

MERSENNE PRIMES IN IMAGINARY QUADRATIC NUMBER FIELDS

KAROLINE PERSHELL AND LORAN HUFF

ABSTRACT. We examine all primes of the form $b^n - 1$ in imaginary quadratic number fields, noting that besides a finite list of specific prime numbers, we find only three interesting classes of primes. Using the rational Mersenne primes (the first of the three cases) as a model, we follow Robert Spira and Mike Oakes in defining the Gaussian Mersenne primes to be the primes of the form $(1 \pm i)^p - 1$ and the Eisenstein Mersenne primes to be the primes of the form $\left(\frac{3 \pm \sqrt{-3}}{2}\right)^p - 1$. We show how to characterize these via their norms, list the known examples and speculate on their distributions.

1. INTRODUCTION

Euclid studied perfect numbers in his famous text *The Elements*. He proved that if $2^k - 1$ is prime, then $2^{k-1}(2^k - 1)$ is perfect. Later Euler proved that every even perfect number has this form [5].

A necessary condition for $2^k - 1$ to be prime is that k must be a prime number. Several early writers believed that this was a sufficient condition; that is, that all numbers of the form $2^p - 1$ are prime when p is prime. The counterexample $p = 11$ shows this is incorrect.

Other generalized forms of prime numbers have been studied. For example, the Cunningham project [3] seeks to factor numbers of the form $b^n - 1$, of which the Mersenne primes are a specific case.

In this paper, we will further generalize the Mersenne primes by examining primes of the form $b^n - 1$ in imaginary quadratic number fields. The distinguishing properties that characterize the rational Mersenne primes are used to characterize both the Gaussian Mersenne primes and the Eisenstein Mersenne primes. We will show the following theorem:

Date: 30 April 2002.

1991 Mathematics Subject Classification. Primary 11A41, 11Y11; Secondary 11R11, 11R27.

Key words and phrases. Elementary prime number theory, imaginary quadratic fields, Mersenne primes, heuristics.

Theorem 1.1. *If b is an element of an imaginary quadratic number field, and n is an integer greater than 1, such that $b^n - 1$ is prime, then n is a rational prime and either*

- * $b = 2$, and $2^n - 1$ is a rational prime,
- * $b = (1 \pm i)$, and $2^p - (2/p)2^{(p+1)/2} + 1$ is a rational prime,
- * $b = \frac{3 \pm \sqrt{-3}}{2}$, and $3^p - (3/p)3^{(p+1)/2} + 1$ is a rational prime.

Or we get one of these special cases:

- * $b = \pm i$ and n is odd, yielding the primes $-1 \pm i$,
- * $b = -1 \pm i$, yielding the primes $\pm 1 \pm 2i$,
- * $b = -2$ yields only the prime 3,
- * $b = \frac{-3 \pm \sqrt{-3}}{2}$ then $b^n - 1 = \frac{-5 \pm \sqrt{-3}}{2}$ (only for $n = 1$) and $\frac{1 \pm 3\sqrt{-3}}{2}$,
- * $b = 1 \pm \sqrt{-3}$ and $n = 1$, yields the primes $1 \pm \sqrt{-3}$,
- * $b = -1 \pm \sqrt{-3}$ and $n = 1$, yielding the primes $-2 \pm \sqrt{-3}$.

The work presented here is related to a number of other results. Robert Spira [13] generalized the concept of Mersennes, not by focusing on the form of the number (as is done in this paper), but by first defining a sum of divisors function and then a generalization of a perfect number for the Gaussian numbers. He was led to a theorem similar to Euclid's and defined complex Mersenne primes to be $-i[(1+i)^k - 1]$ [7]. These are associates of the forms we call Gaussian Mersenne primes.

Steve Ligh and Pat Jones have also investigated a generalization of Mersenne primes by studying the numbers

$$L(k, n) = 1 + 2^n + (2^n)^2 + (2^n)^3 + \dots + (2^n)^{k-1}.$$

This form includes both the Fermat numbers $L(2, 2^n)$ and the Mersenne numbers $L(k, 1)$ [6]. Finally, a recent paper by Peter Beelen and Jeroen Doumen also produces primality conjectures for Gaussian and Eisenstein Mersenne primes using elliptic curves [1].

