MATHEMATICS OF COMPUTATION
Volume 79, Number 271, July 2010, Pages 1779–1791
S 0025-5718(10)02324-0
Article electronically published on March 3, 2010

GAUSSIAN MERSENNE AND EISENSTEIN MERSENNE PRIMES

PEDRO BERRIZBEITIA AND BORIS ISKRA

Abstract. The Biquadratic Reciprocity Law is used to produce a deterministic primality test for Gaussian Mersenne norms which is analogous to the Lucas–Lehmer test for Mersenne numbers. It is shown that the proposed test could not have been obtained from the Quadratic Reciprocity Law and Proth's Theorem. Other properties of Gaussian Mersenne norms that contribute to the search for large primes are given. The Cubic Reciprocity Law is used to produce a primality test for Eisenstein Mersenne norms. The search for primes in both families (Gaussian Mersenne and Eisenstein Mersenne norms) was implemented in 2004 and ended in November 2005, when the largest primes, known at the time in each family, were found.

0. Introduction

Numbers of the form $2^p - 1$, where p is a prime number are known as Mersenne numbers and denoted by M_p. They were named in honor of Father Marin Mersenne (1588–1648). Mersenne numbers have played a key role in the history of primality testing. They arise naturally in the search for primes of the form $a^n - 1$, where a is an integer.

Indeed, from the equation $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$, it is easy to deduce that $a^d - 1$ divides $a^n - 1$ for each divisor d of n. It follows that if $a^n - 1$ is prime, then $a = 2$ and $n = p$ is prime.

Mersenne numbers that are prime are called Mersenne primes. There are currently 47 known Mersenne primes. The largest known Mersenne prime is also the largest known prime. It is $M_{43112609}$ and was found in August 2008 by GIMPS (Great International Mersenne Prime Search). GIMPS is a collaborative project whose goal is to find Mersenne primes, using software designed for that purpose, based on properties of these numbers, the most relevant of these being the Lucas-Lehmer Test. The 13 largest Mersenne primes have been found by GIMPS. The top 9 of this list are the 9 largest primes known to date.

Why is the set of numbers $\{M_n = 2^n - 1 |\ n \in \mathbb{N}\}$ preferred for the search for very large primes? We list the following properties of M_n, the proofs of which can be found in [B], [R], [W] among dozens of other possible references.

MP1: If M_n is prime, then $n = p$ is prime.

MP2 (Euler): If $p > 2$ is prime and q divides M_p, then $q \equiv 1 \pmod{p}$ and $q \equiv \pm 1 \pmod{8}$.

Received by the editor March 3, 2009 and, in revised form, July 17, 2009.
2010 *Mathematics Subject Classification.* Primary 11Y11.

MP3 (Lucas-Lehmer Test): Let $S_0 = 4$ and $S_{k+1} = S_k^2 - 2$ for $k \geq 0$. Let p be an odd prime. Then M_p is prime if, and only if, $S_{p-2} \equiv 0 (\text{mod } M_p)$.

MP4: Reduction modulo M_p is very fast.

MP1 was mentioned above. It indicates that the search for primes of the form $2^n - 1$ may be restricted to prime exponents n. **MP2** is useful for the search for small prime divisors. It shows that the possible divisors of M_p lie in two specific arithmetic progressions with common difference $8p$. **MP3** is the most important property. It provides a very efficient algorithm which determines the primality of M_p. Indeed, **MP3** shows that one only has to compute $p - 2$ (which is less than $\log_2(M_p)$) squares modulo M_p to determine the primality of M_p (recall that the cost of squaring an m bit integer using Fast Fourier Transform is around 2/3 of the cost of multiplying two different m bit integers). We next explain precisely what we mean by **MP4**: The algorithm at step k computes $S_{k+1} = S_k^2 - 2$ from S_k, which is an integer of at most p bits. Hence, S_{k+1} has at most $2p$ bits. It then has to be reduced Modulo M_p, which has p bits. In general, the cost of reducing a $2p$ bit integer modulo a p bit integer is at least as large as the cost of multiplying two different p bit integers. In contrast, the cost of reduction modulo M_p is equivalent to the cost of adding two different p bit integers, which is much less. Indeed, say z is a $2p$ bit integer; then $z = a2^p + b$, where a and b are p bit integers. Since $M_p = 2^p - 1$, then $2^p \equiv 1 (\text{mod } M_p)$, from which $z \equiv a + b (\text{mod } M_p)$.

It is relevant to point out that there are many families of numbers of the form $A2^n \pm 1$ that share a property analogous to **MP3** (see [W] for a detailed study of these numbers). However, in general, these families do not share properties analogous to **MP1**, **MP2** or **MP4**. That gives the advantage of the use of $\{M_n | \, n \in \mathbb{N}\}$ over other families of the form $\{A2^n \pm 1 \mid n \in \mathbb{N}\}$ (A is a fixed positive integer) regarding the search for huge primes.

In this paper we will study two different families of numbers that share properties analogous to **MP1**, **MP2** and **MP3**, the first of which also shares **MP4**. These families are called Gaussian Mersenne norms and Eisenstein Mersenne norms. To prove the property analogous to **MP3** we make use of the Biquadratic Reciprocity Law for the Gaussian Mersenne norms and the Cubic Reciprocity Law for the Eisenstein Mersenne norms. Moreover, we show that in some sense that we clarify later, our result for the Gaussian Mersenne norms cannot be derived from the Quadratic Reciprocity Law. From our main result we conclude that an implementation of a GIMPS like project for searching for Gaussian Mersenne primes is in order.

