2-2011

A short proof and generalization of Lagrange's theorem on continued fractions

Sam Northshield
SUNY Plattsburgh

Recommended Citation
Northshield, S. (2011). A short proof and generalization of Lagrange's theorem on continued fractions. *American Mathematical Monthly, 118* (2), 171-175.

A short proof and generalization of Lagrange's theorem on continued fractions

Sam Northshield

Abstract

We present a short new proof that the continued fraction of a quadratic irrational eventually repeats. The proof easily generalizes; we construct a large class of functions which, when iterated, must eventually repeat when starting with a quadratic irrational.

1 Introduction.

A *quadratic irrational* is an irrational root of a quadratic polynomial with integer coefficients. Lagrange's theorem on continued fractions – that any positive quadratic irrational has an eventually repeating continued fraction – has many proofs. Perhaps the most common proof is one by Charves which can be found in a book by Hardy and Wright [1, Theorem 177]. Many other proofs exist of course; a particularly short proof appears in the book by Hensley [2, p. 9] and a more general result appears in a recent paper by Panti [3]. We present a short new proof which leads to a new generalization.

2 Lagrange's Theorem.

Let $\langle a_0, a_1, a_2, ...\rangle := a_0 + 1/(a_1 + 1/(a_2 + 1/...))$ where each a_i is an integer and, for some N, $a_i = 0$ for $i < N$ and $a_i > 0$ for $i \geq N$. This, of course, is not quite the standard notation for continued fractions. In particular, there are infinitely many representations for a given number. However, if $\langle 0, 0, ...0, a_N, a_{N+1}...\rangle = \langle 0, 0, ...0, b_M, b_{M+1}...\rangle$ where $a_N > 0$ and $b_M > 0$, then $M - N$ is even and $b_{M+k} = a_{N+k}$ for all k. Define a function on positive real numbers by

$$f(x) := \begin{cases} x - 1 & \text{if } x \geq 1, \\ x/(1-x) & \text{if } x < 1. \end{cases}$$

Note that $\langle 0, 0, ...0, a_N, a_{N+1}...\rangle > 1$ if and only if N, the number of zeros, is even and, in general,

$$f(\langle 0, 0, ...0, a_N, a_{N+1}...\rangle) = \langle 0, 0, ..., 0, a_N - 1, a_{N+1}, ...\rangle.$$

Iteration of f then chips away at the leftmost nonzero integer in $\langle a_0, a_1, a_2, ...\rangle$, reducing it by one in each step.

Suppose x is a positive quadratic irrational. Then x is irrational and there exist integers a, b, c such that $ax^2 + bx + c = 0$. We use the notation $x \in [a, b, c]$ for this. It is then easy to verify that

$$a(x-1)^2 + (2a+b)(x-1) + (a+b+c) = ax^2 + bx + c = 0$$

and

$$(a+b+c)x^2 + (b+2c)x(1-x) + c(1-x)^2 = ax^2 + bx + c = 0,$$

and thus

$$f(x) \in [a, 2a+b, a+b+c] \text{ or } f(x) \in [a+b+c, b+2c, c].$$

Let $x_1 := x$ and, for $n \geq 1$, $x_{n+1} := f(x_n)$. Then (x_n) is a sequence of quadratic irrationals and so determines an infinite sequence of triples: $x_n \in [s_n, t_n, u_n]$ where we may assume, without loss of generality, that $s_n > 0$ (since $y \in [s, t, u]$ if and only if $y \in [-s, -t, -u]$). Since

$$(2a+b)^2 - 4a(a+b+c) = b^2 - 4ac = (b+2c)^2 - 4(a+b+c)c,$$

we see that $t_n^2 - 4s_n u_n$ is independent of n.

