MERSENNE PRIMES

SARAH MEIKLEJOHN AND STEVEN J. MILLER

ABSTRACT. A Mersenne prime is a prime that can be written as $2^p - 1$ for some prime p. The first few Mersenne primes are 3, 7 and 31 (corresponding respectively to $p = 2$, 3 and 5). We give some standard conditions on p which ensure that $2^p - 1$ is prime, and discuss an application to even perfect numbers. The proof requires us to study the field $\mathbb{Z}/q\mathbb{Z}[\sqrt{3}]$, where $q \neq 3$ is a prime.

1. INTRODUCTION

If $n \geq 2$ and $a^n - 1$ is prime, we call $a^n - 1$ a Mersenne prime. For which integers a can $a^n - 1$ be prime? We take $n \geq 2$ as if $n = 1$ then a is just one more than a prime.

We know, using the geometric series, that

$$a^n - 1 \;=\; (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1). \tag{1}$$

So, $a-1 \mid a^n-1$ and therefore a^n-1 will be composite unless $a-1 = 1$, or equivalently unless $a = 2$. Thus it suffices to investigate numbers of the form $2^n - 1$.

Further, we need only examine the case of n prime. For assume n is composite, say $n = mk$. Then $2^n = 2^{mk} = (2^m)^k$, and

$$2^n - 1 \;=\; (2^m)^k - 1 \;=\; (2^m - 1)((2^m)^{k-1} + (2^m)^{k-2} + \cdots + (2^m)^2 + 2^m + 1). \tag{2}$$

So if $n = mk$, $2^n - 1$ always has a factor $2^m - 1$, and therefore is prime only when $2^m - 1 = 1$. This immediately reduces to $2^m = 2$, or simply $m = 1$. Thus, if n is composite, $2^n - 1$ is composite.

Now we know we are only interested in numbers of the form $2^p - 1$; if this number is prime then we call it a Mersenne prime. As it turns out, not every number of the form $2^p - 1$ is prime. For example, $2^{11} - 1 = 2047$, which is $23 \cdot 89$.

2. STATEMENT OF THE LUCAS-LEHMER TEST

How do we determine which p yield $M_p = 2^p - 1$ prime? An answer is the Lucas-Lehmer test, which states that M_p is prime if and only if $M_p \mid s_{p-2}$, where we recursively define

$$s_i = \begin{cases} 4 & \text{if } i = 0, \\ s_{i-1}^2 - 2 & \text{if } i \neq 0. \end{cases} \tag{3}$$

We prove one direction of this statement, namely that if $M_p \mid s_{p-2}$, then M_p is prime. We start by defining $u = 2 - \sqrt{3}$ and $v = 2 + \sqrt{3}$. Some immediate properties are

- $u + v = 4 = s_0$;
- $uv = 1$, implying that $(uv)^x = u^x v^x = 1$ (so uv to any power equals one).

Date: December 4, 2005.

We will show that $s_n = u^{t(n)} + v^{t(n)}$, where we have defined $t(s) = 2^s$. We shall see later that this is a useful way to write s_n. Two properties of $t(s)$ that we need are

- $t(0) = 1$;
- $t(s+1) = 2^{s+1} = 2t(s)$.

We prove by induction that $s_n = u^{t(n)} + v^{t(n)}$.

Base Case: Clearly the base case is true, as we have already seen that $s_0 = u^1 + v^1 = 4$.

Inductive Case: Assuming $s_n = u^{t(n)} + v^{t(n)}$, we must show $s_{n+1} = u^{t(n+1)} + v^{t(n+1)} = s_n^2 - 2$. To do this, we look at

$$\begin{aligned} s_{n+1} &= s_n^2 - 2 \\ &= (u^{t(n)} + v^{t(n)})^2 - 2 \\ &= u^{2t(n)} + v^{2t(n)} + 2u^{t(n)}v^{t(n)} - 2. \end{aligned} \tag{4}$$

But we already know that $u^{t(n)}v^{t(n)} = (uv)^{t(n)} = 1$ and $2t(n) = t(n+1)$, so we have

$$\begin{aligned} s_{n+1} &= u^{t(n+1)} + v^{t(n+1)} + 2 - 2 \\ &= u^{t(n+1)} + v^{t(n+1)}, \end{aligned} \tag{5}$$

which shows that $s_{n+1} = u^{t(n+1)} + v^{t(n+1)}$.

3. Proof of the Lucas-Lehmer Test

We prove one direction of the Lucas-Lehmer test. Specifically, we prove by contradiction that if $M_p | s_{p-2}$ then M_p is prime.

3.1. **Preliminaries.**

We assume that s_{p-2} is divisible by M_p, but that M_p is *not* prime. By direct calculation we may assume that $p > 5$. There is therefore an integer $R > 1$ such that

$$s_{p-2} \;=\; u^{t(p-2)} + v^{t(p-2)} \;=\; RM_p. \tag{6}$$

If we multiply both sides by $u^{t(p-2)}$, we obtain

$$u^{t(p-2)} \cdot (u^{t(p-2)} + v^{t(p-2)}) \;=\; u^{t(p-1)} + 1 \;=\; RM_p \cdot u^{t(p-2)}. \tag{7}$$

Subtracting one from each side gives

$$u^{t(p-1)} \;=\; RM_p \cdot u^{t(p-2)} - 1. \tag{8}$$

We square both sides. As $(u^{t(p-1)})^2 = u^{t(p)}$, we obtain that

$$u^{t(p)} \;=\; (RM_p \cdot u^{t(p-2)} - 1)^2. \tag{9}$$

Note $u^{t(p)}$ is not necessarily an integer.