The paper is organized as follows: In section 1 we introduce the Gaussian Mersenne norms and study their basic properties, including those analogous to **MP1**, **MP2** and **MP4**, which we denote by **GMP1**, **GMP2** and **GMP4**. In section 2 we state and prove **GMP3**, and show the limitation of the Quadratic Reciprocity Law for that purpose. In section 3 we introduce the Eisenstein Mersenne norms, and we state and prove **EMP1**, **EMP2** and **EMP3**. Our concluding remarks include details of the implementation of the corresponding algorithms.

1. Gaussian Mersenne numbers, norms and primes

Let $\mathbb{Z}[i]$ denote the ring of Gaussian integers. As for $\mathbb{Z}$, we search for irreducible elements of the form $a^n - 1$, where $a \in \mathbb{Z}[i]$ and n is a positive integer. Since $a^n - 1$ is divisible by $a - 1$, it is reasonable to restrict our attention to the case where $a - 1$ is a unit. (Not doing so leads to a finite set of irreducible elements of the form

$a^n - 1$. In fact it leads only to the irreducible elements of norm 2 or of norm 5.) Moreover, if we assume that $a^n - 1$ is irreducible in $\mathbb{Z}[i]$ and that $a - 1$ is a unit, then it is not difficult to show that n must be prime (since $a^d - 1$ is a nonunit and a nontrivial divisor of $a^n - 1$ for any nontrivial divisor d of n).

Since there are exactly four units in the Gaussian ring of integers, the possible values for a are: $a = 2, 0, 1 + i, 1 - i$. $a = 2$ leads to M_n , $a = 0$ leads nowhere, and $a = 1 - i$ leads to the conjugate of the case $a = 1 + i$. We give the following definition:

Definition 1.1. A Gaussian Mersenne number is an element of $\mathbb{Z}[i]$ of the form $(1 \pm i)^p - 1$, for some rational prime p. $(1 + i)^p - 1$ will be denoted by gm_p. A Gaussian Mersenne prime is an irreducible Gaussian Mersenne number.

For $\alpha \in \mathbb{Z}[i]$ we denote by $\mathbf{N}(\alpha) = \alpha\bar{\alpha}$ the norm of α in $\mathbb{Z}[i]$. We note that $\mathbf{N}(gm_p) = \mathbf{N}(\overline{gm_p})$.

Definition 1.2. Let p be a rational prime. The Gaussian Mersenne norm GM_p is defined by

$$GM_p = \mathbf{N}(gm_p).$$

Examples:

$$GM_2 = \mathbf{N}(gm_2) = \mathbf{N}(2i - 1) = 5,$$
$$GM_3 = \mathbf{N}(gm_3) = \mathbf{N}(2i - 3) = 13.$$

According to Chris Caldwell's web page "The Prime Glossary" [C], in 1961 Robert Spira [S] defined the Gaussian Mersenne primes as above. Spira's interest was not directly related to the goal of our paper. Caldwell's page also points out that Mike Oakes improved the list of known Gaussian Mersenne primes (of different norm) to 34 in the year 2000. Currently there are 37 known. The largest corresponds to the exponent $n = 1203793$ and was found in September 2006 by Jaworski. The second largest (exponent $n = 991961$) was found by the second author of this paper in November 2005, using an implementation of the results we present in this paper.

For a positive integer n we let $gm_n = (1 + i)^n - 1$ and $GM_n = \mathbf{N}(gm_n)$.

A direct calculation of gm_n and GM_n leads to the following elementary proposition whose proof is left to the reader.

Proposition 1.3. (1) *If n is odd, then*

$$gm_n = (1 + i)(2i)^{\frac{n-1}{2}} - 1,$$

$$GM_n = 2^n - (-1)^{\frac{n^2-1}{8}} 2^{\frac{n+1}{2}} + 1 \tag{1.1}$$

$$= \begin{cases} 2^n - 2^{\frac{n+1}{2}} + 1 & \text{if} \quad n \equiv \pm 1 \pmod 8 \\ 2^n + 2^{\frac{n+1}{2}} + 1 & \text{if} \quad n \equiv \pm 3 \pmod 8 \end{cases}$$

$$= \left(2^{\frac{n-1}{2}} - (-1)^{\frac{n^2-1}{8}}\right) 2^{\frac{n+1}{2}} + 1 \tag{1.2}$$

$$= \left(2^{\frac{n-1}{2}}\right)^2 + \left(2^{\frac{n-1}{2}} - (-1)^{\frac{n^2-1}{8}}\right)^2, \tag{1.3}$$

GM_n occurs as a factor in the following Aurifeuillian factorization:

$$(2^n + 2^{\frac{n+1}{2}} + 1)(2^n - 2^{\frac{n+1}{2}} + 1) = 2^{2n} + 1. \tag{1.4}$$

(2) *If* $n \equiv 0 \pmod 4$,

$$\begin{aligned} gm_n &= (-1)^{\frac{n}{4}} 2^{\frac{n}{2}} - 1, \\ GM_n &= \left((-1)^{\frac{n}{4}} 2^{\frac{n}{2}} - 1\right)^2 = 2^n - (-1)^{\frac{n}{4}} 2^{\frac{n+2}{2}} + 1 \\ &= \left(2^{\frac{n}{2}} - 1\right)^2 + \left(2^{\frac{n}{4}}\left(1 - (-1)^{\frac{n}{4}}\right)\right)^2. \end{aligned}$$

(3) *If* $n \equiv 2 \pmod 4$,

$$\begin{aligned} gm_n &= (-1)^{\frac{n-2}{4}} 2^{\frac{n}{2}} i - 1, \\ GM_n &= 2^n + 1. \end{aligned}$$

(4) *The sequence* $\{GM_n\}_{n=1}^{\infty}$ *is an increasing sequence of integers that starts at* 1.

