ON TESTING MERSENNE NUMBERS

BRANDON MULIADI

1. Introduction

Definition 1.1. A *Mersenne number* is a number of the form $2^n - 1$, where n is a positive number. We write the n-th Mersenne number as M_n.

Definition 1.2. A *Mersenne prime* is a prime Mersenne number.

For example, the first four Mersenne primes are 3, 7, 31, and 127. These are M_2, M_3, M_5, and M_7. You might notice these are the first four primes. That isn't exactly a coincidence, because if n is composite, then there is a simple factorization of M_n. Suppose $n = ab$, where $a, b > 0$. Then

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

So we will only concern ourselves with the numbers M_p, where p is prime. (Note that p being prime is not enough, since (for example) $2^{11} - 1 = 2047 = 23 \cdot 89$ is composite.)

The top five largest known primes are all Mersenne primes. In fact, the largest known non-Mersenne prime has 11981518 digits - less than half as many as the largest known prime, $2^{82589933} - 1$, which has 24862048 digits. This is because there is a very fast primality test for Mersenne numbers, called the Lucas-Lehmer test.

2. The Lucas-Lehmer Test

Theorem 2.1 (Lucas-Lehmer test)**.** *Let $s_0 = 4$. For $n > 0$, let $s_n = s_{n-1}^2 - 2$. Then M_p is prime if and only if $M_p \mid s_{p-2}$.*

Proof. First, we prove a closed form for s_i. Let $\omega = 2 + \sqrt{3}$ and $\overline{\omega} = 2 - \sqrt{3}$, and note that $\omega\overline{\omega} = 1$. We claim that $s_i = w^{2^i} + w^{2^i}$. First, notice that $\omega^{2^0} + \overline{\omega}^{2^0} = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4 = s_0$ as desired. Next, we check that this claimed form satisfies the recurrence relation for s_i. Indeed,

$$(\omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}})^2 - 2 = \omega^{2^n} + \overline{\omega}^{2^n} + 2(\omega\overline{\omega})^{2^{n-1}} - 2 = \omega^{2^n} + \overline{\omega}^{2^n}$$

as desired.

Next, we prove the "if" direction. This proof is due to [1]. Suppose that $M_p \mid s_{p_2}$. Then we write

$$\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} = kM_p$$

for some integer k. Multiplying both sides by $\omega^{2^{p-2}}$ gives

$$\omega^{2^{p-1}} + 1 = kM_p\omega^{2^{p-2}}$$

or

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1 \tag{2.1}$$

and, squaring,

$$\omega^{2^p} = (kM_p\omega^{2^{p-2}} - 1)^2 \tag{2.2}$$

Now suppose for the sake of contradiction that M_p is composite. Choose a factor $q \leq \sqrt{M_p}$ of M_p, and note that q is odd. Let X denote the set $\{a + b\sqrt{3} : a, b \in \mathbb{Z}/q\mathbb{Z}\}$. Addition and multiplication are defined on X in the obvious way. We can think of $\omega, \overline{\omega}$ as elements of X, since $q > 2$. Clearly X is closed and thus forms a group under either of these operations. Let X^* denote the the group of invertible elements of X with respect to multiplication. Note that X contains at least one non-invertible element, namely 0, so $|X^*| \leq |X| - 1 = q^2 - 1$.

Now, observe that since $q \mid M_p$, $kM_p\omega^{2^{p-2}}$ is 0 as an element of X. Thus equations (2.1) and (2.2) give us that

$$\omega^{2^{p-1}} = -1$$
$$\omega^{2^p} = 1$$

in X. Equation (2.4) implies that ω is invertible with inverse ω^{2^p-1}, so $\omega \in X^*$. Furthermore, the order of ω divides 2^p but not 2^{p-1}, so the order of ω is 2^p. Since the order of ω is at most $|X^*|$,

$$2^p \leq q^2 - 1.$$

But $q^2 \leq 2^p - 1$, so

$$2^p \leq q^2 - 1 \leq 2^p - 2$$

which is absurd. This completes the proof of the "if" direction.