The plan of this paper is as follows: we will recall the basic properties of the rational Mersenne primes in Section 2 and the basic properties of imaginary quadratic number fields in Section 3. We use these properties to define the Gaussian Mersenne primes in Section 4 and characterize them by their norms in Section 5. Sections 6 and 7 mirror Sections 4 and 5, now defining the Eisenstein Mersenne primes and characterizing these numbers by their norms. Section 8 shows how the Gaussian Mersenne and Eisenstein Mersenne primes are now amenable to the classic primality tests. Finally, we speculate on their distributions in Section 9.

2. THE RATIONAL MERSENNE PRIMES

As an example for future reference, let us consider a general rational Mersenne number. Suppose $b^n - 1$ is a prime number for a rational integer b and a positive integer n . Since $b^n - 1 = (b - 1)(b^{n-1} + b^{n-2} + \dots + 1)$ and $b^n - 1$ is prime, one of the two factors must be a unit.

If the first is a unit, that is $b - 1 = \pm 1$, then $b = 2$ (because $b = 0$ cannot yield a prime). We also need to consider when the second factor, $b^{n-1} + b^{n-2} + \dots + 1$, is a unit. To do so, we will use the following lemma.

Lemma 2.1. *Let b be an integer in an imaginary quadratic number field. If $b^{n-1} + b^{n-2} + \dots + 1$ is a unit with $n > 1$, then $N(b) \leq 4$.*

Proof. If $b^{n-1} + b^{n-2} + \dots + 1 = (b^n - 1)/(b - 1)$ is a unit, then its norm is 1. Since $N(\alpha) = |\alpha|^2$ in imaginary quadratic fields, we have

$$|b^n - 1| = |b - 1|.$$

By the triangle inequality we then have

$$|b|^n - 1 \leq |b^n - 1| = |b - 1| \leq |b| + |-1|$$

Therefore

$$|b|^n \leq |b| + 2.$$

Suppose $|b| > 2$ (otherwise $N(b) \leq 4$ and we are done). The last inequality then gives $|b|^n < |b| + |b|$ which is $|b|^n \leq 2|b|$ or $|b|^{n-1} \leq 2$. However, $n \geq 2$, so this gives us the contradiction

$$|b| \leq |b|^{n-1} \leq 2.$$

□

We see now that if $b^{n-1} + b^{n-2} + \dots + 1 = \pm 1$ for some rational integer b , then either $b = 2$ or one of the following holds:

- * $n = 1$, so b is a prime plus 1 (then $b^n - 1$ yields all primes p),
- * $b = -2$, so $n = 2$ (which yields the prime 3), or
- * $b = -1$, so n is odd (which yields -2)

Mathematicians traditionally consider these cases to be uninteresting. This leaves the case $b = 2$ to consider.

Note that for $2^n - 1$ to be prime, the exponent n must be prime. Otherwise, if the rational integer n has the nontrivial factorization $n = rs$, then $2^n - 1$ has the nontrivial factor $2^s - 1$. This gives us the following definition:

Definition 2.2. The **Mersenne primes** are primes of the form $M_p = 2^p - 1$ where p is a rational prime.

These numbers are known to be prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593$ and 13466917 [16].

3. BACKGROUND

Here we note several of the properties and definitions that we will use. (See [2] for explanations of the following.)

* For a positive integer d , the algebraic integers in $\mathbb{Q}[\sqrt{-d}]$ are the numbers α given by:

$$\alpha = \begin{cases} \frac{a + b\sqrt{-d}}{2} \text{ with } a \equiv b \pmod{2} & \text{if } d \equiv 1 \pmod{4} \\ a + b\sqrt{-d} \text{ with } a, b \in \mathbb{Z} & \text{if } d \not\equiv 1 \pmod{4} \end{cases}$$

[5].

* The **units** are the divisors of 1 (the invertible elements). The units in $\mathbb{Q}[\sqrt{-d}]$ are only ± 1 unless $d = 1$ or 3.

* When $d = 1$ there are four units, $\{\pm 1, \pm i\}$. When $d = 3$ there are six units, $\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$.

* The Gaussian and Eisenstein integers are algebraic integers of the form $a + bi$ and $\frac{a + b\sqrt{-3}}{2}$ with $a \equiv b \pmod{2}$, respectively, where a and b are rational integers.

* An integer, π in $\mathbb{Q}[\sqrt{-d}]$ is prime if and only if the decomposition into the product of two integers, $\pi = \alpha\beta$ implies either α or β is a unit.