(5) *If* d *divides* n, *then* gm_d *divides* gm_n *in* $\mathbb{Z}[i]$ *and* GM_d *divides* GM_n.

(6) *If* d *and* n *are relatively prime, then* gm_d *is relatively prime to* gm_n *in* $\mathbb{Z}[i]$ *and* GM_d *is relatively prime to* GM_n.

□

Since every nonreal element of $\mathbb{Z}[i]$ is irreducible if, and only if, its norm is a rational prime, it follows that Gaussian Mersenne primes of different norms are in one-to-one correspondence with prime Gaussian Mersenne norms. So the search for Gaussian Mersenne primes is equivalent to the search for primes p for which GM_p is prime.

We now state the main result of our paper concerning Gaussian Mersenne norms:

Theorem 1.4. *Gaussian Mersenne norms have the following properties:*

GMP1: *If* GM_n *is prime, then* n *is prime.*

GMP2: *If* p *is an odd prime and* q *divides* GM_p, *then* $q \equiv 1 \pmod{4p}$.

GMP3: *Let* p *be an odd prime. Then,* GM_p *is prime if, and only if,*

$$p \equiv 1 \pmod 4 \quad \textit{and} \quad 5^{\frac{GM_p - 1}{4}} \equiv -1 \pmod{GM_p}$$

$$\textit{or}$$

$$p \equiv 3 \pmod 4 \quad \textit{and} \quad 5^{\frac{GM_p - 1}{2}} \equiv -1 \pmod{GM_p}.$$

GMP4: *If* $z = a2^{\frac{3p-1}{2}} + b2^p + c2^{\frac{p-1}{2}} + d$, *where* $0 \le a, c < 2^{\frac{p+1}{2}}$ *and* $0 \le b, d < 2^{\frac{p-1}{2}}$, *then*

$$z \equiv \left[a + (-1)^{\frac{p^2-1}{8}} 2b + c\right] 2^{\frac{p-1}{2}} + d - b - (-1)^{\frac{p^2-1}{8}} a \pmod{GM_p}.$$

Proof of **GMP1**. The proof is immediate from Proposition 1.3, items (4) and (5). □

Proof of **GMP2**. Although various elementary proofs can be given, we include one for sake of completeness: It is enough to prove it for prime divisors q of GM_p. So let such a q be given. Since p is odd, by (1.4) we have

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

Since one of the two factors in the left hand side of the equation is GM_p, we deduce that $2^{2p} \equiv -1 \pmod q$. It follows that the order of 2 modulo q ($ord_q(2)$) is a divisor of $4p$. 2, p and $2p$ are discarded as possible values for $ord_q(2)$ because otherwise we would have $2^{2p} \equiv 1 \pmod q$ (instead of $-1 \pmod q$). To show that $ord_q(2) \neq 4$, it is enough to show that 5 does not divide GM_p. This follows from the fact that $GM_2 = 5$ and (6) in Proposition 1.3.

Proof of **GMP4**. From (1.1) in Proposition 1.3 we get

$$2^p \equiv (-1)^{\frac{p^2-1}{8}} 2^{\frac{p+1}{2}} - 1 \pmod{GM_p}.$$

The result is straightforward. □

The proof of **GMP3** will be given in the next section.

We end this section with a few historical remarks:

The Cunningham Project seeks to factor the numbers $b^n \pm 1$ for $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers n [BLSTW]. (1.4) shows that for odd n's, GM_n is a factor of $2^{2n} + 1$, which is in the list of the numbers to be factored. Hence the interest in Gaussian Mersenne norms is broader than the one presented in this paper.

Spiro's approach to the Gaussian Mersenne integer, which was later enriched by McDaniel [McD] and by Hausmann and Shapiro [HS], extends the notion of even and odd numbers into the ring of Gaussian Integers, the notion of Perfect numbers into the same ring and the connection between Perfect numbers and Mersenne primes.

2. Primality test for Gaussian Mersenne norms

In this section we will prove **GMP3**, which is a very simple and easy to implement deterministic primality test for Gaussian Mersenne norms, comparable to the Lucas-Lehmer Test for Mersenne primes in speed and elegance. A previous discussion is in order: Note first that equation (1.2) implies that GM_p is of the form $A2^s + 1$, where $A < 2^s$. It follows from Proth's Theorem (cf., for example, [B], [W]) that the primality of GM_p could be determined by the verification of an equation of the type $a^{\frac{n-1}{2}} \equiv -1 \pmod{GM_p}$, for some integer a. According to Proth's Theorem, such an a must satisfy $\left(\frac{a}{GM_p}\right) = -1$, where $\left(\frac{a}{n}\right)$ is the Jacobi symbol. Given p, such an a can be found with not much difficulty via Quadratic Reciprocity for the Jacobi symbol. However, implementation is much easier if the choice of a is independent of p. If no such a can be found, implementers usually look for a finite family of $a's$, such that for every p there is an a in the family such that $\left(\frac{a}{GM_p}\right) = -1$. We next show that this is not possible.

Proposition 2.1. *Let $\{a_1, \dots, a_n\}$ be any set of integers. Then, there exist infinitely many primes p such that*

$$\left(\frac{a_i}{GM_p}\right) = 1 \quad \forall i = 1, \dots, n.$$

Proof. Since

$$GM_p \equiv 1 \pmod 8 \text{ for } p > 3,$$

it follows from the Quadratic Reciprocity Law for 2 that $\left(\frac{2}{GM_p}\right) = 1$, so we can assume that the a_i's are odd.