Now we prove the "only if" direction. This proof is due to [2]. Suppose M_p is prime. Set $\tau = \frac{1+\sqrt{3}}{\sqrt{2}}$, and $\overline{\tau} = \frac{1-\sqrt{3}}{\sqrt{2}}$. Note that $\tau^2 = \omega$, $\overline{\tau}^2 = \overline{\omega}$, and $\tau\overline{\tau} = -1$. Now we have

$$\tau^{M_p} 2^{\frac{M_p-1}{2}} \sqrt{2} = (\sqrt{2}\tau)^{M_p} = (1+\sqrt{3})^{M_p} \equiv 1 + \sqrt{3}^{M_p} = 1 + 3^{\frac{M_p-1}{2}}\sqrt{3} \pmod{M_p}.$$

Note that $M_p \equiv 7 \pmod 8$, so $(2/M_p) = 1$, and $M_p \equiv 7 \pmod{12}$, so $(3/M_p) = -1$, by well-known properties of the Legendre symbol. Thus $2^{\frac{M_p-1}{2}} \equiv 1$ and $3^{\frac{M_p-1}{2}} \equiv -1 \pmod{M_p}$. Substituting this in, we see that

$$\tau^{M_p}\sqrt{2} \equiv 1 - \sqrt{3} \pmod{M_p}$$

so $\tau^{M_p} \equiv \overline{\tau} \pmod{M_p}$ and thus $\tau^{M_p+1} \equiv -1 \pmod{M_p}$. We can also write this as $\tau^{2^p} + 1$ $\pmod{M_p}$, or, using the fact that $\tau^2 = \omega$,

$$\omega^{2^{p-1}} + 1 \pmod{M_p}.$$

Multiplying both sides by $\overline{\omega}^{2^{p-2}}$ gives

$$\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}$$

as desired. ■

When implemented correctly, the most expensive part of the Lucas-Lehmer test is performing the $O(p)$ multiplications, which can each be done in $O(p^{1+\varepsilon})$ with the Schönhage–Strassen algorithm. So the time complexity of the Lucas-Lehmer test is $O(p^{2+\varepsilon})$.

3. Jacobi Error Checking

Random hardware issues can lead to computation errors when running a Lucas-Lehmer test. To totally ensure accuracy, Lucas-Lehmer tests need to be double checked, with the final residue compared between both tests to see if it matches. However, there is a way to improve the accuracy of Lucas-Lehmer tests on unreliable hardware.

Theorem 3.1 (Jacobi error check)**.** *Let i be any positive integer and p be an odd prime. Then*

$$\left(\frac{s_i+2}{M_p}\right) = +1 \tag{3.1}$$

$$\left(\frac{s_i-2}{M_p}\right) = -1. \tag{3.2}$$

Proof. Recall that $s_i = s_{i-1}^2 - 2$. So $s_i + 2 = s_{i-1}^2$ must be a square, proving (3.1). Equation (3.3) requires induction. Note that for $i = 0$, $\left(\frac{s_i-2}{M_p}\right) = \left(\frac{2}{M_p}\right) = 1$ since $M_p \equiv 7 \pmod 8$. This is the base case. Now we induct. Suppose $\left(\frac{s_i-2}{M_p}\right) = -1$. Then

$$\left(\frac{s_{i+1}-2}{M_p}\right) = \left(\frac{s_{i-1}^2-4}{M_p}\right) = \left(\frac{(s_i-2)(s_i+2)}{M_p}\right) = \left(\frac{s_i-2}{M_p}\right)\left(\frac{s_i+2}{M_p}\right) = 1(-1) = -1.$$

This completes the inductive step and the proof. ∎

What makes Jacobi error checking useful is that it doesn't need to be performed on every iteration (which would be too expensive) - if a hardware error causes both $\left(\frac{s_i+2}{M_p}\right)$ and $\left(\frac{s_i-2}{M_p}\right)$ to be $+1$, then they will be $+1$ on each future iteration as well. So it's enough to only perform a Jacobi check every several thousand iterations or so.

4. Modern Mersenne Prime Testing

Although the Lucas-Lehmer test is very fast, it is no longer the main test used by the Great Internet Mersenne Prime Search (GIMPS), a distributed computing project searching for Mersenne primes. Instead, GIMPS tests numbers by running a single Fermat probable prime test (PRP), which simply verifies for one a that $a^{M_p-1} \equiv 1 \pmod{M_p}$, as would be guaranteed by Fermat's Little Theorem if M_p were prime. Large numbers are unlikely to be Fermat pseudoprimes, making a false positive unlikely. Now, PRP tests aren't any faster than LL, also having a time complexity of $O(p^{2+\varepsilon})$, but they are preferred because of Gerbicz error checking, a technique for Fermat probable prime tests that nearly guarantees a correct result. Still, Lucas-Lehmer remains necessary for verifying any pseudoprimes found by PRP tests.

References

[1] James W Bruce. “A really trivial proof of the Lucas-Lehmer test”. In: *The American Mathematical Monthly* 100.4 (1993), pp. 370–371.

[2] Michael I Rosen. “A proof of the Lucas-Lehmer test”. In: *The American Mathematical Monthly* 95.9 (1988), pp. 855–856.