Elementary Proof that an Infinite Number of Cullen Primes Exist

Stephen Marshall

21 February 2017

Abstract

This paper presents a complete proof of the Cullen Primes are infinite, even though only 16 of them have been found as of 21 Feb 2017. We use a proof found in Reference 1, that if $p > 1$ and $d > 0$ are integers, that p and $p+d$ are both primes if and only if for integer m:

$$m = (p-1)!\left(\frac{1}{p} + \frac{(-1)^{\wedge}d(d!)}{p+d}\right) + \frac{1}{p} + \frac{1}{p+d}$$

We use this proof for $d = P2 + 1$ to prove the infinitude of Cullen prime numbers. The author would like to give many thanks to the authors of 1001 Problems in Classical Number Theory, Jean-Marie De Koninck and Armel Mercier, 2004, Exercise Number 161 (see Reference 1). The proof provided in Exercise 6 is the key to making this paper on the Cullen Prime Conjecture possible.

Introduction

James Cullen, (19 April 1867 – 7 December 1933) was born at Drogheda, County Louth, Ireland. At first he was educated privately, then he studied pure and applied mathematics at the Trinity College, Dublin for a while, he went to

Mungret College, Limerick, before deciding to become a Jesuit, studying in England in Mansera House, and St. Mary's, and was ordained as a priest on 31 July 1901. In 1905, he taught mathematics at Mount St. Mary's College in Derbyshire and published his finding of what is now known as Cullen numbers in number theory.

In number theory of prime numbers, a Cullen number is a natural number of the form

$$C_n = n2^n + 1$$

Cullen numbers were first studied by James Cullen in 1905. The only 16 known Cullen primes are those for ***n*** equal:

1, 141, 4713, 5795, 6611, 18496, 32292, 32469, 59656, 90825, 262419, 361275, 481899, 1354828, 6328548, 6679881

Still, it is conjectured that there are infinitely many Cullen primes. As of February 2016, the largest known Cullen prime is $6679881 \times 2^{6679881} + 1$. It is a megaprime with 2,010,852 digits and was discovered by a PrimeGrid participant from Japan.

Proof

To prove there are an infinite number of Cullen Primes, the author will need to use another famous number theory conjecture, the Goldbach Conjecture, which has been unsolved for hundreds of years, until recently proved by the author (see reference 2).

The Goldbach Conjecture states that for every even integer N, and $N > 2$, then $N = P1 + P2$, where $P1$, and $P2$, are prime numbers.

Again, Cullen numbers are of the form $C_n = n2^n + 1$, using the Goldbach Conjecture $n2^n$ is always even since any n multiplied by 2 is even and 2 raised to any power is also even. Therefore, we can rewrite $n2^n$ as follows:

$n2^n = P_1 + P_2$, for any n and where P_1 ***and*** P_2 are both prime.

Then we can rewrite $C_n = n2^n + 1$ as follows:

$$C_n = P_1 + P_2 + 1$$

Now we will rewrite C_n as the sum of prime number and any other integer d > 0

$$C_n = P_1 + P_2 + 1 = P_1 + (P_2 + 1) = P_1 + d, \text{ where } d = P_2 + 1$$

Now that we have rewritten the Cullen number equation, we shall proceed to prove that there are an infinite number of Cullen primes. First we shall assume that the set of 16 Cullen Primes are finite and then we shall prove that this is false, which will prove that are Cullen primes are infinite. Even though we have assumed that the set of 16 Cullen primes is finite since there are an infinite number of prime numbers we can pick a prime number p which is outside the finite Cullen Primes. Therefore a prime $p + d$, ***where*** $d = P_2 + 1$ cannot exist that is outside our finite set of Cullen primes otherwise we would have discovered a Cullen prime which is outside our assumed set of finite Cullen primes. Thus all we need to do is to prove that there exists a Cullen prime outside our assumed finite set is to prove that $p + d$ is prime.

Now we shall proceed to prove at least one $p + d$ is prime as follows:
We use the proof, provided in Reference 1, that if $p > 1$ and $d > 0$ are integers, that p and $p + d$, where for our case, $d = P_2 + 1$, are both primes if and only if for positive integer m:

$$m = (p\text{-}1)!\left(\frac{1}{p} + \frac{(-1)\hat{}d(d!)}{p+d}\right) + \frac{1}{p} + \frac{1}{p+d}$$

Please note that ^ indicates an exponent, $(-1)\hat{}d$ is equivalent to (-1) raised to the d power

For our case ***p*** (also known as P_1, but ***p*** will be used for the remainder of this proof) is known to be prime and $d = P_2 + 1$ for Cullen primes, therefore:

$$m = (p\text{-}1)!\left(\frac{1}{p} + \frac{(-1)\hat{}(P2+1)((P2+1)!)}{p+P2+1}\right) + \frac{1}{p} + \frac{1}{p+P2+1}$$

Multiplying by ***p***, and since $P_2 + 1$ is always even since P_2 is always odd since it is prime, then $(-1)\hat{}(P2 + 1) = 1$

$$mp = (p)!\left(\frac{1}{p} + \frac{(P2+1)!}{p+P2+1}\right) + 1 + \frac{p}{p+P2+1}$$

