1 Mersenne Primes and Perfect Numbers

Basic idea: try to construct primes of the form $a^n - 1; \ a, n \geq 1$. e.g.,
$2^1 - 1 = 3$ but $2^4 - 1 = 3 \cdot 5$
$2^3 - 1 = 7$
$2^5 - 1 = 31$
$2^6 - 1 = 63 = 3^2 \cdot 7$
$2^7 - 1 = 127$
$2^{11} - 1 = 2047 = (2^3)(89)$
$2^{13} - 1 = 8191$

Lemma: $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$

Corollary: $(x - 1)|(x^n - 1)$

So for $a^n - 1$ to be prime, we need $a = 2$.
Moreover, if $n = md$, we can apply the lemma with $x = a^{d}$. Then

$$(a^d - 1)|(a^n - 1)$$

So we get the following

Lemma If $a^n - 1$ is a prime, then $a = 2$ and $n$ is prime.

Definition: A Mersenne prime is a prime of the form

$$q = 2^p - 1, \ p \text{ prime.}$$

Question: are they infinitely many Mersenne primes?

Best known: The 37th Mersenne prime $q$ is associated to $p = 3021377$, and this was done in 1998. One expects that $p = 6972593$ will give the next Mersenne prime; this is close to being proved, but not all the details have been checked.

Definition: A positive integer $n$ is perfect iff it equals the sum of all its (positive) divisors $< n$.

Definition: $\sigma(n) = \sum_{d|n} d$ (divisor function)

So $u$ is perfect if $n = \sigma(u) - n$, i.e. if $\sigma(u) = 2n$.

Well known example: $n = 6 = 1 + 2 + 3$

Properties of $\sigma$:

1. $\sigma(1) = 1$
2. \( n \) is a prime iff \( \sigma(n) = n + 1 \)

3. If \( p \) is a prime, \( \sigma(p^j) = 1 + p + \cdots + p^j = \frac{p^{j+1}-1}{p-1} \)

4. (Exercise) If \( (n_1, n_2) = 1 \) then \( \sigma(n_1)\sigma(n_2) = \sigma(n_1n_2) \) “multiplicativity”.

Consequently, if

\[
 n = \prod_{j=1}^{r} p_j^{e_j}, \quad e_j \geq 1 \quad \forall j, \ p_j \text{ prime},
\]

\[
 \sigma(n) = \prod_{j=1}^{r} \sigma(p_j^{e_j}) = \prod_{j=1}^{r} \left( \frac{p_j^{e_j+1} - 1}{p_j - 1} \right)
\]

Examples of perfect numbers:

\[
\begin{align*}
6 &= 1+2+3 \\
28 &= 1+2+4+7+14 \\
496 &= 64 \cdot 16 \\
8128 &= 256 \cdot 32
\end{align*}
\]

Questions:

1. Are there infinitely many perfect numbers?

2. Is there any odd perfect number?

Note:

\[
6 = (2)(3), \ 28 = (4)(7), \ 496 = (16)(31), \ 8128 = (64)(127)
\]

They all look like

\[
2^{n-1}(2^n - 1),
\]

with \( 2^n - 1 \) prime (i.e., Mersenne).

**Theorem** (Euler) Let \( n \) be a positive, even integer. Then

\[
n \text{ is perfect } \iff n = 2^{p-1}(2^p - 1), \text{ for a prime } p, \text{ with } 2^p - 1 \text{ a prime.}
\]

**Corollary.** There exists a bijection between even perfect numbers and Mersenne primes.

**Proof of Theorem.** \((\iff)\) Start with \( n = 2^{p-1}q \), with \( q = 2^p - 1 \) a Mersenne prime. To show: \( n \) is perfect, i.e., \( \sigma(n) = 2n \). Since \( 2^{p-1}q \), and since \( (2^{p-1}, q) = 1 \), we have

\[
 \sigma(n) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)(q + 1) = q2^p = 2n.
\]
$(\Rightarrow)$: Let $n$ be a even, perfect number. Since $n$ is even, we can write

$$n = 2^j m, \text{ with } j \geq 1, \text{ } m \text{ odd } \neq n$$

$$\Rightarrow \sigma(n) = \sigma(2^j)\sigma(m) = (2^{j+1} - 1)\sigma(m)$$

Since $n$ is perfect,

$$\sigma(n) = 2n = 2^{j+1} m$$

Get

$$2^{j+1}m = \underbrace{(2^{j+1} - 1)\sigma(m)}_{\text{odd}}$$

$$\Rightarrow$$

$$2^{j+1}|\sigma(m)$$;

so

$$r2^{j+1} = \sigma(m)$$ \hspace{1cm} (1)

for some $r \geq 1$

Also

$$2^{j+1}m = (2^{j+1} - 1)r2^{j+1},$$

so

$$m = (2^{j+1} - 1)r$$ \hspace{1cm} (2)

Suppose $r > 1$. Then

$$m = (2^{j+1} - 1)r$$

will have 1, $r$ and $m$ as 3 distinct divisors. (Explanation: by hypothesis, $1 \neq r$. Also, $r = m$ iff $j = 0$ iff $n = m$, which will then be odd!)