* If the ratio of two elements is a unit, then the two elements are called **associates**.

* In all quadratic number fields, the norms of elements α and β satisfy $N(\alpha) = |\alpha|^2$, and $N(\alpha\beta) = N(\alpha)N(\beta)$. Therefore α is a unit if and only if its norm is one. If $N(\alpha)$ is a rational prime, then the integer α is a prime.

For Gaussian integers, the primes can be completely characterized with the following theorem:

Theorem 3.1. *The Gaussian integer $a + bi$ is prime if and only if either its norm is prime, or $b = 0$ and a is a rational prime congruent to 3 (mod 4). (For a proof, see [12, p. 168].)*

For Eisenstein integers, the primes can be completely characterized with the following theorem:

Theorem 3.2. *The Eisenstein integer $\frac{a+b\sqrt{-3}}{2}$ is prime if and only if either its norm is prime, or it is a rational prime congruent to 2 (mod 3). (For a proof, see [11, p. 99].)*

4. THE GAUSSIAN MERSENNE PRIMES

Now, let us fit Gaussian integers into the framework of the Mersenne primes. Suppose $b^n - 1$ is a prime number for a Gaussian integer b and a positive rational integer n . Since $b^n - 1 = (b - 1)(b^{n-1} + b^{n-2} + \dots + 1)$, we again know that either $b - 1$ or $b^{n-1} + b^{n-2} + \dots + 1$ is a unit. We consider when each could be a unit.

If $b - 1$ is our unit, we have the following cases.

- * $b - 1 = -1$, therefore $b = 0$, and $b^n - 1 = -1$. However, -1 is not a prime.
- * $b - 1 = 1$, therefore $b = 2$ and these are the rational Mersenne primes
- * $b - 1 = i$, therefore $b = 1 + i$.
- * $b - 1 = -i$, therefore $b = 1 - i$

The last two choices for b yield the Gaussian Mersenne primes in conjugate pairs.

Lemma 2.1 allows us to do an exhaustive search of all cases for which $b^{n-1} + b^{n-2} + \dots + 1$ is a unit and $b^n - 1$ is prime, by only considering the cases when $N(b) = 0, 1, 2, 3$, or 4.

- $N(b) = 0$ Therefore $b = 0$, but $b^n - 1 = -1$, which is not prime.
- $N(b) = 1$ Therefore $b = \pm 1, \pm i$. When $b = 1$, $b^n - 1 = 0$, which is not prime. When $b = -1$, $b^n - 1 = 0$ or -2 , neither of which is a Gaussian prime. When $b = \pm i$, then $b^n - 1$ will yield only the prime $-1 \pm i$ (when n is odd).
- $N(b) = 2$ Therefore $b = \pm 1 \pm i$. When $b = -1 \pm i$, $b^n - 1$ yields only the primes, $-1 \pm 2i$ and $1 \pm 2i$. When $b = 1 \pm i$, we have the Gaussian Mersenne primes which we will further investigate.
- $N(b) = 3$ We do not need to consider this case because there is no Gaussian integer with norm 3.
- $N(b) = 4$ Therefore $b = \pm 2$ or $\pm 2i$. When $b = 2$, these are the rational Mersenne primes. When $b = -2$, we have seen that this only yields 3. For $n > 1$, the case when $b = \pm 2i$ yields no primes.

We are generalizing the concept of Mersenne primes, so as in the case of the rational Mersenne primes, we will ignore all of these cases as trivial, and instead focus on the case of $b = 1 \pm i$. We have examined all of the other cases above.

Finally, if the rational integer n has the nontrivial factorization $n = rs$, then $(1 \pm i)^n - 1$ has the nontrivial factor $(1 \pm i)^s - 1$, so it cannot be prime. For these reasons we define the following:

Definition 4.1. The **Gaussian Mersenne primes** are the Gaussian primes of the form $(1 \pm i)^p - 1$ where p is a rational prime. These primes come in conjugate pairs.

5. THE NORMS OF THE GAUSSIAN MERSENNE PRIMES

As mentioned before, a Gaussian integer is prime if and only if either its norm is prime or the Gaussian integer is a rational prime congruent to 3 (mod 4). Therefore, we next calculate the norm of the Gaussian Mersenne $(1 \pm i)^n - 1$. First, we prove the following lemma.

