Serret's Theorem

We define the action

$$\mathrm{GL}_2(\mathbb{Z}) \times \mathbb{R} \to \mathbb{R};$$
$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, x\right) \mapsto \frac{ax+b}{cx+d}.$$

This action will be useful to see composition of this map as matrix multiplication.

Definition 1. Let $x, y \in \mathbb{R}$. We say that x is equivalent to y ($x \sim y$) if $\exists A \in \mathrm{GL}_2(\mathbb{Z})$ with $det(A) = \pm 1$ such that $x = Ay$. That is

$$x = \frac{ay+b}{cy+d}, \quad \text{for some } a, b, c, d \in \mathbb{Z} \text{ with } ad - bc = \pm 1.$$

Proposition 1. *"$\sim$" is an equivalence relation.*

Proof. (i) Reflexivity: $x = \mathrm{Id}x$.

(ii) Simmetry: $x = Ay$. We apply A^{-1} to both sides and get $y = A^{-1}x$, where $\det(A^{-1}) = (\det(A))^{-1} = \pm 1$.

(iii) Transitivity: $x = Ay$ and $y = Bz \Rightarrow x = ABz$ with $\det(AB) = \det(A)\det(B) = \pm 1$. □

Lemma 1. *Any two irrational numbers are equivalent.*

Proof. Let $x = p/q \in \mathbb{Q}$ with p, $q \in \mathbb{Z}$ and $\gcd(p, q) = 1$. Then

$$\exists m, n \in \mathbb{Z} : mq - np = 1.$$

Hence

$$\frac{p}{q} = \frac{0 \cdot m + p}{0 \cdot n + q} = \begin{pmatrix} m & p \\ n & q \end{pmatrix} \cdot 0 =: A \cdot 0,$$

with $\det(A) = mq - np = 1$. Hence $x \sim 0$.
Since x was arbitrary the claim follows from transitivity. □

We recall now some properties of continued fractions. We have

$$[a_0; a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

where the a_i's are called partial quotients and $a_n \geq 1$ for $n \geq 1$. We define convergents as

$$\frac{p_n}{q_n} := [a_0; a_1, \dots, a_n].$$

The following holds:

(i) $\forall n \geq 2$

$$\begin{aligned} p_0 &= a_0, & p_1 &= a_1 p_0 + 1, & p_n &= a_n p_{n-1} + p_{n-2}; \\ q_0 &= 1, & q_1 &= a_1 q_0, & q_n &= a_n q_{n-1} + q_{n-2}. \end{aligned}$$

(ii) $\forall n \geq 2$

$$0 \leq q_{n-1} \leq q_n;$$
$$0 \leq |p_{n-1}| \leq |p_n|.$$

Furthermore the p_n's are always all positive or all negative.

(*iii*) $\forall n \geq 2$

$$x = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}},$$

where $x = [a_0; a_1, \ldots, a_{n-1}, x_n]$. The x_n's are called complete quotients.

(*iv*) $\forall n \geq 1$:

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}.$$

(*v*)

$$\begin{aligned} x &\leq \frac{p_n}{q_n}, \quad n \text{ odd}, \\ x &\geq \frac{p_n}{q_n}, \quad n \text{ even}. \end{aligned}$$

(*vi*) $\forall n \geq 0$:

$$0 < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Lemma 2. $\forall n \geq 0$:

$$q_n x - p_n = \frac{(-1)^n \delta_n}{q_{n+1}}.$$

for some $0 < \delta_n < 1$.

Proof. By property (*vi*) we have

$$0 < q_{n+1} |x q_n - p_n| < 1.$$

So with $\delta_n = q_{n+1}|x q_n - p_n|$ it follows

$$|x q_n - p_n| = \frac{\delta_n}{q_{n+1}}.$$

While by property (v) we have

$$\begin{aligned} x q_n - p_n &\leq 0, \quad n \text{ odd}; \\ x q_n - p_n &\geq 0, \quad n \text{ even}. \end{aligned}$$