Let $Q = \{q_1, \dots, q_r\}$ be the set of prime divisors of the a_i's. Dirichlet's Theorem on primes in arithmetic progression guarantees the existence of infinitely many primes p satisfying

$$p \equiv 1 \pmod{8(q_1 - 1) \cdots (q_r - 1)}.$$

We will show that for all these primes p and for all the a_i one has $\left(\frac{a_i}{GM_p}\right) = 1$. By the Quadratic Reciprocity Law for the Jacobi symbol, this is equivalent to showing that $\left(\frac{GM_p}{a_i}\right) = 1$ for each i, and by the properties of the Jacobi symbol it will be enough to prove that $\left(\frac{GM_p}{q_j}\right) = 1$, for each $q_j \in Q$. We will in fact prove that $GM_p \equiv 1 \pmod{q_j}$, from which the result follows.

Recall from (1.2) that

$$GM_p = \left(2^{\frac{p-1}{2}} - (-1)^{\frac{p^2-1}{8}}\right) 2^{\frac{p+1}{2}} + 1.$$

Hence, it suffices to prove that

$$2^{\frac{p-1}{2}} - (-1)^{\frac{p^2-1}{8}} \equiv 0 \pmod{q_j}.$$

Since $p \equiv 1 \pmod 8$, then $(-1)^{\frac{p^2-1}{8}} = 1$. Also, since $p \equiv 1 \pmod{8(q_j-1)}$, then $q_j - 1$ divides $\frac{p-1}{2}$. Hence, $1 \equiv 2^{q_j-1} \pmod{q_j}$ implies $1 \equiv 2^{\frac{p-1}{2}} \pmod{q_j}$, so the result follows. □

In spite of the negative result of Proposition 2.1, we will next prove **GMP3**, which shows that we can test primality for these numbers by using $a = 5$, but sometimes raising a to the power $\frac{GM_p-1}{4}$ instead of just raising to $\frac{GM_p-1}{2}$. The proof of **GMP3** relies on the Biquadratic Reciprocity Law. We will follow the excellent treatment on the subject given in chapter 9 of the book of Ireland and Rosen [IR].

Theorem 2.2. *Let p be an odd prime. GM_p is prime if, and only if,*

$$\begin{aligned} 5^{\frac{GM_p-1}{4}} &\equiv -1 \pmod{GM_p} \quad \textit{for} \quad p \equiv 1 \pmod 4, \\ 5^{\frac{GM_p-1}{2}} &\equiv -1 \pmod{GM_p} \quad \textit{for} \quad p \equiv 3 \pmod 4. \end{aligned}$$

Proof. If $p = 3$, then $GM_p = 13$, which is prime. $5^6 \equiv -1 \pmod{13}$ can be verified trivially. So we let p be a prime $p > 3$. We first assume GM_p is prime. Denote by $\lambda = -(gm_p) = 1 - (1+i)^p$. It is irreducible in the ring of Gaussian Integers $\mathbb{Z}[i]$ because its norm is a rational prime. Also λ is primary (i.e., $\lambda \equiv 1 \pmod{(1+i)^3}$). Let $\pi = 2i - 1$. Then, it is easy to see that $\pi\overline{\pi} = 5$ is the primary decomposition of 5 in $\mathbb{Z}[i]$.

By the Biquadratic Reciprocity Law ([IR], Theorem 2 of chapter 9), we have

$$\chi_\lambda(\pi) = \chi_\pi(\lambda),$$

where χ_λ denotes the biquadratic symbol modulo λ and χ_π the biquadratic symbol modulo π. (We note that the power of -1 that appears in the theorem is 1 in our case because $N(\lambda) \equiv 1 \pmod 8$ for $p > 3$.)

By the defining property of the Biquadratic symbol we have $\chi_\lambda(5) \equiv 5^{\frac{GM_p-1}{4}} \pmod{\lambda}$. Since $\pi\overline{\pi} = 5$, then $\chi_\lambda(5) = \chi_\lambda(\pi)\chi_\lambda(\overline{\pi})$, which equals, by the Biquadratic Reciprocity Law, $\chi_\pi(\lambda)\chi_{\overline{\pi}}(\lambda)$. Hence, we need only to compute $\chi_\pi(\lambda)$ and $\chi_{\overline{\pi}}(\lambda)$:

$$\begin{aligned} \chi_\pi(\lambda) &\equiv \lambda^{\frac{N(\pi)-1}{4}} \equiv \lambda \equiv 1 - (1+i)^p \\ &\equiv 1 - (1+i)(2i)^{\frac{p-1}{2}} \equiv 1 - (1+i)(1)^{\frac{p-1}{2}} \equiv -i \pmod{\pi}. \end{aligned}$$

Hence, $\chi_\pi(\lambda) = -i$.

A similar calculation leads to

$$\chi_{\overline{\pi}}(\lambda) = \begin{cases} -i & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

It follows that

$$\chi_{\lambda}(5) = \begin{cases} -1 & \text{if } p \equiv 1 \pmod 4, \\ i & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

from which we obtain

$$\begin{aligned} 5^{\frac{GM_p-1}{4}} &\equiv -1 \pmod{GM_p} \quad \text{for} \quad p \equiv 1 \pmod 4, \\ 5^{\frac{GM_p-1}{2}} &\equiv -1 \pmod{GM_p} \quad \text{for} \quad p \equiv 3 \pmod 4. \end{aligned}$$

Conversely, letting q be any prime divisor of GM_p, from (1.2) we have that $GM_p = 2^{m+1}k + 1$, where $k = 2^m - \left(\frac{2}{p}\right)$ is odd and $m+1 = \frac{p+1}{2}$. Then 5^k has order 2^m modulo q if $p \equiv 1 \pmod 4$ and has order 2^{m+1} modulo q if $p \equiv 3 \pmod 4$. In any case $q \equiv 1 \pmod{2^m}$. Since we also know that $q \equiv 1 \pmod p$, it follows that $q \geq 2^m p + 1 > \sqrt{GM_p}$.

