# Proof that Wagstaff Prime Numbers are Infinite

**Stephen Marshall**

**29 November 2018**

## Abstract

The Wagstaff prime is a prime number $q$ of the form:

$$q = \frac{2^p - 1}{3}$$

where, $p$ is an odd prime. Wagstaff primes are named after the mathematician Samuel S. Wagstaff Jr. Wagstaff primes appear in the New Mersenne conjecture and have applications in cryptography.

The New Mersenne conjecture (Bateman et al. 1989) states that for any odd natural number p, if any two of the following conditions hold, then so does the third:

1. $p = 2k \pm 1$ or $p = 4k \pm 3$ for some natural number k.
2. $2p - 1$ is prime (a Mersenne prime).
3. $(2p + 1) / 3$ is prime (a Wagstaff prime).

There is no simple primality test analogous to the Lucas-Lehmer test for Wagstaff primes, so all recent primality proofs of Wagstaff primes have used elliptic curve primality proving which is very time consuming.

A Wagstaff prime can also be interpreted as a repunit prime of base $-2$, as

$$\frac{(-2)^p - 1}{-2 - 1} = \frac{2^p + 1}{3}$$

if $p$ is odd, as it must be for the above number to be prime.

The first three Wagstaff primes are 3, 11, and 43 because

$$3 = \frac{2^3 + 1}{3},$$
$$11 = \frac{2^5 + 1}{3},$$
$$43 = \frac{2^7 + 1}{3}.$$

The first few Wagstaff primes are:

3, 11, 43, 683, 2731, 43691, 174763, 2796203, 715827883, 2932031007403, 768614336404564651, … (sequence A000979 in the OEIS)

As of October 2014, known exponents which produce Wagstaff primes or probable primes are:

3, 5, 7, 11, 13, 17, 19, 23, 31, 43, 61, 79, 101, 127, 167, 191, 199, 313, 347, 701, 1709, 2617, 3539, 5807, 10501, 10691, 11279, 12391, 14479, 42737, 83339, (all known Wagstaff primes)

95369, 117239, 127031, 138937, 141079, 267017, 269987, 374321, 986191, 4031399, …, 13347311, 13372531 (Wagstaff probable primes) (sequence A000978 in the OEIS)

In February 2010, Tony Reix discovered the Wagstaff probable prime:

$$\frac{2^{4031399} + 1}{3}$$

which has 1,213,572 digits and was the 3rd biggest probable prime ever found at this date.

In September 2013, Ryan Propper announced the discovery of two additional Wagstaff probable primes:

$$\frac{2^{13347311} + 1}{3}$$

and,

$$\frac{2^{13372531}+1}{3}$$

Each is a probable prime with slightly more than 4 million decimal digits. It is not currently known whether there are any exponents between 4031399 and 13347311 that produce Wagstaff probable primes.

Note that when *p* is a Wagstaff prime, $\frac{2^p+1}{3}$ need not to be prime, the first counterexample is p = 683, and it is conjectured that if p is a Wagstaff prime and p>43, then $\frac{2^p+1}{3}$ is composite.

## Proof of Infinite Wagstaff Primes

The divergence of the harmonic series was independently proved by Johann Bernoulli in 1689 in a counter-intuitive manner (reference 1). His proof is worthy of deep study, as it shows the counter-intuitive nature of infinity. We will use Bernoulli's proof and apply it toward proving the Wagstaff prime numbers are infinite.

Let the finite set of, *p*, Wagstaff primes be listed in reverse order from the largest to smallest Wagstaff primes as follows:

$$n_1 = q_1 = \frac{2^{p1}-1}{3} = \text{largest Wagstaff prime}$$

$$n_2 = q_2 = \frac{2^{p2}-1}{3} = \text{second largest Wagstaff prime}$$

$$n_3 = q_3 = \frac{2^{p3}-1}{3} = \text{third largest Wagstaff prime}$$

.

.

.

$$n_p = q_p = \frac{2^p - 1}{3} = \text{smallest Wagstaff prime number} = 3$$

This reverse ordering of the finite set of Wagstaff prime numbers is key to our proof. We assume that the following Wagstaff prime reciprocal series have a finite sum, which we call *S*.

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \cdots + \frac{1}{n_p} > \frac{1}{2n_1} + \frac{1}{3n_2} + \frac{1}{4n_3} + \cdots + \frac{1}{kn_p} = S$$

Where, *k* is the denominator factor for the smallest Wagstaff prime number that exists in our finite set.