Hence the claim follows directly. □

Lemma 3. *If*

$$x = \begin{pmatrix} P & R \\ Q & S \end{pmatrix} \omega = \frac{P\omega + R}{Q\omega + S}$$

for some $P, Q, R, S \in \mathbb{Z}$ *with* $Q > S > 0$ *and* $PS - QR = \pm 1$, *then* $\frac{P}{Q}$ *and* $\frac{R}{S}$ *are two consequent convergent of* x, *i.e.*

$$\frac{P}{Q} = \frac{p_n}{q_n}, \quad \frac{R}{S} = \frac{p_{n-1}}{q_{n-1}},$$

for some $n \geq 1$; *and* ω *is a complete quotient of* x, *i.e.*

$$x = [a_0; a_1, \ldots, a_n, \omega].$$

Proof. Let

$$\frac{P}{Q} = \frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n].$$

Notice $\gcd(P, Q) = 1$. W.l.o.g. we can assume $PS - QR = (-1)^{n-1}$. Otherwise we can "adjust" the length of the continued fraction. Indeed if $a_n \geq 2$, then

$$[a_0; a_1, \ldots, a_n] = [a_0; a_1, \ldots, a_n - 1, 1];$$

and if $a_n = 1$

$$[a_0; a_1, \dots, a_n] = [a_0; a_1, \dots, a_{n-2}, a_{n-1} + 1].$$

By property (iv) we get

$$p_n S - q_n R = PS - QR = (-1)^{n-1} = p_n q_{n-1} - p_{n-1} q_n.$$

Hence

$$p_n(S - q_{n-1}) = q_n(R - p_{n-1}).$$

Assume $S - q_{n-1} \neq 0$, then q_n must divide $S - q_{n-1}$ since p_n and q_n are coprime. So

$$q_n \leq S - q_{n-1}.$$

On the other hand $q_n = Q > S$, so

$$q_n \leq S - q_{n-1} < q_n - \underbrace{q_{n-1}}_{>0} . \lightning$$

Thus $S = q_{n-1}$ and $R = p_{n-1}$. Now since

$$x = \frac{p_n \omega + p_{n-1}}{q_n \omega + q_{n-1}}$$

we conclude $x = [a_0; a_1, \dots, a_n, \omega]$. □

Theorem 1 (Serret)**.** *Let $x, y \in \mathbb{R} \smallsetminus \mathbb{Q}$. Then x is equivalent to y if and only if the sequences of partial quotients of x and y are equal after some point, i.e.*

$$\begin{aligned} x &= [a_0; a_1, \dots, a_m, c_0, c_1, c_2, \dots], \\ y &= [b_0; b_1, \dots, b_n, c_0, c_1, c_2, \dots]. \end{aligned}$$

Proof. "$\Leftarrow$" Let $\omega = [c_0, c_1, c_2, \dots]$. Then

$$x = [a_0; a_1, \dots, a_m, \omega] = \frac{\omega p_m + p_{m+1}}{\omega q_m + q_{m+1}} = \begin{pmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{pmatrix} \omega =: A\omega,$$

and $\det(A) = p_m q_{m-1} - q_m p_{m-1} = \pm 1$. So x is equivalent to ω. Similarly y is equivalent to ω, thus by transitivity x is equivalent to y.
"$\Rightarrow$" Suppose $y \sim x$, i.e. $y = Ax$ with $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $ad - bc = \pm 1$. So $y = \frac{ax+b}{cx+d}$. W.l.o.g. we assume $cx + d > 0$ (otherwise substitute every coefficient with its negative). For some $k \geq 2$ write

$$x = [a_0; a_1, \dots, a_{k-1}, x_k] = \frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + q_{k-2}} = \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} x_k.$$

Then $y = Ax = ABx_k =: Cx_k$ with $\det(C) = \det(A)\det(B) = \pm 1$. We have

$$C = AB = \begin{pmatrix} ap_{k-1} + bq_{k-1} & ap_{k-2} + bq_{k-2} \\ cp_{k-1} + dq_{k-1} & cp_{k-2} + dq_{k-2} \end{pmatrix} =: \begin{pmatrix} P & R \\ Q & S \end{pmatrix}.$$

Our goal is to use lemma 3.