Lemma 5.1.

$$N((1 \pm i)^n - 1) = \begin{cases} 2^n + 1 & \text{if } 2 \parallel n \\ (2^{n/2} - (-1)^{n/4})^2 & \text{if } 4 \mid n \\ 2^n - (-1)^{(n^2-1)/8} 2^{(n+1)/2} + 1 & \text{if } 2 \nmid n \end{cases}$$

Proof. The key to this proof is that $(1 + i)^4 = (1 - i)^4 = -4$. We also note that

$$\begin{aligned} (1 + i)^0 + (1 - i)^0 &= 2 \\ (1 + i)^1 + (1 - i)^1 &= 2 \\ (1 + i)^2 + (1 - i)^2 &= 0 \\ (1 + i)^3 + (1 - i)^3 &= -4. \end{aligned}$$

It then follows that

$$\begin{aligned} (1 + i)^{0+4m} + (1 - i)^{0+4m} &= 2(-4)^m = (-1)^m 2^{2m+1} \\ (1 + i)^{1+4m} + (1 - i)^{1+4m} &= 2(-4)^m = (-1)^m 2^{2m+1} \\ (1 + i)^{2+4m} + (1 - i)^{2+4m} &= 0(-4)^m = 0, \text{ and} \\ (1 + i)^{3+4m} + (1 - i)^{3+4m} &= (-4)^{m+1} = (-1)^{m+1} 2^{2m+2} \end{aligned}$$

The first and third of these give the first two cases of the following:

$$(5.1) \quad (1 + i)^n + (1 - i)^n = \begin{cases} 0 & \text{if } 2 \parallel n \\ (-1)^{n/4} 2^{n/2+1} & \text{if } 4 \mid n \\ (-1)^{(n^2-1)/8} 2^{(n+1)/2} & \text{if } 2 \nmid n \end{cases}$$

To see the second and fourth give the third case, it is sufficient to check that $(-1)^{(n^2-1)/8} = (-2/p)$ matches $(-1)^m$ (and $(-1)^{m+1}$ respectively) in these cases.

Finally,

$$\begin{aligned} N((1 \pm i)^n - 1) &= ((1 + i)^n - 1)((1 - i)^n - 1) \\ &= (1 + i)^n(1 - i)^n - (1 + i)^n - (1 - i)^n + 1 \end{aligned}$$

so the lemma follows easily from equation 5.1. □

By Theorem 3.1 we now have the following theorem.

Theorem 5.2. $(1 \pm i)^p - 1$ are Gaussian Mersenne primes if and only if p is 2 or

$$2^p - (-1)^{(p^2-1)/8}2^{(p+1)/2} + 1 = 2^p - (2/p)2^{(p+1)/2} + 1$$

is a rational prime, where $(2/p)$ is the Legendre symbol.

Note that this norm is one of the factors in the Aurifeuillian factorization

$$2^{4n+2} + 1 = (2^p - (2/p)2^{(p+1)/2} + 1)(2^p + (2/p)2^{(p+1)/2} + 1).$$

There are several dozen known prime numbers of these two forms [3]. The following theorem shows why the other factor in the Aurifeuillian factorization of $(1 + i)^p - 1$ is always composite.

Theorem 5.3. For every odd prime p , 5 divides $2^p - (2/p)2^{(p+1)/2} + 1$.

Proof. We note that $2^p \pmod{5}$ is cyclic modulo 4, $2^{(p+1)/2} \pmod{5}$ is cyclic modulo 8, and $(2/p) \pmod{5}$ is cyclic modulo 8. Therefore it is sufficient to only check the values of $2^p - (2/p)2^{(p+1)/2} + 1$ for each prime $p \equiv 1, 3, 5, 7 \pmod{8}$. We used 3, 5, 7, and 17 to see 5 always divides $2^p - (2/p)2^{(p+1)/2} + 1$. □

The Gaussian Mersenne primes have, therefore, been characterized by their norms, with a condition that can be checked and is amendable to the classic primality tests, as is later shown.

Wayne McDaniel's work in 1973 also characterizes the Gaussian Mersenne primes, or "complex Mersennes," as he refers to them. Our work above begins with the norm of the numbers, then case by case determines which yield primes. McDaniel, however, begins with a definition, Gaussian perfect numbers, then develops the requirements for primality [7]. He ends with the form of Gaussian numbers

$$-i[(1 + i)^k - 1].$$

Note these are associates of ours.