Let us choose some prime factor $q > 1$ of M_p such that $q \le \sqrt{M_p}$, or equivalently so that $q^2 \le M_p$. Does such a q exist? There is no problem with assuming $q > 1$, but what about $q \le \sqrt{M_p}$? If $M_p = bc$ then either b or c is at most $\sqrt{M_p}$, for if both were larger then the product would exceed M_p. Note we are not claiming that $q < \sqrt{M_p}$, just that $q \le \sqrt{M_p}$.

We use below the fact that $q \neq 3$; we need $q \neq 3$ so that 3 will have a multiplicative inverse in $\mathbb{Z}/q\mathbb{Z}$. We are assuming $p > 5$ (as the other cases can be handled by direct

computation). Thus we may write p as $4n + a$, where n is an integer and $a \in \{1, 3\}$. Thus

$$\begin{aligned} M_p &= 2^p - 1 \\ &= 2^{4n+a} - 1 \\ &= 2^{4n} \cdot 2^a - 1 \\ &= (2^4)^n \cdot 2^a - 1 \\ &\equiv 2^a - 1 \bmod 3, \end{aligned} \tag{10}$$

since $2^4 = 16 \equiv 1 \bmod 3$. If $a = 1$ then $2^{4n+a} - 1 \equiv 1 \bmod 3$, while if $a = 3$ then $2^{4n+a} - 1 \equiv 1 \bmod 3$. Thus 3 does not divide M_p, and we may assume that $q \neq 3$ below.

The proof is completed by analyzing the order of $u^{t(p)}$ in the field $\mathbb{Z}/q\mathbb{Z}[\sqrt{3}]$, where q is a prime dividing M_p. There are two different cases, depending on whether or not 3 is a square modulo q. Note that if 3 is a square modulo q, then this field is actually just $\mathbb{Z}/q\mathbb{Z}$.

3.2. 3 **is not a square modulo** q**.** We finish the proof in the case that 3 is not a square modulo q. This means that $t^2 - 3$ does not have a root in $\mathbb{Z}/q\mathbb{Z}$, or equivalently that $t^2 - 3$ is irreducible in $\mathbb{Z}/q\mathbb{Z}$.

Proof. Consider the ring $\mathbb{Z}/q\mathbb{Z}[\sqrt{3}] = \left\{a + b\sqrt{3} : \ a, b \in \mathbb{Z}/q\mathbb{Z}\right\}$; note there are q^2 elements, and $q^2 - 1$ non-zero elements. As $q \neq 3$ is prime, $\mathbb{Z}/q\mathbb{Z}$ is a field. Further, $\mathbb{Z}/q\mathbb{Z}[\sqrt{3}]$ is a field as $\sqrt{3}$ is invertible in $\mathbb{Z}/q\mathbb{Z}[\sqrt{3}]$; the inverse is $b\sqrt{3}$, where $b \in \mathbb{Z}/q\mathbb{Z}$ is such that $3b \equiv 1 \bmod q$. More generally, let $p(t) = t^2 - 3 \in \mathbb{Z}/q\mathbb{Z}[t]$ be the irreducible monic polynomial for $\sqrt{3}$ over $\mathbb{Z}/q\mathbb{Z}$. Given any $a + b\sqrt{3} \in \mathbb{Z}/q\mathbb{Z}[\sqrt{3}]$ with a and b not both zero, consider the linear polynomial $g(t) = a + bt$. Then $p(t)$ and $g(t)$ are relatively prime (since $p(t)$ is monic and irreducible). Thus there are polynomials such that $h_1(t)g(t) + h_2(t)p(t) = 1$; letting $t = \sqrt{3}$ yields $h_1(\sqrt{3})g(\sqrt{3}) = 1$, so we have found an inverse to $g(\sqrt{3}) = a + b\sqrt{3}$, proving $\mathbb{Z}/q\mathbb{Z}[\sqrt{3}]$ is a field.

We may study the subset of elements with multiplicative inverses, $\left(\mathbb{Z}/q\mathbb{Z}[\sqrt{3}]\right)^*$. The order of this multiplicative group is $q^2 - 1$; thus by Lagrange's theorem every element $x \in \mathbb{Z}/q\mathbb{Z}[\sqrt{3}]$ satisfies $x^{q^2-1} = 1$; note that here by equals 1 we mean with respect to the multiplication operation of $\mathbb{Z}/q\mathbb{Z}[\sqrt{3}]$ (which includes multiplication modulo q and $\sqrt{3} \cdot \sqrt{3} = 3$).