Therefore, every prime divisor of GM_p is greater than $\sqrt{GM_p}$, which implies that GM_p is prime. □

Using 3 instead of 5, a similar calculation leads to the following result:

Theorem 2.3. *If $p > 3$, then GM_p is prime if, and only if,*

$$\begin{aligned} 3^{\frac{GM_p-1}{4}} &\equiv -1 \pmod{GM_p} \quad \textit{for} \quad p \equiv 1, 3 \pmod 8, \\ 3^{\frac{GM_p-1}{2}} &\equiv -1 \pmod{GM_p} \quad \textit{for} \quad p \equiv 5, 7 \pmod 8. \end{aligned}$$

Remarks. (1) With the proof of Theorem 2.2 we also end the proof of our main result on Gaussian Mersenne norms, Theorem 1.4. Both Theorems 2.2 and 2.3 give a deterministic primality test for Gaussian Mersenne norms as efficient as the Lucas-Lehmer Test for Mersenne numbers. In fact, the implementation of the test requires the computation of $p-2$ or $p-1$ squares modulo GM_p and only 1 modular multiplication of different numbers which in half of the cases will be a multiplication by either 3 or 5. This fact, together with the other properties of the GM_p's obtained from Theorem 1.4, and together with the fact that $|M_p - GM_p| = O(\sqrt{M_p})$, which makes it reasonable to believe that the distribution of primes in each family is equivalent, indicates that a GIMPS like project for the Gaussian Mersenne primes would produce similar kinds of results with a similar amount of computing power.

(2) The biquadratic character of 5 or 3 modulo GM_p was actually obtained by Emma Lehmer in 1958 in [L]. Theorems 2.2 and 2.3 can be derived from her theorem on quartic residuacity, which depends on knowing the factorization of GM_p as a sum of squares (given by (1.3) in Proposition 1.3). Lehmer's result on cubic and quartic residuacity can be respectively derived from the cubic and the biquadratic reciprocity laws, which motivates our presentation of Theorem 2.2.

(3) A primality test for numbers of the form $A2^s \pm 1$, where $A < 2^s$, based on the biquadratic reciprocity law, was first given in [BB] and works for all $A \not\equiv 0 \pmod 5$. We note that such a test would not apply to GM_p for $p \equiv 1 \pmod 4$, since in that case $GM_p = A2^{\frac{p-1}{2}} + 1$ and $A \equiv 0 \pmod 5$ (see (1.4) in Proposition 1.3).

(4) Note that in the proof of Theorem 2.2 we showed that $\chi_\pi(-gm_p) = -i$ for all odd values of p. The biquadratic reciprocity law implies that $-i = \chi_{gm_p}(\pi) \equiv (\pi)^{\frac{GM_p-1}{4}} \pmod{gm_p}$ (the congruence takes place in the ring of Gaussian integers). Hence it is not difficult to deduce that GM_p is prime if, and only if, $(\pi)^{\frac{GM_p-1}{4}} \equiv -i \pmod{gm_p}$. Since the absolute value of gm_p is $O(\sqrt{GM_p})$, the implementation of this test as an alternative to Theorem 2.2 or Theorem 2.3 may be worth considering.

3. Eisenstein Mersenne norms

The objective of this section is to present a theorem, analogous to Theorem 1.4, that applies to Eisenstein Mersenne norms, which arise naturally when searching for prime elements of the form $a^n - 1$ in the ring $R = \mathbb{Z}[\omega]$, where ω is a cube root of 1.

The ring R, known as the ring of Eisenstein integers, has properties which are either the same or analogous to properties of the ring of Gaussian integers $\mathbb{Z}[i]$. For instance, they are both Euclidean domains, hence unique factorization domains. In both rings it is true that nonreal elements are irreducible if, and only if, their norms are rational primes. Hence Eisenstein Mersenne numbers and Eisenstein Mersenne norms will be defined in a way which is completely analogous to the definitions of Gaussian Mersenne numbers and Gaussian Mersenne norms we gave in section 1. The ring of Eisenstein integers is the natural domain for the cubic reciprocity law, the ring of Gaussian integers, the natural domain for the biquadratic reciprocity law.

The biquadratic reciprocity law has been used to produce a primality test for numbers of the form $A2^s \pm 1$, where $A < 2^s$ (in particular for the GM_p's in the previous section, when p is prime). In this section the cubic reciprocity law will be used to produce a primality test for the EM_p's, which we will soon see are of the form $A3^s + 1$, where $A < 3^s$. A primality test for numbers of that form was first studied by Edouard Lucas in the nineteenth century by using properties of what are now called Lucas sequences. These methods were studied and extended by H. C. Williams in the 1970s. A complete account of the history and the results may be found in [W]. In the 1990s, Guthmann [G], and later the authors of [BB1], used the cubic reciprocity law to produce a primality test for such numbers. We will see that the cubic character of 2 modulo EM_p suffices to produce a primality test for the EM_p's. Additionally we will see that the EM_p's have properties **EMP1** and **EMP2**, which simplify the search for primes in the family. However, they do not share a property analogous to **GMP4**, mainly because binary numbers are natural to computers and they cannot handle base 3 numbers as efficiently.

Since the results and techniques used in the proof are analogous to those used in the previous two sections, we will limit ourselves to state without proof (or with a very sketchy one) most of the results of this section.

Definition 3.1. For a positive integer n, the n-th Eisenstein Mersenne norm EM_n is defined by

$$EM_n = N\left((1-\omega)^n - 1\right),$$

where $N(\alpha) = \alpha\bar{\alpha}$ is the norm of α in $\mathbb{Z}[\omega]$.