6. THE EISENSTEIN MERSENNE PRIMES

We now consider the Eisenstein integers. Again, suppose $b^n - 1$ is prime. We know that either $b - 1$ is a unit, or $b^{n-1} + b^{n-2} + \dots + 1$ is a unit. If $b - 1$ is a unit then we have the following cases:

- * $b - 1 = \pm 1$, therefore $b = 0$ or 2 , but these cases have already been considered.
- * $b - 1 = \frac{-1 \pm \sqrt{-3}}{2}$, therefore $b = \frac{1 \pm \sqrt{-3}}{2}$. This is a unit and will only yield the primes, $\frac{-3 \pm \sqrt{-3}}{2}$.
- * $b - 1 = \frac{1 \pm \sqrt{-3}}{2}$, therefore $b = \frac{3 \pm \sqrt{-3}}{2}$. This case gives rise to the Eisenstein Mersennes in conjugate pairs.

We also need to consider when $b^{n-1} + b^{n-2} + \dots + 1$ is a unit, and we refer back to Lemma 2.1. We will consider when $a^2 + 3b^2 \leq 16$, which only gives the following cases:

- $N(b) = 0$ Therefore $b = 0$ and $b^n - 1 = -1$ which is not prime.
- $N(b) = 1$ Therefore $b = \pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}$. The cases of $b = \pm 1$ and $\frac{1 \pm \sqrt{-3}}{2}$ have already been considered. When $b = \frac{-1 \pm \sqrt{-3}}{2}$, $b^n - 1$ will yield the primes $\frac{-3 \pm \sqrt{-3}}{2}$ only for $n = 1$.
- $N(b) = 2$ There is nothing to consider since there is no Eisenstein integer with norm 2.
- $N(b) = 3$ Therefore $b = \pm \sqrt{-3}$ and $b = \frac{\pm 3 \pm \sqrt{-3}}{2}$. When $b = \pm \sqrt{-3}$ then $b^n - 1$ yields no primes. If $b = \frac{-3 \pm \sqrt{-3}}{2}$, then $b^n - 1 = \frac{-5 \pm \sqrt{-3}}{2}$ (only for $n = 1$) and $\frac{1 \pm 3\sqrt{-3}}{2}$. When $b = \frac{3 \pm \sqrt{-3}}{2}$ we get the Eisenstein Mersenne primes which will be considered later.
- $N(b) = 4$ Therefore $b = \pm 2$ and $\pm 1 \pm \sqrt{-3}$. The case of $b = \pm 2$ has already been considered. If $b = 1 \pm \sqrt{-3}$, then $b^n - 1$ yields the primes $\pm \sqrt{-3}$ only for $n = 1$. If $b = -1 \pm \sqrt{-3}$, then $b^n - 1$ yields the primes $-2 \pm \sqrt{-3}$ only for $n = 1$.

We have completely examined these cases and found that all, except for the case of $b = \frac{3 \pm \sqrt{-3}}{2}$, yield a finite set of primes. Therefore only the case of $b = \frac{3 \pm \sqrt{-3}}{2}$ is of interest. For these reasons we define the following:

Definition 6.1. The **Eisenstein Mersenne primes** are the Eisenstein primes of the form $\left(\frac{3 \pm \sqrt{-3}}{2}\right)^p - 1$ where p is a rational prime.

We require the exponent to be prime because if the rational integer n has the nontrivial factorization $n = rs$, then $\left(\frac{3 \pm \sqrt{-3}}{2}\right)^n - 1$ has the nontrivial factor $\left(\frac{3 \pm \sqrt{-3}}{2}\right)^s - 1$, and cannot be prime.

7. THE NORMS OF THE EISENSTEIN MERSENNE PRIMES

An Eisenstein integer is prime if and only if either its norm is prime or it is a rational prime congruent to 2 (mod 3). Therefore, we next need to calculate the norm of the Eisenstein Mersenne $\left(\frac{3 \pm \sqrt{-3}}{2}\right)^p - 1$.