Multiplying by $(p + P2 + 1)$,

$$(p + P2 + 1)mp = (p + P2 + 1)(p)!\left(\frac{1}{p} + \frac{(P2+1)!}{p+P2+1}\right) + p + P2 + 1 + p$$

Reducing again,

$$(p + P2 + 1)mp = (p)!\left(\frac{(p+P2+1)}{p} + (P2 + 1)!\right) + 2p + P2 + 1$$

Factoring out, **(*p*)!,**

$$(p + P2 + 1)mp = p(p\text{-}1)!\left(\frac{(p+P2+1)}{p} + (P2 + 1)!\right) + 2p + P2 + 1$$

And reducing one final time,

$$(p + P2 + 1)mp = (p-1)!(p + P2 + 1 + p(P2 + 1)!) + 2p + P2 + 1$$

We already know **p** is prime, therefore, ***p*** = integer. Since ***p*** is an integer and by definition $P2 + 1$ is an integer, the right hand side of the above equation is an integer (likewise the left hand side of the equation must also be an integer). Since the right hand side of the above equation is an integer and ***p*** and $P2 + 1$ are integers on the left hand side of the equation, then ***p*** **+** $P2 + 1$ is also an integer. Therefore there are only 4 possibilities (see 1, 2a, 2b, and 2c below) that can hold for ***m*** so the left hand side of the above equation is an integer, they are as follows:

1) ***m*** is an integer, or

2) ***m*** is a rational fraction that is divisible by ***p***. This implies that ***n*** **=** $\frac{x}{p}$ where, p is prime and ***x*** is an integer. This results in the following three possibilities:

a. Since ***m*** **=** $\frac{x}{p}$, then **p =** $\frac{x}{m}$, since ***p*** is prime, then ***p*** is only divisible by ***p*** and **1**, therefore, the first possibility is for n to be equal to ***p*** or 1 in this case, which are both integers, thus ***m*** is an integer for this first case.

b. Since ***m*** **=** $\frac{x}{p}$***,*** and x is an integer, then ***x*** is not evenly divisible by ***p*** unless ***x = p,*** or ***x*** is a multiple of ***p***, where ***x = yp***, for any integer **y**. Therefore ***m*** is an integer for ***x = p*** and ***x = yp***.

c. For all other cases of, integer ***x, m = xp , m*** is not an integer.

To prove there is a Cullen Prime, outside our set of finite Cullen Primes, we only need to prove that there is at least one value of ***m*** that is an integer, outside our finite set. There can be an infinite number of values of ***m*** that are not integers, but that will not negate the existence of one Cullen Prime, outside our finite set of Cullen Primes.

First the only way that n cannot be an integer is if every ***m*** satisfies paragraph 2.c above, namely, ***m*** **=** $\frac{x}{p}$, where ***x*** is an integer***, x ≠ p, x ≠ yp, m ≠ p, and m ≠ 1*** for any integer ***y***. To prove there exists at least one Cullen Prime outside our finite set, we will assume that no integer ***m*** exists and therefore no Cullen Primes exist outside our finite set. Then we shall prove our assumption to be false.

Proof: Assumption no values of ***m*** are integers, specifically, every value of ***m*** is ***m*** **=** $\frac{x}{p}$,where ***x*** is an integer, ***x ≠ p, x ≠ yp, m ≠ p,*** and ***m ≠ 1***, for any integer ***y***. Paragraphs **1, 2.a, and 2.b** prove cases where ***m*** can be an integer, therefore our assumption is false and **there exist values of *m* that are integers.**

Since we have already shown that ***p*** and ***p+*** $P2 + 1$**,** where ***d*** **=** $P2 + 1$**,** are both primes if and only if for integer ***m***:

$$m = (p-1)!\left(\frac{1}{p} + \frac{(-1)\hat{}d(d!)}{p+d}\right) + \frac{1}{p} + \frac{1}{p+d}$$

It suffices to show that there is at least one integer n to prove there exists a Cullen Prime outside our set of finite set of Cullen Primes.
Since there exists an ***m*** = integer, we have proven that there is at least one ***p*** and $P2 + 1$ that are both prime. Since ***p*** + $P2 + 1$ is prime and it is also greater than ***p*** then it also is not in the finite set of Cullen primes, therefore, since we have proven that there is at least one ***p*** + $P2 + 1$ that is prime, then we have proven that there is a Cullen prime outside the our assumed finite set of Cullen primes. This is a contradiction from our assumption that the set of Cullen primes is finite, therefore, by contradiction the set of Cullen primes is infinite. Also this same proof can be repeated infinitely for each finite set of Cullen primes, in other words a new Cullen prime can added to each set of finite Cullen primes making the Cullen primes countably infinite. This thoroughly proves that an infinite number of Cullen primes exist.

References:

1) 1001 Problems in Classical Number Theory, Jean-Marie De Koninck and Armel Mercier, 2004, Exercise Number 161

2) Elementary Proof of the Goldbach Conjecture, Stephen Marshall, 13 February 2017, http://vixra.org/abs/1702.0150