Claim. $Q > S$

Proof. By lemma 2 we have

$$\begin{aligned} p_{k-1} &= xq_{k-1} + \frac{\delta}{q_k}, \\ p_{k-2} &= xq_{k-2} + \frac{\delta'}{q_{k-1}}, \end{aligned}$$

for some $|\delta|, |\delta'| < 1$. Then

$$Q = cp_{k-1} + dq_{k-1} = (cx+d)q_{k-1} + \frac{c\delta}{q_k},$$
$$S = cp_{k-2} + dq_{k-2} = (cx+d)q_{k-2} + \frac{c\delta'}{q_{k-1}},$$

where $q_{k-1} > q_{k-2}$ and the sequence of the q_k's is increasing. Hence we can choose k big enough such that the second term in the above equations become irrelevant, thus showing that $Q > S$. □

We can now apply lemma 3 finding

$$y = [b_0; b_1, \ldots, b_n, x_k].$$

□

Remark. In the last part of the proof we found some k "big enough" to show the theorem but we don't say anything about how big this k actually is. So what we want to do now is to improve Serret's Theorem finding a bound for k.

Bound to Serret's Theorem

Recall our action

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} x = \frac{ax+b}{cx+d}.$$

Definition 2. We define Γ to be the set of all transformation $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $\det(\gamma) = \pm 1$ that induce the action above. Note that for every $\gamma \in \Gamma$ we have $\gamma = -\gamma$.

Let $\varepsilon = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with $\varepsilon x = \frac{1}{x}$, the inverse transformation; and $T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ with $Tx = x+1$, the translation transformation. Then the step of the continued fraction algorithm becomes

$$x_{i+1} = \varepsilon T^{-a_i}(x_i) = \begin{pmatrix} 0 & 1 \\ 1 & -a_i \end{pmatrix} = \frac{1}{x_i - a_i}.$$

Recall that $x_0 = x$, so recursively we see that each x_i is the image of x by a matrix $\gamma_{i,x} \in \Gamma$ given by

$$\gamma_0 = Id, \qquad \gamma_{i,x} = \begin{pmatrix} 0 & 1 \\ 1 & -a_{i-1} \end{pmatrix} \gamma_{i-1,x};$$

or explicitly

$$\gamma_{i,x} = \begin{pmatrix} 0 & 1 \\ 1 & -a_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -a_0 \end{pmatrix}.$$

We will now write $\gamma_i = \gamma_{i,x}$ when the argument x is obvious and we introduce the following convention:

$$p_{-2} = 0, \quad p_{-1} = 1;$$
$$q_{-2} = 1, \quad q_{-1} = 0;$$

Claim.

$$\gamma_i = \begin{pmatrix} q_{i-2} & -p_{i-2} \\ -q_{i-1} & p_{i-1} \end{pmatrix}.$$

Proof. We use induction on i. For $i = 0$ we trivially see that $\gamma_0 = \mathrm{Id}$. Now assume the claim holds for $i \geq 1$, then

$$\gamma_{i+1} = \begin{pmatrix} 0 & 1 \\ 1 & -a_i \end{pmatrix} \gamma_i = \begin{pmatrix} 0 & 1 \\ 1 & -a_i \end{pmatrix} \begin{pmatrix} q_{i-2} & -p_{i-2} \\ -q_{i-1} & p_{i-1} \end{pmatrix} = \begin{pmatrix} -q_{i-1} & p_{i-1} \\ q_{i-2} + a_i q_{i-1} & -p_{i-2} - a_i p_{i-1} \end{pmatrix}$$
$$= \begin{pmatrix} -q_{i-1} & p_{i-1} \\ q_i & -p_i \end{pmatrix} = \begin{pmatrix} q_{i-1} & -p_{i-1} \\ -q_i & p_i \end{pmatrix}.$$

□

Definition 3. $\Gamma(x) = \{ \gamma_1, \gamma_2, \gamma_3, \dots \}$.

Note that $\Gamma(x)$ is an unordered set.

Lemma 4. *Every rational number satisfying*

$$\left| \frac{p}{q} - x \right| < \frac{1}{2q^2}$$

is a convergent of x.

We will not prove this lemma here.