The key to calculating these norms is to note that $\left(\frac{3 \pm \sqrt{-3}}{2}\right)^6 = -27$.

$$\begin{aligned} N(b^{6n} - 1) &= 3^{6n} - 2(-3)^{3n} + 1 \\ N(b^{6n+1} - 1) &= 3^{6n+1} + (-3)^{3n+1} + 1 \\ N(b^{6n+2} - 1) &= 3^{6n+2} + (-3)^{3n+1} + 1 \\ N(b^{6n+3} - 1) &= 3^{6n+3} + 1 \\ N(b^{6n+4} - 1) &= 3^{6n+4} + (-3)^{3n+2} + 1 \\ N(b^{6n+5} - 1) &= 3^{6n+5} - (-3)^{3n+3} + 1 \end{aligned}$$

The first case is a perfect square and therefore not prime. The third case yields multiples of 7, therefore 7 is the only prime. The fourth case is even, but is never 2, thereby yielding no primes. The fifth case again gives us only multiples of 7 and no primes. All of these cases are trivial, so we will ignore them and instead focus on the second and sixth cases, which give rise to the following theorem.

Theorem 7.1. *The numbers $\left(\frac{3 \pm \sqrt{-3}}{2}\right)^p - 1$ are Eisenstein Mersenne primes if and only if p is 2 or*

$$3^p - (3/p)3^{(p+1)/2} + 1$$

is a rational prime, where $(3/p)$ is the Legendre symbol.

Note how the norms of the Eisenstein Mersenne primes are identical in structure to the norms of the Gaussian Mersenne primes. This expression in 7.1 is also related to an Aurifeuillian factorization of

$$3^{3p} + 1 = (3^p - (3/p)3^{(p+1)/2} + 1)(3^p + (3/p)3^{(p+1)/2} + 1).$$

The following theorem shows why the other factor in the Aurifeuillian factorization of $\left(\frac{3 \pm \sqrt{-3}}{2}\right)^p - 1$ is always composite.

Theorem 7.2. *For odd primes p , 7 divides $3^p - (3/p)3^{(p+1)/2} + 1$.*

Proof. We note that $3^p \pmod{7}$ is cyclic modulo 6, $3^{(p+1)/2} \pmod{7}$ is cyclic modulo 12, and $(3/p) \pmod{7}$ is cyclic modulo 12. Therefore it is sufficient to only check the values of $3^p - (3/p)3^{(p+1)/2} + 1$ for one prime, $p \equiv 1, 5, 7,$ or 11 , modulo 12. We used 5, 7, 11 and 13 to see 7 always divides $3^p - (3/p)3^{(p+1)/2} + 1$. \square

8. PROVING PRIMALITY

We have now established characterizations of the Gaussian Mersenne and Eisenstein Mersenne primes. By the above theorems, we see that both are amenable to the classic primality tests. For the Gaussian Mersenne primes, we need only to determine if

$$2^n - (-1)^{(n^2-1)/8} 2^{(n+1)/2} + 1$$

is prime. To do so, we can use Proth's theorem [10, p. 52]:

Theorem 8.1 (Proth's Theorem 1878). *Let $n = 2^k h + 1$ with $2^k > h$. If there is an integer a such that $a^{(n-1)/2} \equiv -1 \pmod{n}$, then n is prime.*

It has been proven that $(1 \pm i)^p - 1$ is prime for $p = 2, 3, 5, 7, 11, 19, 29, 47, 73, 79, 113, 151, 157, 163, 167, 239, 241, 283, 353, 367, 379, 457, 997, 1367, 3041, 10141, 14699, 27529, 49207, 77291, 85237, 106693, 160423, 203789$ and 364289 . Mike Oakes, using this theorem and Chris Nash's program OpenPFG [9], is credited with discovering most of the largest values of n . He teamed with Nicholas M. Glover to find the largest in June 2001 [4].

For the Eisenstein Mersenne primes, we can apply a theorem of Henry Pocklington's [15, p. 123] to test whether either of the norms listed in Theorem 7.1 are prime.

Theorem 8.2 (Pocklington, 1914). *Let $n = q^k h + 1$ where q is a prime and $q^k > h$. If there is an integer a such that $a^{n-1} \equiv 1 \pmod{n}$, and $\gcd(a^{(n-1)/q}, n) = 1$, then n is prime.*

It has been proven that $\left(\frac{3 \pm \sqrt{-3}}{2}\right)^p - 1$ is prime for $p = 2, 5, 7, 11, 17, 19, 79, 163, 193, 239, 317, 353, 659, 709, 1049, 1103, 1759, 2029, 5153, 7541, 9049, 10453,$ and 23743 [1].