Hence

$$\sigma(m) \geq 1 + r + m$$

$$= 1 + r + (2^{j+1} - 1)r$$

$$= 1 + 2^{j+1}r$$

$$= 1 + \sigma(m)$$

Contradiction!
So $r = 1$, and so (1) and (2) become
\[
\sigma(m) = 2^{j+1} \quad (1')
\]
\[
m = 2^{j+1} - 1 \quad (2')
\]
Since $n = 2^j m$, we will be done if we prove that $m$ is a prime. It suffices to show that $\sigma(m) = m + 1$. But this is clear from (1’) and (2’).

$M_n = 2^n - 1$ Mersenne number. Define numbers $S_n$ recursively by setting $S_n = S_{n-1}^2 - 2$, and $S_1 = 4$.

**Theorem:** (Lucas-Lehmer Primality Test) Suppose for some $n \geq 1$ that $M_n$ divides $S_{n-1}$. Then $M_n$ is prime.

**Proof.** (Very clever) Put $\alpha = 2 + \sqrt{3}, \beta = 2 - \sqrt{3}$. Note that $\alpha + \beta = 4, \alpha\beta = 1$. So $S_1 = \alpha + \beta$.

**Lemma.** For any $n \geq 1$, $S_n = \alpha^{2^{n-1}} + \beta^{2^{n-1}}$.

**Proof of Lemma:** $n = 1$: $S_1 = \alpha + \beta = 4$. So let $n > 1$, and assume that the lemma holds for $n - 1$. Since

\[
S_n = S_{n-1}^2 - 2
\]
we get (by induction)
\[
S_n = (\alpha^{2^{n-1}} + \beta^{2^{n-1}})^2 - 2
\]

Note:
\[
(\alpha^k + \beta^k)^2 = \alpha^{2k} + 2\alpha^k\beta^k + \beta^{2k}
= \alpha^{2k} + \beta^{2k} + 2, \text{ as } \alpha\beta = 1.
\]
So we get (setting $k = 2^{n-2}$)
\[
S_n = \alpha^{2^{n-1}} + \beta^{2^{n-1}} + 2 - 2.
\]
Hence the lemma.

**Proof of Theorem** (continued): Suppose $M_n | S_{n-1}$. Then we may write $rM_n = S_{n-1}$, some positive integer. By the lemma, we get
\[
rM_n = \alpha^{2^{n-2}} + \beta^{2^{n-2}} \quad (3)
\]
Multiply (3) by $\alpha^{2n-2}$ and subtract 1 to get:
\[ \alpha^{2n-1} = r M_n \alpha^{2n-2} - 1 \] (4)

Squaring (4) we get
\[ \alpha^{2n} = (r M_n \alpha^{2n-2} - 1)^2 \] (5)

Suppose $M_n$ is not a prime. Then $\exists$ a prime $\ell$ dividing $M_n$, $\ell \leq \sqrt{M_n}$. Let us work in the number system
\[ R = \{ a + b\sqrt{3} | a, b \in \mathbb{Z} \} \]

Check: $R$ is closed under addition, subtraction, and multiplication (it is what one calls a ring). Equations (4) and (5) happen in $R$. Define $R/\ell = \{ a + b\sqrt{3} | a, b \in \mathbb{Z}/\ell \}$.

Note: $|R/\ell| = \ell^2$

We can view $\alpha, \beta$ as elements of $R/\ell$. Since $\ell | M_n$, (4) becomes the following congruence in $R/\ell$:
\[ \alpha^{2n-1} \equiv -1 \pmod{\ell} \] (6)

Similarly, (5) says
\[ a^{2n} \equiv 1 \pmod{\ell} \]

Put
\[ X = \{ \alpha^j \mod \ell | 1 \leq j \leq 2^n \} \]

Claim $|X| = 2^n$.

**Proof of claim.** Suppose not. Then $\exists j, k$ between 1 and $2^n$, with $j \neq k$, such that $\alpha^j \equiv \alpha^k \pmod{\ell}$.

If $r$ denotes $|j - k|$, then $0 < r < 2^n$ and $\alpha^r \equiv 1 \pmod{\ell}$. Let $d$ denote the gcd of $r$ and $2^n$, so that $ar + b2^n = d$ for some $a, b \in \mathbb{Z}$. Then we have
\[ \alpha^d = \alpha^{ar+b2^n} = (\alpha^r)^a \cdot (\alpha^{2n})^b \equiv 1 \pmod{\ell}. \]

But since $d|2^n$, $d$ is of the form $2^m$ for some $m < n$, and $\alpha^d \equiv 1 \pmod{\ell}$ contradicts $\alpha^{2^n-1} \equiv -1 \pmod{\ell}$. Hence the claim.

So $|X| \leq \ell^2 - 1$, i.e., we need $2^n \leq \ell^2 - 1$.

Since
\[ \ell \leq \sqrt{M_n}, \ \ell^2 - 1 < M_n = 2^n - 1. \]
\[ \Rightarrow 2^n < 2^n - 1, \text{ a contradiction!} \]
So $M_n$ is prime.