last.  $\square$

**Lemma 2.2.** *Each convergent of a real number is closer than the last.*

*Proof.* Write  $r = [a_0, \dots, a_n, b_n]$ , where  $a_n$  agree with the continued fraction for  $r$ . Then if  $\frac{b_n}{c_n}$  are the usual convergents of  $r$ , one computes  $|r - \frac{b_n}{c_n}| = \frac{1}{c_n(c_n b_n + c_{n-1})}$ . We compute  $|r - \frac{b_{n+1}}{c_{n+1}}| = \frac{b_n - \lfloor b_n \rfloor}{c_{n+1}(c_n b_n + c_{n-1})}$ , which is clearly smaller.  $\square$

**Theorem 2.3.** *If  $r_k = \frac{b_k}{c_k}$  are the convergents of  $r$ ,  $k > 0$ , then they are best approximation of  $r$  with denominator at most  $c_k + c_{k-1} - 1$ .*

*Proof.* Since  $k > 0$  we can assume WLOG  $r$  is between 0 and 1. Then this follows from the lemma about the Farey sequences, and the facts that the determinant between  $r_k$  and  $r_{k-1}$  is  $\pm 1$ , and that  $r_k$  is the better approximation.  $\square$

There is another sense in which we can ask that the continued fraction be a good approximation of  $r$ . Namely we can say that  $\frac{p}{q}$  is a good approximation if  $|qr - p|$  is small. Our bounds from before show that if  $\frac{b_k}{c_k}$  are the convergents of  $r$ , then  $|c_k r - b_k| < \frac{1}{c_{k+1}}$ . We should note that the proof of Lemma 2.2 actually shows:

**Lemma 2.4.**  $|c_k r - b_k| > |c_{k+1} r - b_{k+1}|$ .

Thus the convergents get closer in this sense as well.

**Theorem 2.5.**  $\frac{p}{q}$  is a reduced convergent of  $r$  with  $q \geq c_1$  iff for all different  $\frac{a}{b}$  with  $b \leq q$ ,  $|qr - p| < |br - a|$ .

*Proof.* The case when  $b = q$  is covered from the statement about Farey sequences. If  $b$  is not the denominator of a convergent, let  $c_k < b < c_{k+1}$ . We can interpret the statement as with Farey sequences by observing that  $|qr - p|$  is the horizontal distance from the point  $(p, q)$  to the line  $(cr, c)$ . If  $(a, b)$  lies outside the area between the rays generated by  $(b_k, c_k)$  and  $(b_{k-1}, c_{k-1})$ , then it certainly cannot be closer to the line  $(cr, c)$  than either of them. If it is inside, then by Lemma 2.1,  $(a, b)$  is a positive linear combination of  $(b_k, c_k)$  and  $(b_{k-1}, c_{k-1})$ , with coefficients  $i_1, i_2$ . Note that  $c_{k+1}$  is when  $i_1 = 1$  and  $i_2 = a_{k+1}$ , and it is defined so that  $i_1 = 1$  and  $i_2 = a_{k+1} - 1$  lies on the same side of the line  $(cr, c)$  as  $(b_{k-1}, c_{k-1})$ . Thus the closest  $(a, b)$  could get to the line is  $(b_{k-1} + (a_{k+1} - 1)b_k, c_{k-1} + (a_{k+1} - 1)c_k)$ . But since  $(b_{k+1}, c_{k+1}), (b_k, c_k)$  lie on different sides of the line, we have  $|r(b_{k-1} + (a_{k+1} - 1)b_k) - (c_{k-1} + (a_{k+1} - 1)c_k)| = |rb_{k+1} - c_{k+1}| + |rb_k - c_k|$ , giving the result.  $\square$

**Proposition 2.6.** *An irrational  $r$  has infinitely many rational approximations  $\frac{p}{q}$  with error less than  $\frac{1}{2q^2}$ . Every such rational number is a convergent. For any  $\epsilon, c > 0$ , A rational number has finitely many approximations  $\frac{p}{q}$  with error at most  $\frac{c}{q^{1+\epsilon}}$ .*