If only finitely many of the triples $[s_n, t_n, u_n]$ have $u_n < 0$, then from some point on, $s_n, u_n > 0$ and, consequently, $t_n < 0$ (because $x_n > 0$). This is impossible since $(s_n - t_n + u_n)$ would then be strictly decreasing and nonnegative. Therefore, $s_n u_n < 0$ infinitely often and, since $t_n^2 - 4s_n u_n$ is constant, there must be a triple which appears three times in the sequence $([s_n, t_n, u_n])$. Hence $x_n = x_m$ for some m and n satisfying $m > n$. If $x = \langle a_0, a_1, a_2, \dots\rangle$ then x_n is of the form $\langle 0, \dots, 0, b, a_i, a_{i+1}, \dots\rangle$ and x_m is of the form $\langle 0, \dots, 0, c, a_j, a_{j+1}, \dots\rangle$ where $b > 0$, $c > 0$, and, necessarily, $j > i$. Since these are equal, the difference $j - i$ is positive and even and so $b = c$ and, for all k, $a_{j+k} = a_{i+k}$. That is, the sequence a_k is eventually periodic and we have Lagrange's theorem:

Theorem 1. *If x is a positive quadratic irrational then its continued fraction is eventually periodic.*

3 Generalizations.

There are only three facts about f necessary so that if x is a quadratic irrational then x_n eventually repeats. They are that f takes positive numbers to positive numbers, that for any of the corresponding triples $[s_n, t_n, u_n]$, $t_n^2 - 4s_n u_n$ is independent of n, and that whenever $s_n u_n > 0$ and $s_{n+1}u_{n+1} > 0$, $|s_{n+1}| + |t_{n+1}| + |u_{n+1}| \leq |s_n| + |t_n| + |u_n|$.

We say that a function is *regular* if it is a fractional linear transformation $(ax+b)/(cx+d)$ where a, b, c, d are integers satisfying $|ad-bc| = 1$, $(a-b)(d-c) > 0$, and there exists $t > 0$ such that $(at+b)/(ct+d) > 0$. (This last condition, although made redundant by the hypotheses of the next two theorems, will be useful later.) We then have:

Theorem 2. *Let $f : (0, \infty) \to (0, \infty)$ be any function which is piecewise regular. If x is a positive quadratic irrational then the iterates of f, starting at x, eventually repeat.*

Proof. It is not hard to verify that for any s, t, u, a, b, c, d, if $S = d^2 s - cdt + c^2 u$, $T = -2bds + (ad + bc)t - 2acu$, and $U = b^2 s - abt + a^2 u$, then

$$t^2 - 4su = (ad - bc)^2 (T^2 - 4SU)$$

and

$$S(ax + b)^2 + T(ax + b)(cx + d) + U(cx + d)^2 = (ad - bc)^2 (sx^2 + tx + u).$$

Suppose x is a quadratic irrational, so that there exist integers s, t, u such that $sx^2 + tx + u = 0$. Then for S, T, and U as defined above,

$$S\left(\frac{ax + b}{cx + d}\right)^2 + T\left(\frac{ax + b}{cx + d}\right) + U = 0. \tag{1}$$

Let $x_1 := x$ and, for $n \geq 1$, $x_{n+1} = f(x_n)$. By the hypothesis of the theorem, if $x_n \in [s_n, t_n, u_n]$, then $x_{n+1} \in [s_{n+1}, t_{n+1}, u_{n+1}]$ where $t_{n+1}^2 - 4s_{n+1}u_{n+1} = t_n^2 - 4s_n u_n$. Since there are only finitely many triples $[a, b, c]$ where $b^2 - 4ac$ is bounded and $ac < 0$, either there exist i, j, k such that $i < j < k$ and $[s_i, t_i, u_i] = [s_j, t_j, u_j] = [s_k, t_k, u_k]$ (hence, at least two of x_i, x_j, x_k agree) or $s_n u_n > 0$ for all sufficiently large n.