From (7), we see that

$$u^{t(p-1)} \ \equiv \ RM_p \cdot u^{t(p-2)} - 1 \bmod q. \tag{11}$$

As $q|M_p$, $M_p \equiv 0 \bmod q$. Therefore

$$u^{t(p-1)} \ \equiv \ -1 \bmod q. \tag{12}$$

Similarly, looking at (9), we see that

$$u^{t(p)} \ \equiv \ (RM_p \cdot u^{t(p-2)} - 1)^2 \bmod q, \tag{13}$$

which implies that

$$u^{t(p)} \ \equiv \ (0 - 1)^2 \ \equiv \ 1 \bmod q. \tag{14}$$

The order of an element g in our multiplicative group $\left(\mathbb{Z}/q\mathbb{Z}[\sqrt{3}]\right)^*$ is the smallest positive k such that $g^k = 1$; we often denote this by $\mathrm{ord}(g)$. By Lagrange's theorem, $k|q^2-1$. Further, by (14) we know that $\mathrm{ord}(u) \mid t(p)$.

We now show that $\mathrm{ord}(u)$ is exactly $t(p)$. From (14) we see that $\mathrm{ord}(u)|t(p)$. As $t(s) = 2^s$, if $\mathrm{ord}(u) \neq t(p)$ then $\mathrm{ord}(u)|t(p-1)$. But if $\mathrm{ord}(u)$ divided $t(p-1)$ then

$$u^{t(p-1)} \equiv 1 \bmod q, \tag{15}$$

which contradicts (12). Thus $\mathrm{ord}(u) = t(p) = 2^p$.

However, since the order of any element is at most the order of the group, we have

$$\mathrm{ord}(u) = 2^p \leq q^2 - 1 < M_p = 2^p - 1, \tag{16}$$

where the second inequality follows from $q^2 \leq M_p$. We thus obtain the contradiction

$$2^p < 2^p - 1, \tag{17}$$

which proves that M_p is prime. □

3.3. 3 **is a square modulo** q**.** We finish the proof in the case that 3 is a square modulo q. This means that t^2-3 has a root in $\mathbb{Z}/q\mathbb{Z}$, or equivalently that t^2-3 factors into two linear terms in $\mathbb{Z}/q\mathbb{Z}$. For example, if $q = 13$ then $t^2 - 3 \equiv (t-4)(t-9) \bmod q$.

Proof. We now assume that 3 is a square modulo q; for definiteness, let $b^2 = 3$. In §3.1 we showed that

$$u^{t(p-1)} = RM_p \cdot u^{t(p-2)} - 1 \tag{18}$$

and

$$u^{t(p)} = (RM_p \cdot u^{t(p-2)} - 1)^2. \tag{19}$$

Note $u^{t(n)}$ is not necessarily an integer. We may regard these equations modulo q. Doing so, we replace $\sqrt{3}$ with b. Reducing these equations modulo q yield

$$u^{t(p-1)} \equiv -1 \bmod q \tag{20}$$

and

$$u^{t(p)} \equiv 1 \bmod q. \tag{21}$$

Arguing as in §3.2, $\mathrm{ord}(u) = 2^p$; the only difference is that now there are $q-1$ non-zero elements in our field $\mathbb{Z}/q\mathbb{Z}$, and not q^2-1. We therefore have

$$\mathrm{ord}(u) = 2^p \leq q - 1 \leq M_p = 2^p - 1, \tag{22}$$

and this contradiction completes the proof. □

4. Mersenne Primes and Perfect Numbers

Another interesting fact about Mersenne primes is their correspondence with perfect numbers. Perfect numbers are integers whose proper divisors (all divisors except the number itself) sum to the number. For example, $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$. There is a one-to-one correspondence between even perfect numbers and Mersenne primes. While it can be shown that every even perfect number is of the form $(2^p - 1) \cdot 2^{p-1}$, where $2^p - 1$ is a Mersenne prime, we content ourselves with showing that any number of the form $(2^p - 1) \cdot 2^{p-1}$ is perfect when $2^p - 1$ is a Mersenne prime.

Let $q = 2^p - 1$ be a Mersenne prime; we show that $q \cdot 2^{p-1}$ is perfect. We know that the proper divisors break up into two disjoint sets:

$$\{1, 2, 4, \ldots, 2^{p-1}\} \cup \{q, 2q, 4q, \ldots, 2^{p-2}q\}. \tag{23}$$

So, using the geometric formula

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}, \tag{24}$$

we see that the first set sums to

$$1 + 2 + 4 + \cdots + 2^{p-1} = \frac{2^p - 1}{2 - 1} = 2^p - 1 = q, \tag{25}$$

and the second set sums to

$$q+2q+4q+\cdots+2^{p-2}q = q(1+2+4+\cdots+2^{p-2}) = q\left(\frac{2^{p-1}-1}{2-1}\right) = q(2^{p-1}-1). \tag{26}$$

Thus the sum of the proper divisors is

$$q + q(2^{p-1} - 1) = q + 2^{p-1}q - q = 2^{p-1}q, \tag{27}$$

proving that $(2^p - 1) \cdot 2^{p-1}$ is perfect.

E-mail address: sjmiller@math.brown.edu

DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RI 02912