We now proceed to derive a contradiction in the following manner. First we rewrite each term occurring in *S* thus:

$$\frac{1}{3n_2} = \frac{2}{6n_2} = \frac{1}{6n_2} + \frac{1}{6n_2}\ ,\ \frac{1}{4n_3} = \frac{3}{12n_3} = \frac{1}{12n_3} + \frac{1}{12n_3} + \frac{1}{12n_3}\ , \ldots,$$

Next we write the resulting fractions in an array as shown below:

$$\begin{array}{ccccccccc}
\frac{1}{2n_1} & \frac{1}{6n_2} & \frac{1}{12n_3} & \frac{1}{20n_4} & \frac{1}{30n_5} & \frac{1}{42n_6} & \frac{1}{56n_7} & \cdots \\
& \frac{1}{6n_2} & \frac{1}{12n_3} & \frac{1}{20n_4} & \frac{1}{30n_5} & \frac{1}{42n_6} & \frac{1}{56n_7} & \cdots \\
& & \frac{1}{12n_3} & \frac{1}{20n_4} & \frac{1}{30n_5} & \frac{1}{42n_6} & \frac{1}{56n_7} & \cdots \\
& & & \frac{1}{20n_4} & \frac{1}{30n_5} & \frac{1}{42n_6} & \frac{1}{56n_7} & \cdots \\
& & & & \frac{1}{30n_5} & \frac{1}{42n_6} & \frac{1}{56n_7} & \cdots
\end{array}$$

$$\frac{1}{42n_6}\ \ \frac{1}{56n_7}\ldots$$

$$\frac{1}{56n_7}\ldots$$

Note that the column sums are just the fractions of the Wagstaff primes; thus S is the sum of all the fractions occurring in the array. As Bernoulli did, we now sums the rows using the telescoping technique. Next we assign symbols to the row sums as shown below,

$$A = \frac{1}{2n_1} + \frac{1}{6n_2} + \frac{1}{12n_3} + \frac{1}{20n_4} + \frac{1}{30n_5} + \frac{1}{42n_6} + \frac{1}{56n_7} + \ldots,$$

$$B = \frac{1}{6n_2} + \frac{1}{12n_3} + \frac{1}{20n_4} + \frac{1}{30n_5} + \frac{1}{42n_6} + \frac{1}{56n_7} + \ldots,$$

$$C = \frac{1}{12n_3} + \frac{1}{20n_4} + \frac{1}{30n_5} + \frac{1}{42n_6} + \frac{1}{56n_7} + \ldots,$$

$$D = \frac{1}{20n_4} + \frac{1}{30n_5} + \frac{1}{42n_6} + \frac{1}{56n_7} + \ldots,$$

We now rearrange as follows:

$$A = \left(\frac{1}{n_1} - \frac{1}{2n_1}\right) + \left(\frac{1}{2n_2} - \frac{1}{3n_2}\right) + \left(\frac{1}{3n_3} - \frac{1}{4n_3}\right) + \left(\frac{1}{4n_4} - \frac{1}{5n_4}\right) + \ldots$$

Since, $n_1 > n_2 > n_3 > n_4$

$$A = \frac{1}{n_1} + \left(\frac{1}{2n_2} - \frac{1}{2n_1}\right) + \left(\frac{1}{3n_3} - \frac{1}{3n_2}\right) + \left(\frac{1}{4n_4} - \frac{1}{4n_3}\right) + \left(\frac{1}{5n_5} - \frac{1}{5n_4}\right) + \ldots$$

Since, $\left(\frac{1}{2n_2} - \frac{1}{2n_1}\right) > 0$ , $\left(\frac{1}{3n_3} - \frac{1}{3n_2}\right) > 0$ , $(\frac{1}{4n_4} - \frac{1}{4n_3}) > 0$ , $(\frac{1}{5n_5} - \frac{1}{5n_4}) > 0$

Then, $A > \frac{1}{n_1}$

$$B = (\frac{1}{2n_2} - \frac{1}{3n_2}) + (\frac{1}{3n_3} - \frac{1}{4n_3}) + (\frac{1}{4n_4} - \frac{1}{5n_4}) + (\frac{1}{5n_5} - \frac{1}{6n_5})\ldots$$

Since, $n_1 > n_2 > n_3 > n_4$ , the same rearranging that we did with *A* can be done with *B*.

Then, $B > \frac{1}{2n_2}$

$$C = (\frac{1}{3n_3} - \frac{1}{4n_3}) + (\frac{1}{4n_4} - \frac{1}{5n_4}) + \left(\frac{1}{5n_5} - \frac{1}{6n_5}\right) + (\frac{1}{6n_5} - \frac{1}{7n_5}) \ldots$$

Since, $n_1 > n_2 > n_3 > n_4$ , the same rearranging that we did with *A* can be done with *C*.