Lemma 5. *Let $r/t, s/u \in \mathbb{Q}$, with $u, t > 0$, $\frac{r}{t} \leq x \leq \frac{s}{u}$ and $ru - st = \pm 1$. Then r/t or s/u is a convergent of x.*

Proof. Suppose r/t and s/u are not convergent of x. Then using the reverse triangle inequality and lemma 4 we have

$$\frac{1}{tu} = \frac{|ru - st|}{tu} = \left| \frac{r}{t} - \frac{s}{u} \right| \geq \left| \frac{r}{t} - x \right| + \left| \frac{s}{u} - x \right| \geq \frac{1}{2t^2} + \frac{1}{2u^2}.$$

But this can hold only if $t = u = 1$. So $r \leq x \leq s$ and $r - s = \pm 1$, that is $s = r + 1$. Now consider the convergent $\frac{p_0}{q_0} = \lfloor x \rfloor$. Since $x \in [r, r+1]$ we must have either $\lfloor x \rfloor = r$ or $\lfloor x \rfloor = r + 1$. But this would imply that either $r = r/t$ or $r + 1 = s = s/u$ is a convergent of x. ↯ □

Proposition 2. $\forall x \in \mathbb{R} : \ \Gamma(x) = W \smallsetminus (W_1 \cup W_2)$, *where*

$$\begin{aligned} W &= \{ \gamma \in \Gamma \mid -1 \leq \gamma(\infty) \leq 0, \, \gamma(x) > 1 \}, \\ W_1 &= \{ \gamma \in W \mid \gamma(\infty) = 0, \, \det(\gamma) = 1 \}, \\ W_2 &= \{ \gamma \in W \mid \gamma(\infty) = -1, \, \det(\gamma) = -1 \}. \end{aligned}$$

Remark. This proposition will be very useful for the next theorem but will not prove it here. Notice that if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $\gamma(\infty) = \frac{a}{c}$. So in other words $\gamma(\infty)$ is just a property of the matrix γ.

Theorem 2. *Let $\gamma \in \Gamma$ and $r = \#$partial quotients of $\gamma^{-1}(\infty)$. Then*

$$\forall x \in \mathbb{R} \ \exists s < r + 3 \ \exists t > 1 : \ x_s = y_t,$$

where $y = \gamma(x)$.

Remark. The bound on the index t is obtained in the same way considering γ^{-1} instead of γ.

Proof. Let $y = \gamma(x)$. We have $\forall s, t$

$$x_s = \gamma_{s,x}(x), \qquad y_t = \gamma_{t,y}(y) = \gamma_{t,y}\gamma(x).$$

We want to show that $\exists s \leq r + 3$ such that $\gamma_{s,x} = \gamma_{t,y}\gamma$ for some $t \geq 1$. Instead we will show that if $\gamma_{i,x} \neq \gamma_{t,y}\gamma$, then $i \leq 2$. In fact this is equivalent to say that if $i \geq r + 3$, then $\gamma_{i,x} = \gamma_{t,y}\gamma$, which means that at least for $i \leq r + 3$ we have $\gamma_{i,x} = \gamma_{t,y}\gamma$. So suppose

$\gamma_{i,x} \neq \gamma_{t,y}\gamma$. Then $\gamma_{i,x}\gamma^{-1}(y) \notin \Gamma(y) = W \setminus (W_1 \cup W_2)$. Recalling the definitions of W, W_1 and W_2 we see that

$$\gamma_{i,x}\gamma^{-1}(\infty) \geq 0 \qquad \text{or} \qquad \gamma_{i,x}\gamma^{-1}(\infty) \leq -1.$$

Suppose first that $\gamma^{-1}(\infty) \neq \infty$. Then $\gamma^{-1}(\infty) = \frac{p}{q}$. If $\gamma_{i,x}\gamma^{-1}(\infty) \geq 0$, then

$$0 \leq \gamma_{i,x}(p/q) = \begin{pmatrix} q_{i-2} & -p_{i-2} \\ -q_{i-1} & p_{i.1} \end{pmatrix} \frac{p}{q} = \frac{pq_{i-2} - qp_{i-2}}{-pq_{i-1} + qp_{i-1}}.$$

Solving the inequality gives

$$\frac{p}{q} \in \left| \frac{p_{i-2}}{q_{i-2}}, \frac{p_{i-1}}{q_{i-1}} \right|.$$

Remark. We introduce here the notation

$$|a, b| = \begin{cases} [a, b], & if\ a \leq b \\ [b, a], & if\ b < a \end{cases}.$$

