A PROOF OF THE INFINITUDE OF PRIMES VIA CONTINUED FRACTIONS

Joseph Vandehey
Department of Mathematics, University of Texas at Tyler, Tyler, Texas
jvandehey@uttyler.edu

Received: 5/14/19, Accepted: 2/18/20, Published: 3/6/20

Abstract
We provide a proof of the infinitude of primes based on the idea that successive denominators of continued fraction convergents are relatively prime.

1. The Result

Euclid's theorem on the infinitude of primes is one of the most reproved theorems in mathematics. Romeo Meštrović [4] catalogued 183 different proofs as of 2017. The first chapter of Paul Pollack's book [6] contains a thorough exposition of several notable proofs.

In this short note, we will provide a new proof of the infinitude of primes based on the theory of continued fractions.

Two other proofs of the infinitude of primes have involved continued fractions. Harris [3] gave an infinite sequence $A_0, A_1, A_2, \dots$ of pairwise coprime positive integers that arise naturally as the denominators of the convergents of a particular continued fraction. Barnes [2] used the connection between periodic continued fractions, quadratic irrationals, and solutions to Pell's equation to give another proof.

We make use of the following basic facts about continued fractions, which can be found in many elementary texts on number theory (see, for example, [5]).

1. Every rational number in $(0,1)$ can be written as a finite continued fraction expansion:
$$[a_1, a_2, \dots, a_k] := \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots + \cfrac{1}{a_k}}},$$
with $a_1, \dots, a_k \in \mathbb{N}$. In particular, there are always two such expansions, one with k even and one with k odd. This is due to the fact that if $a_k > 1$, then $[a_1, \dots, a_{k-1}, a_k] = [a_1, \dots, a_{k-1}, a_k - 1, 1]$.

2. Consider a finite continued fraction expansion $x = [a_1, a_2, \ldots, a_k]$. Then for any j, with $1 \leq j \leq k$, we define the jth convergent to x by
$$\frac{A_j}{B_j} = [a_1, a_2, \ldots, a_j]$$
with A_j, B_j relatively prime to one another and positive. Successive convergents obey the following relation: $A_{j-1}B_j - A_jB_{j-1} = (-1)^j$ for $2 \leq j \leq k$.

We are now ready to begin our proof.

Proof of the infinitude of primes. Suppose, by way of contradiction, that there are only n odd primes, $p_1, p_2, \ldots, p_n$. (We will assume that 7 is a known prime.) Let $P = p_1p_2 \ldots p_n$ be the product of these primes. Consider the fraction $2/P$, which we note is in lowest terms. This fraction can be written as a finite continued fraction expansion $[a_1, a_2, \ldots, a_k]$ with k even.

Consider the convergents $A_{k-1}/B_{k-1} = [a_1, \ldots, a_{k-1}]$ and $A_k/B_k = [a_1, \ldots, a_k] = 2/P$. Since $2/P$ is in lowest terms, we have that $A_k = 2$ and $B_k = P$.

Recall that $A_{k-1}B_k - A_kB_{k-1} = (-1)^k$, i.e., that $A_{k-1}P - 2B_{k-1} = 1$. From this relation we can read off three facts very quickly:

1. The GCD of P and B_{k-1} must divide 1 and so must be 1;
2. Since $7 \leq P$ and $1 \leq A_{k-1}$, we have that $B_{k-1} \geq 3$; and,
3. Since 7 divides P and since $-(2^\ell) \equiv 1 \pmod 7$ has no solutions, we cannot have that B_{k-1} is a power of 2.

As a consequence of these three facts, we have that B_{k-1} must be divisible by some prime that is at least 3, but must be relatively prime to P. This produces a contradiction and so there are infinitely many primes. □

We note a few things on this proof.

First, this proof contains a different proof in disguise. We can calculate B_{k-1} exactly. In particular, we have
$$\frac{2}{P} = \frac{1}{\left\lfloor \frac{P}{2} \right\rfloor + \frac{1}{2}}.$$

Thus, the even-length continued fraction expansion of $2/P$ is just $[\lfloor \frac{P}{2} \rfloor, 2]$, so that $A_{k-1} = 1$ and $B_{k-1} = \lfloor P/2 \rfloor$. By the nature of the floor function, we can easily show that $2B_{k-1}+1 = P$. Clearly B_{k-1} and P are relatively prime as a consequence, and by the same reasoning as above, B_{k-1} cannot be a power of 2. However, the proof above could be applied to other fractions. Namely, if j is a positive integer such that $2^j \le P$, then we could apply the proof to the fraction $2^j/P$ with no changes. In this case we could show that one obtains $2^j B_{k-1} + 1 = xP$, where $x \in [1, 2^j - 1]$ is the unique integer such that $xP \equiv 1 \pmod{2^j}$.

Second, in an earlier draft of this proof, we used $\frac{1}{2} + \frac{1}{P}$ instead of $2/P$, until we realized that in order to check that this was in lowest terms, we would already have to prove that $P + 2$ and $2P$ were relatively prime, which would essentially reduce to Stieltjes's proof of the infinitude of primes.

Third, we could alternatively look at a number like

$$x = \frac{1}{2P} + \frac{1}{3(2P)^2}.$$

Legendre's theorem states that if there exists a fraction a/b in lowest terms such that $|x - a/b| < 1/2b^2$, then a/b must be a convergent to x [1]. Thus $1/2P$ must be a convergent to x. Moreover, it cannot be the last convergent, since it does not equal x. So one could show that the denominator of the next convergent must be relatively prime to $2P$.

References

[1] D. Barbolosi and H. Jager, On a theorem of Legendre in the theory of continued fractions, *J. Théor. Nombres Bordeaux* (1) **6** (1994), 81–94.

[2] C. W. Barnes, The infinitude of primes; a proof using continued fractions, *Enseign. Math.* (2) **22** (1976), 313–316.

[3] V. C. Harris, Another proof of the infinitude of primes, *Amer. Math. Monthly* **63** (1956), 711.

[4] R. Meštrović, Euclid's Theorem of the infinitude of primes: a historical survey of its proofs (300 B.C.–2017), `https://arxiv.org/pdf/1202.3670.pdf`

[5] C. D. Olds, *Continued Fractions*, Random House, New York, 1963.

[6] P. Pollack, *Not Always Buried Deep: A Second Course in Elementary Number Theory*, American Mathematical Society, Providence, RI, 2009.