*Proof.* The inequality holds for at least one out of every two convergents. Otherwise, we have  $\frac{1}{c_k c_{k+1}} = |\frac{b_k}{c_k} - \frac{b_{k+1}}{c_{k+1}}| \geq \frac{1}{2c_k^2} + \frac{1}{2c_{k+1}^2}$ , which cannot be an equality as  $c_k < c_{k+1}$ . Conversely, if the inequality is satisfied for  $\frac{a}{b}$ , then we will show that  $\frac{a}{b}$  satisfies the theorem above. Let  $\frac{c}{d}$  be any different reduced fraction which is closer in the sense of the above theorem. Then  $\frac{1}{bd} \leq |\frac{a}{b} - \frac{c}{d}| \leq |\frac{a}{b} - r| + |\frac{c}{d} - r| \leq \frac{1}{2b^2} + \frac{1}{2bd}$ , which implies  $b < d$ .

For the last statement, if our rational number is  $\frac{a}{b}$  and we want  $|\frac{a}{b} - \frac{p}{q}| \leq \frac{c}{q^{1+\epsilon}}$ . WLOG we can assume  $\frac{p}{q} \leq \frac{a}{b}$ ,  $a, q > 0$ . Then  $aq^{1+\epsilon} - pq^\epsilon b \leq b$ , so  $q$  is bounded, and takes finitely many values.  $p$  does as well.  $\square$

Let's define some notation. If  $x, y \in \mathbb{R}$ , we can say that  $x \rightarrow y$  if  $y = \frac{1}{x - [x]}$ , and  $x \twoheadrightarrow y$  if  $x \rightarrow x_1 \rightarrow x_2 \rightarrow \dots y$ . Clearly if  $x = [c_0, \dots], y = [c'_0, \dots]$  are the continued fractions, then  $x \rightarrow y$  iff  $c'_i = c_{i+1}$ .

**Lemma 2.7.**  $\exists x$  such that  $x \rightarrow y$  iff  $y > 1$ .

*Proof.* Then if  $x \rightarrow y$ , this is clear, and conversely, we can let  $x$  be  $\frac{1}{y} + n$  for any  $n$ .  $\square$

### 3. CONTINUED FRACTIONS OF REAL QUADRATIC NUMBERS

Suppose that the continued fraction of some irrational  $x$  is repeating, i.e  $x \twoheadrightarrow x$ . Then we can write  $x = [a_0, \dots, a_n, x]$ . We can simplify the right hand side to a quotient of two linear polynomials in  $x$ , showing that  $x$  is the root of a quadratic equation. More precisely if  $\frac{d_i}{e_i}$ , by the magic box,  $x = \frac{d_n x + d_{n-1}}{e_n x + e_{n-1}}$ , so  $x = \frac{-(e_{n-1} - d_n) \pm \sqrt{(e_{n-1} - d_n)^2 + 4e_n d_{n-1}}}{2e_n}$ . Using the determinant identity from the magic box, this is equal to  $x = \frac{-(e_{n-1} - d_n) \pm \sqrt{(e_{n-1} + d_n)^2 + 4(-1)^n}}{2e_n}$ . Replace  $n$  with  $kn$ , and let  $k \rightarrow \infty$  and noting that  $e_n \rightarrow \infty$ , the two roots are  $\lim_{k \rightarrow \infty} -\frac{e_{kn-1}}{e_{kn}}$  for negative, and  $\lim_{k \rightarrow \infty} \frac{d_{kn}}{e_{kn}}$  for positive. But the first is  $y| \frac{-1}{y} = [a_n, \dots, a_0, y]$ , and the latter is  $x$ , so we get:

**Theorem 3.1.** *If  $x$  has continued fraction  $[a_0, \dots, a_n, x]$ , then  $x = \frac{-(e_{n-1} - d_n) + \sqrt{(e_{n-1} + d_n)^2 + 4(-1)^n}}{2e_n}$  where  $\frac{d_n}{e_n}$  is the  $n^{\text{th}}$  convergent. Moreover,  $a_i, d_i, e_i > 0$ ,  $x > 1, -1 < \bar{x} < 0$ , and  $\frac{-1}{\bar{x}} = [a_n, \dots, a_0, \frac{-1}{\bar{x}}]$ .*

Even if  $x$  has a continued fraction that eventually repeats, i.e.  $x \twoheadrightarrow y \twoheadrightarrow y$ , we can subtract the first few terms and take reciprocals to get another number with repeating continued fraction, so  $x$  will lie in the field generated by that element, hence will again be the root of some quadratic polynomial.

In the case that  $x = \sqrt{d}$ , there is a fast way to organize the computation of the continued fraction of  $x$ . Normally, at each step, we would expect to have something of the form  $\frac{a+g\sqrt{d}}{b}$ , subtract its floor, and compute its reciprocal in  $\mathbb{Q}[\sqrt{d}]$ . However in this case, at every step,  $g = 1$ ! To see this, let  $c$  be the floor of  $\frac{a+\sqrt{d}}{b}$ . Then at the next step we will have  $\frac{b(bc-a+\sqrt{d})}{-N(a-bc+\sqrt{d})}$ . So in the next step  $g = 1$  iff  $b|N(a-bc+\sqrt{d})$  iff  $a^2 \equiv d \pmod{b}$ . If this is the case, then letting  $x = bc - a$ ,  $y = \frac{d-x^2}{b}$ , we get that

the number at the next step is  $\frac{x+\sqrt{d}}{y}$ . Note that  $x^2 \equiv d \pmod{y}$  by definition of  $y$ . Thus if  $g = 1$  at one step and  $a^2 \equiv d \pmod{b}$ , then  $g = 1$  at every step. Moreover, we have seen how to compute the next step, and we can organize this information into a table called the **super magic box**.

We will consider the super magic box for  $\frac{a_0+\sqrt{n}}{b_0}$ , where  $a_0^2 \equiv n \pmod{b_0}$ . Note that the congruence condition can always be arranged by multiplying the denominator and numerator by a sufficiently divisible number (for example  $b_0$ ). Let  $w = \lfloor \sqrt{n} \rfloor$ . Then we write a table

$$\begin{array}{c|ccc} a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_n \\ \hline c_0 & c_1 & \dots & c_n \end{array}$$

$$\text{where } a_i = b_{i-1}c_{i-1} - a_{i-1}, \quad b_i = \frac{n-a_i^2}{b_{i-1}}, \quad c_i = \lfloor \frac{a_i+w}{b_i} \rfloor.$$

Then  $\frac{a_i+\sqrt{n}}{b_i} = [c_i, c_{i+1}, \dots]$ , so in particular the  $c_i$  are convergents of the original number.

We can bound  $b_{i+1}$  in terms of  $b_i$  and  $n$ . Note that WLOG we can assume  $c_i = 0$  by subtracting it off. Now, assume that  $b_i > 0$ . Thus  $b_{i+1} = \frac{n-a_i^2}{b_i}$ . Clearly  $b_{i+1} \leq \frac{n}{b_i}$ . Now note that  $b_i - \sqrt{n} \geq a_i \geq -\sqrt{n}$ . This shows that either  $|b_{i+1}| < |b_i| - 2\sqrt{n}$  or  $|b_{i+1}|$  is less than  $\max\{n, 2\sqrt{n}\}$ . If  $b_i < 0$ ,  $\sqrt{n} - b_i \geq -a_i \geq \sqrt{n}$ . It follows that  $0 \leq b_{i+1} \leq -b_i + 2\sqrt{n}$ . Thus it follows that  $|b_i| \leq 2\sqrt{n} + \max\{|b_0|, n\}$  so that there are only finitely many values it takes on. The bounds for  $a_i$  above in general give bounds on  $a_{i+1}$  dependant on  $b_i$ , so there are also finitely many possibilities for the  $a_i$ . Thus the columns of the super magic box repeat and we get:

**Theorem 3.2.**  *$a$  has an eventually repeating continued fraction iff  $a$  lies in a real quadratic field. When it repeats,  $c_i, b_i, a_i > 0$ ,  $2a_i, b_i < 2\sqrt{n}$ .*

*Proof.*  $c_i$  is clearly positive,  $b_i$  is positive by the theorem on irrationals with repeating continued fractions, and  $a_i$  is positive since  $\frac{a_i-\sqrt{n}}{b_i} \in (-1, 0)$ , and  $\frac{a_i+\sqrt{n}}{b_i} > 1$  which implies the bound. The average of the number and its conjugate is  $\frac{a_i}{b_i}$ , which cannot be negative, so  $a_i > 0$ .  $a_i < \sqrt{n}$  follows from the fact that  $\frac{a_i-\sqrt{n}}{b_i}$  is negative.  $\square$

When does a number  $r$  have strictly repeating continued fraction? A necessary condition is that  $r > 1$  and  $\bar{r} \in (-1, 0)$ . Is this sufficient? Say that  $r$  is **regular** if it is in some real quadratic field and satisfies these two conditions. We can try to run the magic box backwards.

**Lemma 3.3.** *If  $r$  is regular, then there is a unique regular  $r_{-1}$  with  $r_{-1} \rightarrow r$ .*

*Proof.*  $0 < \frac{1}{r} < 1$  and  $\frac{1}{r} < -1$ . Thus there is a unique number such  $n > 0$  such that  $\frac{1}{r} + n \in (-1, 0)$ . Let  $r_{-1} = \frac{1}{r} + n$ .  $\square$

Thus we can run a reverse super magic box on  $r$ . One has to check via a calculation that this works with some constant number in the square root. By the bounds for Theorem 3.2,  $a_i, b_i$  take on finitely many values. Thus it eventually repeats. But going forward, this means that  $r$  has a repeating continued fraction! We obtain:

**Theorem 3.4.**  *$r$  is regular iff  $r$  has a repeating continued fraction.*

As an application, we can study the continued fraction of  $\sqrt{r}$  where  $r$  is a positive rational.

**Theorem 3.5.** *If  $r > 1$  is a rational, then  $\sqrt{r}$  has a continued fraction of the form  $[a_0, \overline{a_1, \dots, a_r}]$ , where the line signifies repetition. Moreover,  $a_r = 2a_0$ , and  $a_i = a_{r-i+1}$ .*

*Proof.* To see that the continued fraction is of that form, we only need to note that  $\sqrt{r} + \lfloor \sqrt{r} \rfloor$  satisfies the conditions of the theorem above. To see the last two conditions, note that  $\frac{-1}{\sqrt{r}} = \frac{1}{\sqrt{r}}$  so that  $\sqrt{r} = [a_0, \overline{a_1, \dots, a_r}] = [a_0, \overline{a_1, \dots, a_r}] = [a_0, \overline{a_1, \dots, a_r - a_0, 0, a_0}] = [a_0, \overline{a_1, \dots, a_r - a_0, 0}]$  but on the other hand it is equal to  $[0, \overline{0, a_r - a_0, a_{r-1} \dots a_0}] = [\overline{a_r - a_0, a_{r-1} \dots a_0, 0}] = [a_r - a_0, \overline{a_{r-1} \dots a_0, 0, a_r - a_0}] = [a_r - a_0, \overline{a_{r-1} \dots a_1, a_r}]$  by the last part of Theorem 3.1.  $\square$

Given a non-square  $d$ , we can find all solutions  $(x, y)$  to Pell's equation,  $x^2 - dy^2 = \pm 1$  using continued fractions. This is the same as finding a  $x + \sqrt{d}y$  with norm  $\pm 1$ . WLOG, we can assume  $x, y > 0$ , which is the same as restricting to  $x + \sqrt{d}y > 1$ .