By lemma 5 we have then that $\frac{p_{i-1}}{q_{i-1}}$ or $\frac{p_{i-2}}{q_{i-2}}$ is a convergent of $\frac{p}{q}$. Now in the case $\gamma_{i,x}\gamma^{-1}(\infty) \leq -1$ we get

$$\frac{pq_{i-2} - qp_{i-2}}{-pq_{i-1} + qp_{i-1}} \leq -1.$$

Solving this equality gives

$$\frac{p}{q} \in \left| \frac{p_{i-1} - p_{i-2}}{q_{i-1} - q_{i-2}}, \frac{p_{i-1}}{q_{i-1}} \right|.$$

One can show that

$$\frac{p_{i-1} - p_{i-2}}{q_{i-1} - q_{i-2}} \in \left| \frac{p_{i-3}}{q_{i-3}}, \frac{p_{i-1}}{q_{i-1}} \right|,$$

hence obtaining

$$\frac{p}{q} \in \left| \frac{p_{i-3}}{q_{i-3}}, \frac{p_{i-1}}{q_{i-1}} \right|.$$

Notice that

$$\left| \frac{p_{i-3}}{q_{i-3}}, \frac{p_{i-1}}{q_{i-1}} \right| = \left| \frac{\frac{p_{i-3}}{a_{i-1}}}{\frac{q_{i-3}}{a_{i-1}}}, \frac{p_{i-1}}{q_{i-1}} \right|$$

and

$$\frac{p_{i-3}}{a_{i-1}} qi - 1 - \frac{p_{i-3}}{a_{i-1}} p_{i-1} = \frac{p_{i-3}}{a_{i-1}}(a_{i-1}q_{i-2} + q_{i-3}) - \frac{q_{i-3}}{a_{i-1}}(a_{i-1}p_{i-2} + p_i - 3)$$
$$= p_{i-3}q_{i-2} - q_{i-3}p_{i-2} = \pm 1.$$

Hence we can use lemma 5 obtaining that $\frac{p_{i-3}}{q_{i-3}}$ or $\frac{p_{i-1}}{q_{i-1}}$ is a convergent of $\frac{p}{q}$. Recall that p/q has r partial quotients whose last index is $r - 1$. Hence in the worst case we get

$$i - 3 \leq r - 1,$$

i.e. $i \leq r + 2$.
Now consider the case when $\gamma^{-1}(\infty) = \infty$. Then $\forall i \geq 1$

$$\gamma_{i,x}\gamma^{-1}(y) = \gamma_{i,x}(x) = x_i > 0$$

and since $\gamma_{i,x} \in W$:

$$-1 \leq \gamma_{i,x}\gamma^{-1}(\infty) = \gamma_{i,x}(\infty) \leq 0.$$

By our assumption we are only left with $\gamma_{i,x}(\infty) = 0$ or $\gamma_{i,x}(\infty) = -1$. Let $\gamma_{i,x} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. In the first case we must have $a = 0$ and $bc = 1$ since $\det(\gamma_{i,x}) = -1$. W.l.o.g. $b = c = 1$ (with $b = c = -1$ we will end up with the same result). To find d we use the inequality

$\gamma_{i,x}(x) > 1$. So

$$\frac{1}{x+d} > 1 \quad \Rightarrow \quad 0 \leq x + d \leq 1 \quad \Rightarrow \quad -x \leq d \leq 1 - x,$$

which implies $d = \lceil -x \rceil = -\lfloor x \rfloor = -a_0$. hence

$$\gamma_{i,x} = \begin{pmatrix} 0 & 1 \\ 1 & -a_0 \end{pmatrix} = \gamma_{1,x} \quad \Rightarrow \quad i = 1.$$

In the second case with a similar procedure we find that $a_1 = 1$ and

$$\gamma_{i,x} = \begin{pmatrix} 1 & -a_0 \\ -1 & 1 + a_0 \end{pmatrix} = \gamma_{2,x} \quad \Rightarrow \quad i = 2.$$

So in general $i \leq 2 \leq r + 2$ which ends our proof. □

Bibliography

[1] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers.*

[2] P. Bengoechea, *On a theorem of Serret on continued fractions*, Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas, 110 (2) (2016) 379-384.

[3] V. Beresnevich, *Number Theory*, Lecture notes, University of York, 2013.