9. WAGSTAFF CONJECTURE

It has been conjectured that for rational Mersenne primes M_n , the graph of the $\log_2 \log_2 M_n$ versus n is approximately linear, where M_n is the n th Mersenne prime. In fact, Wagstaff conjectured that $\log_2 \log_2 M_n$ has Poisson distribution with mean 2 to the power $1/e^\gamma$ or about

1.47576 [12, p. 33] and [14]. Figure 1 shows $\log_2 \log_2 M_n$ versus n . As Wagstaff conjectured, it is approximately linear.

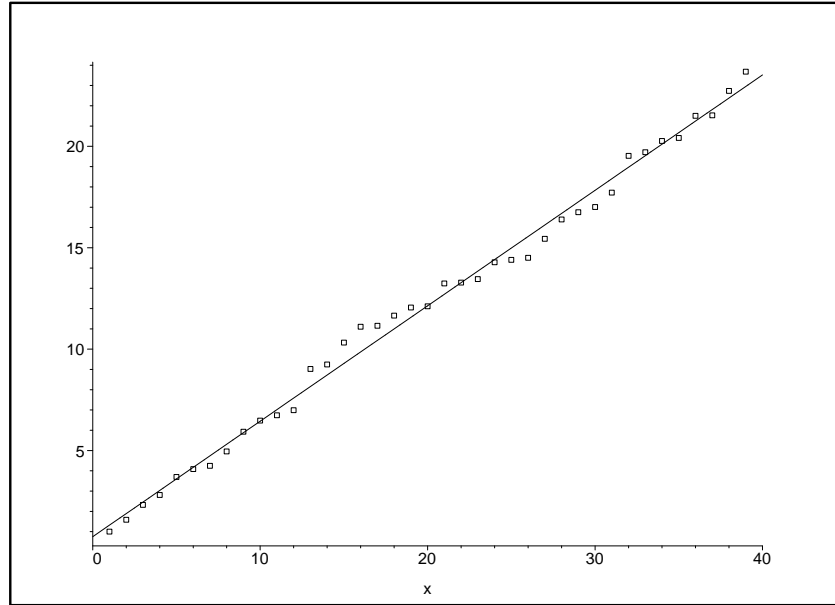
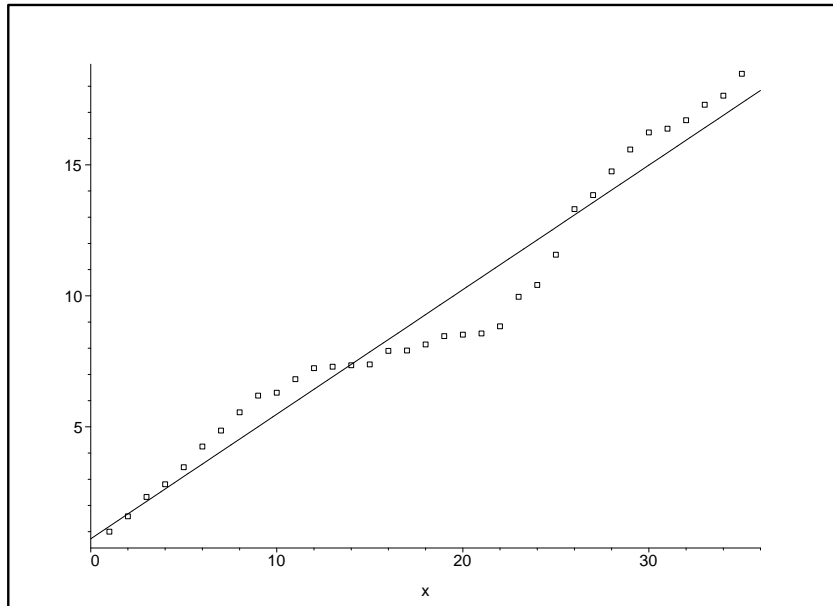
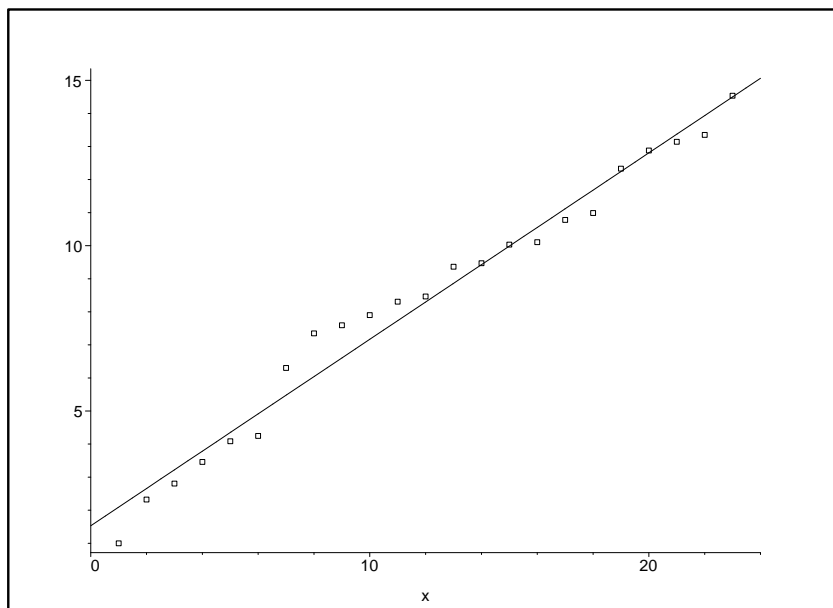