**Theorem 3.6.** *If  $x, y > 0$ , and  $(x, y)$  solves Pell's equation,  $\frac{x}{y}$  is a convergent of  $\sqrt{d}$ . Infinitely many such solutions exist, and are powers of a fundamental solution.*

*Proof.*  $|x^2 - dy^2| = 1 \implies |\frac{x}{y} - \sqrt{d}| \leq \frac{1}{y^2 |\frac{x}{y} + \sqrt{d}|} \leq \frac{1}{2y^2}$ , so  $x, y$  is a solution. To see that a solution exists, note that  $|b_k^2 - dc_k^2|$  is bounded above by a constant like  $2d + 1$ . These infinitely many things must generate finitely many ideals, since there are finitely many index  $n$  subgroups of  $\mathbb{Z}^2$ . Thus there are infinitely many units. Taking log of the positive units, they must form a discrete subgroup as the convergents are discrete. Thus there is a fundamental solution.  $\square$

#### 4. FAREY SEQUENCES AND HYPERBOLIC GEOMETRY

A finite continued fraction with integer coefficients takes values in  $\mathbb{QP}^1 = \mathbb{Q} \cup \infty$ . We can define a symmetric relation on  $\mathbb{QP}^1$  by saying that  $a \sim b$  iff  $a = [a_0, \dots, a_n], b = [a_0, \dots, a_{n-1}]$  for some integers  $a_0, \dots, a_n$ . Here are axioms for this relation:

**Lemma 4.1.**  *$\sim$  is the least symmetric relation that is invariant under the action of  $\mathrm{SL}_2(\mathbb{Z})$  (via fractional linear transformations) such that  $0 \sim \infty$ . the action on  $\mathbb{QP}^1$  is transitive.*

*Proof.* Clearly  $0 \sim \infty$ . Moreover,  $[a_0, \dots, a_n] \sim [a_0, \dots, a_{n-1}] \implies [a_0+m, \dots, a_{n-1}] \simeq [a_0+m, \dots, a_n]$  so the relation is invariant under  $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ . Moreover,  $[a_0, \dots, a_n] \sim [a_0, \dots, a_{n-1}] \implies [0, -a_0, \dots, -a_{n-1}] \sim [0, -a_0, \dots, -a_n]$ , so it is invariant under  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  so it is invariant under  $\mathrm{SL}_2(\mathbb{Z})$ . Conversely, if  $0 \sim \infty$ , then  $[] \sim [0]$ , and we can build our relation up from the two operations above.  $\square$

Here is another characterization.

**Lemma 4.2.**  *$\sim$  is the symmetrization of the relation  $\frac{a}{b} \sim \frac{c}{d}$  iff  $ad - bc = 1$  for reduced fractions.  $\mathrm{SL}_2(\mathbb{Z})$  acts transitively on pairs that are related.*

*Proof.* This is clearly  $\mathrm{SL}_2(\mathbb{Z})$ -invariant, and  $\frac{n}{1}$  is related to  $\frac{1}{0}$ , so the relation described is contained in the one we want. Conversely, we can apply  $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$  to  $\infty \sim 0$  to get the other direction, and that the action is transitive.  $\square$

Here is another characterization of the relation using Farey sequences.