Suppose $x \in [s, t, u]$ and $f(x) = (ax + b)/(cx + d)$. Let $S = d^2 s - cdt + c^2 u$, $T = -2bds + (ad + bc)t - 2acu$, and $U = b^2 s - abt + a^2 u$ so that $f(x) \in [S, T, U]$. It is not hard to verify that, since $|ad - bc| = 1$,

$$s - t + u = (a - b)^2 S - (a - b)(d - c)T + (c - d)^2 U. \tag{2}$$

Now suppose that $SU, su > 0$. Then since x and $f(x)$ are positive, t must have the opposite sign from s and u, and T must have the opposite sign from S and U. Also, since $(a - b)(d - c) \geq 1$, we must have $(a - b)^2 \geq 1$ and $(c - d)^2 \geq 1$. Therefore,

$$\begin{aligned} |s| + |t| + |u| &= |s - t + u| = |(a - b)^2 S - (a - b)(d - c)T + (c - d)^2 U| \\ &= (a - b)^2 |S| + (a - b)(d - c)|T| + (c - d)^2 |U| \geq |S| + |T| + |U|. \end{aligned} \tag{3}$$

Since there are only finitely many triples $[a, b, c]$ where $|a| + |b| + |c|$ is bounded, there must exist i, j, k such that $i < j < k$ and $[s_i, t_i, u_i] = [s_j, t_j, u_j] = [s_k, t_k, u_k]$. Hence, at least two of x_i, x_j, x_k agree and the result follows. □

Example 1. *If $f(x) = \{1/x\}$ (where $\{x\}$ denotes the fractional part of x; this f is usually called the Gauss map) and x is a positive quadratic irrational then the iterates of f eventually repeat.*

Example 2. *If $f(x) = \{x\}/(1 - \{x\})$ and x is a positive quadratic irrational then the iterates of f eventually repeat.*

We may extend further; the proof of the following theorem is essentially contained in that of Theorem 2 and is left to the reader.

Theorem 3. *Let $f_1, f_2, ...$ be any sequence of regular functions. Given x, define a sequence recursively by $x_1 := x$ and, for $n \geq 1$, $x_{n+1} = f_n(x_n)$. If x is a positive quadratic irrational and $x_n > 0$ for all n, then there exist distinct j, k such that $x_j = x_k$.*

Example 3. *For any n, choose one of the two functions $\{1/x\}$ or $\{x\}/(1 - \{x\})$ at random and so form a random sequence f_n. For any positive quadratic irrational x, the sequence (x_n) defined by $x_1 := x$ and $x_{n+1} := f_n(x_n)$ satisfies $x_j = x_k$ for some pair of distinct integers j, k.*

4 Understanding Regular Functions.

Recall $PGL_2(\mathbb{Z})$ can be taken to be the group of linear fractional transformations $(ax+b)/(cx+d)$ where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$. A function $g(x)$ is then regular if it is an element of $PGL_2(\mathbb{Z})$ such that $g(-1) < 0$ and there exists $t > 0$ such that $g(t) > 0$. It turns out, by a careful consideration of several cases, that if g is regular then $g(s) < 0$ for *all* $s < 0$. Since g takes on all values except possibly $\lim_{x \to -\infty} g(x)$, which is nonpositive, the range of g must contain all positive numbers. It follows that the set of regular functions is closed under composition.

We may then classify all regular functions. First, g is regular with determinant -1 if and only if $1/g$ is regular with determinant 1; it is then enough to classify regular functions in $SL_2(\mathbb{Z})$. Given a, b positive and relatively prime, let $a' := a^{-1} \pmod{b}$ and $b' := b^{-1} \pmod{a}$ (e.g., a' is the unique number between 1 and b satisfying $aa' \equiv 1 \pmod{b}$) and define