$((1-\omega)^n - 1)$ is denoted by em_n. It is an Eisenstein Mersenne number, as well as $\overline{em_n}$.

Examples:

$$EM_2 = \mathbf{N}\left((1-\omega)^2 - 1\right) = \mathbf{N}\left(-1-3\omega\right) = 7,$$
$$EM_3 = \mathbf{N}\left((1-\omega)^3 - 1\right) = \mathbf{N}\left(-4-6\omega\right) = 28.$$

In http://www.research.att.com/~njas/sequences/A066408, Mike Oakes has kept an updated list of the known prime Eisenstein Mersenne norms. There are currently 25. In a related e-mail in the internet he shows that if EM_n is prime, then n is prime (**EMP1**). He mentions that the list of the first 12 was known to the "Cunningham Project" (http://homes.cerias.purdue.edu/~ssw/cun/).

The main result of this section will be the following:

Theorem 3.2. **EMP1:** *If EM_p is prime, then p is prime.*

EMP2: *Let $p > 3$ be a prime. If q divides EM_p, then $q \equiv 1 \pmod{6p}$.*

EMP3: *Let $p > 3$ be a prime. EM_p is prime if, and only if, $2^{\frac{EM_p - 1}{3}} + 2^{2\frac{EM_p-1}{3}} + 1 \equiv 0 \pmod{EM_p}$.*

Before proving the theorem we state some basic properties of Eisenstein Mersenne numbers and norms that we need to prove the theorem. The proposition is elementary, and we state it without proof.

Proposition 3.3. *If $p > 3$ is odd, then*

$$EM_p = \begin{cases} 3^p - 3^{\frac{p+1}{2}} + 1 & \textit{if} \quad p \equiv \pm 1 \pmod{12}, \\ 3^p + 1 & \textit{if} \quad p \equiv \pm 3 \pmod{12}, \\ 3^p + 3^{\frac{p+1}{2}} + 1 & \textit{if} \quad p \equiv \pm 5 \pmod{12}, \end{cases}$$

$$em_p = (1-\omega)^p - 1 = (1-\omega)(-3\omega)^{\frac{p-1}{2}} - 1,$$

$$EM_p = 3^{\frac{p+1}{2}}\left(3^{\frac{p-1}{2}} - \left(\frac{3}{p}\right)\right) + 1, \tag{3.1}$$

$$4EM_p = \left(3^{\frac{p+1}{2}} - \left(\frac{3}{p}\right)2\right)^2 + 27\left(3^{\frac{p-3}{2}}\right)^2 \tag{3.2}$$

where $\left(\frac{a}{p}\right)$ is the Jacobi symbol

$$(3^p + 3^{\frac{p+1}{2}} + 1)(3^p - 3^{\frac{p+1}{2}} + 1)(3^p + 1) \quad = \quad 3^{3p} + 1. \tag{3.3}$$

If p is even, then:

- *If $p \equiv 0 \pmod 3$, then $EM_p = ((-1)^{\frac{p}{2}+1}3^{\frac{n}{2}} + 1)^2$.*
- *If $p \not\equiv 0 \pmod 3$, then $EM_p = 3^p + (-3)^{\frac{p}{2}} + 1$.*

Proof of Theorem 3.2. (1) **EMP1**. If d divides n, then em_d divides em_n; hence EM_d divides EM_n. To show that EM_d is a nontrivial divisor when $d > 1$ it is enough to show that the absolute value of em_d is > 1. But $|em_d| = |(1-\omega)^d - 1| \geq \sqrt{3}^d - 1 > 1$ when $d > 1$.

(2) **EMP2**. This can be proved from (3.3) in Proposition 3.3 in a way which is analogous to the proof of **GMP2** for Gaussian Mersenne norms. Details are left to the reader.

(3) **EMP3**. Assume EM_p is prime. Proposition 9.6.2, page 118 in [IR], states that 2 is a cube modulo EM_p iff 2 divides A and B, where A^2 and B^2 are the unique integers such that $4EM_p = A^2 + 27B^2$. This result was in fact known to Jacobi. In any case, (3.2) in Proposition 3.3 shows that A and B are odd, so 2 is not a cube modulo EM_p; hence $2^{\frac{EM_p-1}{3}}$ has order 3 modulo EM_p, from which $2^{\frac{EM_p-1}{3}} + 2^{2\frac{EM_p-1}{3}} + 1 \equiv 0 \pmod{EM_p}$.

The converse is obtained from a standard argument originally due to Pocklington (see for instance [W]). Indeed, let $x = 2^{\frac{EM_p-1}{3}}$; from the elementary identity $\gcd(\frac{x^d-1}{x-1}, x-1) = \gcd(d, x-1)$, valid for every pair of integers x and $d > 1$, and from the fact that $EM_p \equiv 1 \pmod 3$, we can easily deduce from the hypothesis that $\gcd(2^{\frac{EM_p-1}{3}} - 1, EM_p) = 1$. Also, (3.1) in Proposition 3.3 shows that $EM_p = A3^{\frac{p+1}{2}} + 1$, where $A < 3^{\frac{p+1}{2}}$. The hypotheses of Pocklington's Theorem are satisfied, and the conclusion is that EM_p is prime. □

We end with a result which slightly improves on **GMP3** and **EMP3**.