**Lemma 4.3.**  *$a \sim \infty \iff a \in \mathbb{Z}$ ,  $a, b \in \mathbb{Q}, a \sim b \implies |a - b| \leq 1$ ,  $a \sim b \iff a + n \sim b + n$ , and if  $0 \leq a, b \leq 1$ ,  $a \sim b$  iff  $a$  and  $b$  are consecutive in some Farey sequence.*

*Proof.* First note that need to observe that by Lemma 2.1, if  $\frac{a}{b}, \frac{c}{d}$  are consecutive in a Farey sequence,  $\mathrm{SL}_2(\mathbb{Z})$ , then  $ad - bc = 1$ , so we can apply the transformation  $\frac{(a-c)z+c}{(b-d)z+d}$  to  $0 \sim 1$ . Thus the relation defined in the theorem is contained in the relation  $\sim$ . Conversely, if  $ad - bc = 1$ ,  $\frac{a}{b}, \frac{c}{d}$  are within 1 of each other, so after subtracting them, they will be in the unit interval, at which Lemma 2.1 applies again to say that they are consecutive.  $\square$

**Lemma 4.4** (Compatibility with the order). *If  $a \sim b, c \sim d$  and  $a \leq c \leq b$ , then  $a \leq d \leq b$ .*

*Proof.* We can assume  $a, b \in [0, 1]$ , for which it follows from Lemma 2.1.  $\square$

Our relation determines some undirected graph on  $\mathbb{Q} \cup \infty$ . We can embed this graph onto the upper graph by taking the geodesics between the two points on the boundary of the upper half plane. This is called the **Farey tiling** of the upper half plane. Note that if  $\gamma_1$  is the geodesic between two real numbers  $\alpha \leq \beta$ , and  $\gamma_2$  is the geodesic between  $a \leq b$ , and  $a \in [\alpha, \beta]$ , then the interiors of  $\gamma_1, \gamma_2$  intersect iff



$b \geq \beta$ . The previous lemma shows that none of these geodesics intersect each other except at the boundary in the Farey tiling.

**Lemma 4.5.** *If  $\frac{a}{b} \sim \frac{c}{d}$ ,  $\frac{a}{b} < \frac{c}{d}$ , then  $\frac{a+c}{b+d}$  is the unique number between them related to both.*

*Proof.* That this is related to both and in between is obvious. To show it is unique, by transitivity of the  $\mathrm{SL}_2(\mathbb{Z})$  action and due to its preservation of the cyclic order on  $\mathbb{Q}\mathbb{P}^1$ , it is enough to consider  $0 = \frac{0}{1} \sim \frac{1}{0} = \infty$ . In this case, it follows since the only positive number  $0, \infty$  are both related to is 1.  $\square$

Define  $m|M$  for rationals  $m, M$  to be the unique number in the lemma above.

**Theorem 4.6.** *Begin with  $m = 0$  and  $M = \infty$ , and let  $\alpha \geq 0$ . We will construct a sequence of letters  $R$ s and  $L$ s as follows: If  $\alpha$  is greater than or equal to  $m|M$ , then we replace  $m$  with  $m|M$  and record a  $R$ . Otherwise, we replace  $M$  with  $m|M$  and record an  $L$ . Repeating this process gives an infinite collection of  $L$ s and  $R$ s. Now count the number of times  $L$ s or  $R$ s happens consecutively, and let  $c_i$  be these numbers.  $c_1$  is the number of times  $R$  happens at the beginning. Then  $[c_0, c_1, \dots]$  is the continued fraction for  $\alpha$ .*

*Proof.* Observe that the number of times  $R$  will appear at the beginning is  $\lfloor \alpha \rfloor$ . Then, apply the transformation  $z \mapsto \frac{1}{z-\alpha}$ , and observe that the number of rights that appear by starting over except using  $\frac{1}{\alpha-\lfloor \alpha \rfloor}$  is exactly the number of lefts that would have appeared right after. Moreover, if  $\alpha = [a_0, \dots]$ , then  $\frac{1}{\alpha-\lfloor \alpha \rfloor} = [a_1, \dots]$ , so by induction we are done.  $\square$

Note that this has the following geometric interpretation: we can find the sequence of  $R, L$ s by taking the geodesic connecting  $\alpha$  and  $-\alpha$  and looking at how it intersects the Farey tiling.