FIGURE 1. n versus $\log_2 \log_2 M_n$

It seems reasonable to conjecture that the graph $\log_2 \log_2$ of the n^{th} Gaussian Mersenne prime (GM_n) versus n follows a similar distribution. Figure 2 shows that the Gaussian Mersenne primes are not as nicely linear as the Mersenne primes, in fact deviating quite smoothly from the regression line. Perhaps as more Gaussian Mersenne primes are found, the graphs will more closely resemble one another.

Finally, we plot the graph of $\log_2 \log_2$ of the n^{th} Eisenstein Mersenne prime (E_n) versus n . Figure 3 shows that the distribution follows the regression line fairly well.

FIGURE 2. n verses $\log_2 \log_2 GM_n$ FIGURE 3. n verses $\log_2 \log_2 E_n$

REFERENCES

1. Beelen, P. and Doumen, J. *Math. of Comp.*, 2002, preprint.
2. Bressoud, D. and Wagon, S. *Computational Number Theory*, Key College Publishing, 2000.

3. Brillhart, J. et al., *Factorization of $b^n \pm 1$* , American Mathematical Society, 1985.
4. Caldwell, C. "The Largest Known Primes," June 2001,
<http://www.utm.edu/research/primes/largest.html>.
5. Dence, J. *Elements of the Theory of Numbers*, Academic Press, 1999.
6. Ligh, S. and Jones, P. "Generalized Fermat and Mersenne Numbers,"
Fibonacci Quarterly, 20 1982, 12-16.
7. McDaniel, W. "Perfect Gaussian integers," *Acta Arith.* 25, 1973/74, 137-144.
8. Mullin, A. Letter to the editor: "The new Mersenne conjecture," *Amer. Math. Monthly* 96, No. 6, 1989, 511.
9. Nash, C. "User Group for the PrimeForm Program," April 2002,
<http://groups.yahoo.com/group/primeform/>.
10. Ribenboim, P. *The New Book of Prime Number Records*, Springer-Verlag, 1996.
11. Rose, H. *A Course in Number Theory: 2nd Edition*, Oxford University Press, 1994.
12. Schroeder, M. *Number Theory in Science and Communication, With Applications in Cryptography, Physics, Biology, Digital Information, and Computing*, Springer-Verlag, 1984.
13. Spira, R. "The complex sum of divisors" *Amer. Math. Monthly*, 68, 1961, 120-124.
14. Wagstaff, S. Jr. "Divisors of Mersenne Numbers" *Math. Comp.*, 40, No. 161, 1983, 385-397.
15. Williams, H. C. *Eduard Lucas and Primality Testing: Canadian Mathematical Society Series of Monographs and Advanced Texts*, John Wiley & Sons, Inc., 1998.
16. Woltman, G. "The Great Internet Mersenne Prime Search," March 2001,
<http://www.mersenne.org>

KAROLINE PERSHELL, UNDERGRADUATE STUDENT, DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF TENNESSEE AT MARTIN
E-mail address: karppers@mars.utm.edu

LORAN HUFF, UNDERGRADUATE STUDENT, DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF TENNESSEE AT MARTIN
E-mail address: huff@math.utk.edu