Theorem 3.4. *Let $p > 3$ be a prime.*

(1) *GM_p is prime if, and only if,*

$$5^{\frac{GM_p-1}{4}} \quad \equiv \quad \begin{cases} -1 \pmod{GM_p} & \textit{if} \quad p \equiv 1 \pmod 4, \\ 2^p \pmod{GM_p} & \textit{if} \quad p \equiv -1 \pmod 4. \end{cases}$$

(2) *EM_p is prime if, and only if, $2^{\frac{EM_p-1}{3}} \equiv 3^p - 1 (\mathrm{mod}\ EM_p)$.*

Proof. (1) $5^{\frac{GM_p-1}{4}} \equiv -1 (\mathrm{mod}\ GM_p)$ when $p \equiv 1 (\mathrm{mod}\ 4)$ is as in the statement of Theorem 2.2. Also, in the proof of that theorem we showed that if $p \equiv -1$ (mod 4) and GM_p is prime, then $\lambda = 1 - (1+i)^p$ is a primary prime satisfying $\chi_\lambda(5) = i$, where χ_λ is the biquadratic character modulo λ.

We next show that $2^p \equiv i (\mathrm{mod}\ \lambda)$: Note first that $(1+i)^p \equiv 1 (\mathrm{mod}\ \lambda)$, which is immediate from the definition of λ. Hence, $2^p = (1+i)^p(1-i)^p = (1+i)^{2p}(-i)^p \equiv (-i)^p \equiv i (\mathrm{mod}\ \lambda)$ (for the last congruence we used that $p \equiv -1 (\mathrm{mod}\ 4)$).

We deduce that $i = \chi_\lambda(5) \equiv 5^{\frac{GM_p-1}{4}} \equiv 2^p (\mathrm{mod}\ \lambda)$; hence $5^{\frac{GM_p-1}{4}} \equiv 2^p$ (mod $\lambda \cap \mathbb{Z} = GM_p$), as desired.

For the converse, if the last congruence holds, then $5^{\frac{GM_p-1}{4}} \equiv 2^p \equiv i$ (mod λ) from which $5^{\frac{GM_p-1}{2}} \equiv -1 (\mathrm{mod}\ \lambda \cap \mathbb{Z} = GM_p)$. The primality of GM_p now follows from Theorem 2.2.

(2) Let $\delta = -(em_p) = 1 - (1-\omega)^p$. Then $N(\delta) = EM_p$. Let χ_δ denote the cubic character modulo δ and let χ_2 denote the cubic character modulo 2 (see [IR], page 113). We will show the following:

i) $\chi_2(\delta) = \omega^p$,

ii) $\omega^p \equiv 3^{2p} \equiv 3^p - 1 (\mathrm{mod}\ \delta)$.

The result will then be deduced by combining the cubic reciprocity law and Theorem 3.2 with i) and ii).

i) By definition of the cubic character, $\chi_2(\delta) \equiv (\delta)^{\frac{2^2-1}{3}} \equiv \delta \,(\text{mod } 2) \equiv (1+\omega)^p + 1 \equiv (-\omega^2)^p + 1 \equiv \omega^{-p} + 1 \equiv \omega^p \,(\text{mod } 2)$, from which i) follows.

ii) Note that by definition of δ we have $(1-\omega)^p \equiv 1 \,(\text{mod } \delta)$. Then $3^{2p} = (1-\omega)^{2p}(1-\omega^{-1})^2p = (1-\omega)^{4p}(\omega^{-1})^{2p} \equiv \omega^p \,(\text{mod } \delta)$. From (3.3) we deduce $3^{2p} \equiv 3^p - 1 \,(\text{mod } EM_p)$, hence modulo δ.

Assume now that EM_p is prime. Then δ is a primary prime in the ring R of Eisenstein integers, and so is 2. The Cubic Reciprocity Law ([IR], page 114) states for this case that $\chi_2(\delta) = \chi_\delta(2)$. It follows, by using i), ii) and the definition of χ_δ that $2^{\frac{EM_p-1}{3}} \equiv 3^p - 1 \,(\text{mod } \delta)$, so the congruence holds modulo $\delta \cap \mathbb{Z} = EM_p$, as desired. For the converse it is not difficult to see that if $2^{\frac{EM_p-1}{3}} \equiv 3^p - 1 \,(\text{mod } EM_p)$, then $2^{\frac{EM_p-1}{3}} + 2^{2\frac{EM_p-1}{3}} + 1 \equiv 0$ $(\text{mod } EM_p)$, so the primality of EM_p follows by Theorem 3.2.

Remarks. (1) The technique used in the proof of (2) in Theorem 3.4 could have been used to prove **EMP3**. In fact, if EM_p is prime, then the Cubic Reciprocity Law and the fact shown above $\chi_\delta(2) \neq 1$ lead easily to $2^{\frac{EM_p-1}{3}} + 2^{2\frac{EM_p-1}{3}} + 1 \equiv 0 \;(\text{mod } EM_p)$. The converse is as in the proof of Theorem 3.2. Moreover, it can be verified that $\chi_\delta(7)$ is also nontrivial when EM_p is prime. It follows that 2 can be replaced by 7 in the statement of **EMP3**.

(2) Theorem 3.4 should be used instead of **EMP3** and **GMP3** when implementing the search for large primes, even though its use will just save up to one modular multiplication in the determination of the primality of GM_p or EM_p for any given p. However, we must say that the implementation we made of the test in 2004 did not include this result, since we found the result after the search was over. We also note that $3^p - 1 \,(\text{mod } EM_p) = 3^p - 1$ when $p \equiv \pm 5 \,(\text{mod } 12)$; in contrast, $3^p - 1 \,(\text{mod } EM_p) = 3^{\frac{p+1}{2}} - 2$ when $p \equiv \pm 1 \,(\text{mod } 12)$. This too should be noted for the implementation of the search based on Theorem 3.4. An analogous observation should be made for the search of primes GM_p.