Then, $C > \frac{1}{3n_3}$

$$D = (\frac{1}{4n_4} - \frac{1}{5n_4}) + \left(\frac{1}{5n_5} - \frac{1}{6n_5}\right) + \left(\frac{1}{6n_5} - \frac{1}{7n_5}\right) + \left(\frac{1}{7n_6} - \frac{1}{8n_6}\right) \ldots$$

Since, $n_1 > n_2 > n_3 > n_4$ , the same rearranging that we did with *A* can be done with *D*.

Then, $D > \frac{1}{4n_4}$

and so on. Thus the sum *S,* which we had written in the form $A + B + C + D + \dots$ , turns out to be greater than

$$S > \frac{1}{n_1} + \frac{1}{2n_2} + \frac{1}{3n_3} + \frac{1}{4n_4} + \cdots$$

At the start we had defined *S* to be the following finite series,

$$S = \frac{1}{2n_1} + \frac{1}{3n_2} + \frac{1}{4n_3} + \cdots + \frac{1}{kn_{\mathrm{p}}}$$

And we defined that, $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \frac{1}{n_4} + \cdots > S = \frac{1}{2n_1} + \frac{1}{3n_2} + \frac{1}{4n_3} + \cdots$

However, we just proved that $S > \frac{1}{n_1} + \frac{1}{2n_2} + \frac{1}{3n_3} + \frac{1}{4n_4} + \cdots > S = \frac{1}{2n_1} + \frac{1}{3n_2} + \frac{1}{4n_3} + \cdots + \frac{1}{kn_{\mathrm{p}}}$

However, this is a contradiction, since in the finite realm *S* can't be equal to and greater than $\frac{1}{2n_1} + \frac{1}{3n_2} + \frac{1}{4n_3} + \cdots + \frac{1}{kn_{\mathrm{p}}}$ at the same time. Therefore, *S* must be infinite.

Now we can rewrite the *S*, the Wagstaff prime series as,

$$S > \frac{1}{n_1} + \frac{1}{2n_2} + \frac{1}{3n_3} + \frac{1}{4n_4} + \cdots > \frac{1}{2n_1} + \frac{1}{3n_2} + \frac{1}{4n_3} + \cdots + \frac{1}{kn_{\mathrm{p}}} = S$$

This implies that $S > S$

However, no finite number can satisfy such an equation. Therefore, we have a contradiction and must conclude that $S = \infty$**.** Remember our definition of *S* from the above series:

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \cdots + \frac{1}{n_p} > S = \infty$$

$$\text{Therefore, } \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \cdots + \frac{1}{n_p} > \infty$$

Therefore, we have proven that the reciprocal Wagstaff prime series diverges to infinity. Obviously, this cannot possibly happen if there are only finitely many Wagstaff prime reciprocals, therefore the Wagstaff prime reciprocals are infinite in number. Since the Wagstaff prime reciprocals are infinite in number, the Wagstaff prime numbers must be infinite as well.

This proof shows the shows the counter-intuitive nature of infinity, and why it has taken so long to prove the Wagstaff primes are infinite, as it is not obvious that the reciprocal Wagstaff prime series would diverge.

The author expresses many thanks to the work of Johann Bernoulli in 1689, without his work this proof would not have been possible. It was solely through the study of Johann Bernoulli's work that the author was inspired to see this divergent proof. The author would also like to express many thanks to Shailesh Shirali's work in which he documented Johann Bernoulli's work in the most fascinating and interesting way.

References:


1. On the Infinitude of the Prime Numbers, Shailesh A Shirali, Kishi Valley School (Krishnamurti Foundation of India), Kishi Valley, Anclhra Pradesh, India

2. The Irregular Primes to 125000, Samuel S. Wagstaff Jr., April 1978

3. Number Theory, Prime Number, Samuel S. Wagstaff Jr., Prime Pages, Cryptology, Probable Prime, Lambert M. Surhone, 22 Aug 2010

4. Guy, Richard K., Unsolved problems in number theory, (3rd edition). Springer-Verlag (2004).

5. Congruence Properties of Wagstaff Primes, M. S. Srinath1, Garimella Rama Murthy, V. Chandrasekaran

6. From Euclid to Present: A Collection of Proofs regarding the Infinitude of Primes, Lindsey Harrison, December 14, 2013.

7. Fermat and Wagstaff Primes, Chapter 4.

8. The Primes: Infinitude, Density and Substance, Pete L. Clark