$$g_{a/b}(x) := \frac{a'x + b' - a}{(a' - b)x + b'}.$$

It is not hard to show that $aa' + bb' = ab + 1$ and that $g_{a/b}$ is regular and in $SL_2(\mathbb{Z})$. Conversely, every regular function g in $SL_2(\mathbb{Z})$ is of that form! To see this, note that $g(x) = 1$ has a positive solution since $g(s) < 0$ for all $s < 0$. Hence $g^{-1}(1) = a/b$ for some positive relatively prime a and b. Suppose $g(x) = (sx+t)/(ux+v)$. Since $g(a/b) = 1$, there exists c such that $sa + tb = c = ua + vb$ and thus $u = s - bk$ and $v = t + ak$ for some k. By multiplying all of s, t, u, and v by -1 if necessary, we may assume without loss of generality that $c > 0$. Since $g \in SL_2(\mathbb{Z})$, $(as + bt)k = sv - tu = 1$ and thus $as + bt = 1$, $k = 1$, $u = s - b$, and $v = t + a$. Since $g(-1) < 0$, $(s - t)(t + a - s + b) \geq 1$ and so $0 < s - t < a + b$. Since there is a *unique* pair s, t such that $as + bt = 1$ and $0 < s - t < a + b$, it follows that $s = a'$, $t = b' - a$, and the function g must coincide with $g_{a/b}$.

We can go further. Suppose a, b are positive integers with $a > b$. By the easily verified facts that $(a - b)^{-1} \pmod{b} = a^{-1} \pmod{b}$ and b^{-1} (mod $a -$

$b) = a^{-1} \pmod b + b^{-1} \pmod a - b$, it follows that $g_{(a-b)/b}(x-1) = g_{a/b}(x)$. Equivalently, for $r > 1$,

$$g_{r-1}(x-1) = g_r(x).$$

Since for positive rational r, $g_{1/r}(1/x) = 1/g_r(x)$, it follows that for $r \in (0,1)$,

$$g_{r/(1-r)}(x/(1-x)) = g_r(x).$$

Letting f be defined as in Section 2 and given a positive rational r, there exists n such that the n-fold iterate $f \circ f \circ \cdots \circ f(r) = 1$. Hence there exists a sequence of functions $h_1, h_2, \ldots, h_n$ such that each $h_i(x)$ is either $x-1$ or $x/(1-x)$ and $H := h_n \circ \cdots \circ h_1$ satisfies $H(r) = 1$ and therefore

$$g_r(x) = g_{H(r)}(H(x)) = g_1(H(x)) = H(x).$$

Hence every g_r is a composition of the functions $x-1$ and $x/(1-x)$ and thus every regular function is a composition of the functions $x-1$ and $1/x$. Since $x-1$ and $1/x$ are regular and the set of regular functions is closed under composition, we see that the set of regular functions is the monoid generated by $x-1$ and $1/x$.

This leads to a characterization of quadratic irrationals. Note that if $x = \langle a_0, a_1, a_2, ... \rangle$, then $1/x = \langle 0, a_0, a_1, a_2, ... \rangle$. Let

$$S_t := \{g(t) : g \text{ is regular and } g(t) > 0\}.$$

Since every g is a composition of $x-1$ and $1/x$, it follows that if $t = \langle a_0, a_1, a_2, ... \rangle$ then any element in S_t is of the form $\langle 0, ..., 0, b, a_n, a_{n+1}, ... \rangle$, where $b \leq a_{n-1}$, and so S_t is finite if and only if the sequence (a_n) eventually repeats.

Theorem 4. *A positive irrational number t is a quadratic irrational if and only if S_t is finite.*

The regular functions in $SL_2(\mathbb{Z})$ can be parametrized by the positive rational numbers. This leads to an interesting associative (but not commutative) binary operation $*$ with identity 1 defined by $g_r \circ g_s = g_{r*s}$. Since $r * s = (g_r \circ g_s)^{-1}(1)$, one may write out $a/b * c/d$ explicitly:

$$\frac{a}{b} * \frac{c}{d} = \frac{bc + (a-b)d'}{ad + (b-a)c'}, \tag{2}$$

where $c' = c^{-1} \pmod d$ and $d' = d^{-1} \pmod c$.

References

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, New York, 1979.

[2] D. Hensley, *Continued Fractions*, World Scientific, Hackensack, NJ, 2006.

[3] G. Panti, A general Lagrange theorem, this MONTHLY **116** (2009) 70-74.

Department of Mathematics, SUNY, Plattsburgh, NY 12901
northssw@plattsburgh.edu