(3) For primes $q \equiv 1 \,(\text{mod } 3)$ and integers d which are not cubes modulo q, Kenneth S. Williams [WK] appears to be the first to study how to choose $\epsilon = \pm 1$ such that $d^{\frac{q-1}{3}} \equiv \frac{L+\epsilon 9M}{L-\epsilon 9M} \,(\text{mod } q)$, where $L^2 + 27M^2 = 4q$. In our case $q = EM_p$ and the corresponding values of L and M are given in (3.2). Surely, Theorem 3.4 could have been derived from K. S. Williams' results. However, the authors of this paper have been aware for many years that the main results in [WK], together with the main result in [L] concerning cubic residuacity, are equivalent to the Cubic Reciprocity Law, and that there is an analogous equivalence of the Biquadratic Reciprocity Law with results in biquadratic residuacity. This awareness, together with the fact that 2^p has order 4 modulo GM_p and 3^{2p} has order 3 modulo EM_p made possible the simple proof presented here, easily derived from the classical Cubic and Biquadratic Reciprocity Laws.

(4) As was mentioned earlier, there are currently 25 known Eisenstein Mersenne norms that are prime. The largest of these primes was obtained in November 2005 with an implementation of an algorithm that searches for primes in this family based on the results of this paper. The prime is EM_{534827}. The second author of this paper implemented the search for primes in both families, the Gaussian Mersenne norms and the Eisenstein

Mersenne norms. Also in November 2005 the algorithm determined the primality of GM_{991961}. At the moment this was also the largest prime known in that family. The algorithm was used to verify that EM_n was composite for all $255361 < n < 534827$. Hence the 25 known Eisenstein Mersenne norms that are prime are in fact the smallest 25 primes in that family. The same was done for the Gaussian Mersenne family: GM_{991961} was the 36th known prime in that family and these were the smallest 36 primes in the family.

The search was made by using the free CPU time of 6 PC's assigned to different professors of the Mathematics Department at University Simon Bolivar (USB). Additionally, a couple of PC's assigned to our research group (GID-24) by the Decanato de Investigaciones of the USB were devoted almost entirely to the search. The search took around a year and was stopped in December 2005. In December 2006, Jaworsky determined that $GM_{1203793}$ is prime (see [C]). There are now 37 Gaussian Mersenne norms that are known to be prime. □

Acknowledgment

We are grateful to the "Departamento de Matemáticas de la Universidad Simón Bolívar" and to the "Decanato de Investigaciones y Desarrollo de la Universidad Simón Bolívar" for their collaboration and support on this project. We also are grateful to Tom Berry for his valuable comments and suggestions that helped to improve the overall quality of the paper.

References

[B] P. Berrizbeitia. *Deterministic proofs of primality.* (Spanish) Gac. R. Soc. Mat. Esp. 4 (2001), no. 2, 447–456. MR1852299 (2002g:11010)

[BB1] P. Berrizbeitia and T. G. Berry, *Cubic Reciprocity and generalized Lucas-Lehmer Test for Primality of* $A3^n \pm 1$, Proc. Amer. Math. Soc. 26 (1999), 1926–1925. MR1487359 (99j:11006)

[BB] P. Berrizbeitia and T. G. Berry, *Biquadratic reciprocity and a Lucasian primality test.* Math. Comp. 73 (2004), no. 247, 1559–1564. MR2047101 (2004m:11005)

[BLS] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, *New Primality criteria and factorization of* $2^m \pm 1$, Math. Comp. 29 (1975), 620–647. MR0384673 (52:5546)

[BLSTW] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr. *Factorization of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 12$ *up to high powers*, Amer. Math. Soc., Providence, RI, ISBN 0-8218-5078-4. MR715603 (84k:10005)

[C] C. Caldwell, *The Prime Glossary,* http://primes.utm.edu/glossary/

[CP] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer-Verlag, New York (2001), ISBN 0-387-94777-9. MR1821158 (2002a:11007)

[G] A. Guthmann, *Effective primality tests for integers of the forms* $N = k \cdot 3^n + 1$ *and* $N = k \cdot 2^m 3^n + 1$. BIT 32 (1992), no. 3, 529–534. MR1179238 (93h:11008)

[HS] M. Hausmann and H. Shapiro, *Perfect Ideals over the Gaussian Integers,* Comm. Pure Appl. Math., 29, 3 (1976), 323–341. MR0424745 (54:12704)

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory,* Springer-Verlag, Berlin (1982). MR661047 (83g:12001)

[L] E. Lehmer, *Criteria for cubic and quartic residuacity,* Mathematika, 5 (1958), 20–29. MR0095162 (20:1668)

[McD] W. McDaniel, *Perfect Gaussian integers,* Acta. Arith., 25 (1973/74) 137–144. MR0332708 (48:11034)

[R] P. Ribenboim, *The little book of big primes.* Springer-Verlag, New York, 1991. viii+237 pp. ISBN: 0-387-97508-X MR1118843 (92i:11008)

[S] R. Spira, *The complex sum of divisors,* Amer. Math. Monthly, 68 (1961) 120–124. MR0148594 (26:6101)

[W] H. C. Williams, *Édouard Lucas and primality testing.* Canadian Mathematical Society Series of Monographs and Advanced Texts, 22. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998. x+525 pp. ISBN: 0-471-14852-0 MR1632793 (2000b:11139)

[WK] K. S. Williams, *On Euler's Criteria for Cubic Nonresidues,* Proc. Amer. Math. Soc. 49, 2 (1975), 277–283. MR0366792 (51:3038)

Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Caracas, Venezuela
E-mail address: pedrob@usb.ve

Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Caracas, Venezuela
E-mail address: iskra@usb.ve