Math 406 Section 7.3: Perfect Numbers and Mersenne Primes

1. **Introduction:** The definition of the sum of the divisors of a positive integer leads to the concept of a perfect number which is intrinsically connected to a Mersenne prime.

2. **Definition:** A positive integer \( n \in \mathbb{Z}^+ \) is perfect if the sum of the positive divisors equals twice the integer, that is, \( \sigma(n) = 2n \).

   **Example:** The integer \( n = 6 \) is perfect since \( \sigma(6) = 1 + 2 + 3 + 6 = 12 = 2(6) \).

3. **Finding Perfect Numbers:** It’s unknown whether there are infinitely many perfect numbers and it’s unknown whether there are any odd perfect numbers - all perfect numbers which have been found have been even.

   However the following theorem applies to the even ones:

4. **Theorem:** The integer \( n \in \mathbb{Z}^+ \) is an even perfect number iff 
   \[
   n = 2^{m-1}(2^m - 1)
   \]
   for some \( m \in \mathbb{Z} \) with \( m \geq 2 \) and \( 2^m - 1 \) prime.

   What this implies is that finding even perfect numbers boils down to finding such \( m \). In other words if we check \( m = 2, 3, 4, \ldots \) then if \( 2^m - 1 \) is prime then \( n = 2^{m-1}(2^m - 1) \) is perfect.

   **Example:** When \( m = 2 \) we see \( 2^m - 1 = 3 \) is prime and so \( n = 2^{m-1}(2^m - 1) = 6 \) is perfect.

   **Proof:**
   \[
   \begin{align*}
   \sigma(n) &= \sigma(2^{m-1}(2^m - 1)) = \sigma(2^{m-1})\sigma(2^m - 1) \\
   &\text{Since } 2^m - 1 \text{ is prime the divisors are } 1 \text{ and } 2^m - 1 \text{ and so we know } \sigma(2^m - 1) = 1 + 2^m - 1 = 2^m \\
   &\text{and since } \sigma(p^k) = \frac{p^{k+1} - 1}{p - 1} \text{ we know } \sigma(2^{m-1}) = 2^{m-1} - 1. \text{ Therefore} \\
   \sigma(n) &= (2^m - 1)2^m = 2(2^{m-1}(2^m - 1)) = 2n
   \end{align*}
   \]

   \( \Rightarrow \): This direction is fairly lengthy and will be omitted. It's in the text if you're interested.

   \( Q\&E\)

   So now the question is - when is \( 2^m - 1 \) prime? Well one thing we can say is:

5. **Theorem:** If \( m \in \mathbb{Z}^+ \) then if \( 2^m - 1 \) is prime then so is \( m \).

   **Proof:** If \( m \) is not prime with \( m = ab \) with \( a, b > 1 \) then observe that:
   \[
   2^m - 1 = (2^a - 1) \left( 2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1 \right)
   \]
   and so \( 2^m - 1 \) is not prime.

   The reverse is not true, for example \( m = 11 \) is prime but \( 2^{11} - 1 = 2047 = (23)(89) \) is not.

   What this means is finding perfect numbers is equivalent to finding prime \( m \) with \( 2^m - 1 \) also prime. This yields the following definitions:

   **Definition:** The \( m \)th **Mersenne number** is \( M_m = 2^m - 1 \).

   **Example:** The fourth Mersenne number is \( 2^4 - 1 = 15 \).

   **Definition:** If \( p \) is prime and if \( 2^p - 1 \) is also prime then \( M_p = 2^p - 1 \) is a **Mersenne prime**.

   It follows that Mersenne primes correspond to a perfect numbers (and somewhat correspond to primes):
   \[
   [p \text{ prime}] \iff [2^p - 1 \text{ prime}] \iff [2^{p-1}(2^p - 1) \text{ perfect}]
   \]
Example: $p = 5$ is prime and so is $2^p - 1 = 2^5 - 1 = 31$ and so it is a Mersenne prime. Consequently $n = 2^{p-1}(2^p - 1) = 2^4(2^5 - 1) = 496$ is perfect and in fact $\sigma(496) = 992 = 2(496)$.

Okay great, so if $p$ is prime then how can we check if $2^p - 1$ is prime? We could just check all divisors but there’s a slightly more slick way.

6. **Theorem:** If $p$ is an odd prime then any divisors of $M_p = 2^p - 1$ must have the form $2kp + 1$ for $k \in \mathbb{Z}^+$.

What this states is that if we start with a prime $p$ and create $2^p - 1$ (which we don’t know is prime) then we can check if it’s prime by testing all divisors of this form.

**Example:** Consider our $p = 11$ which gave us $2^{11} - 1 = 2047$. This theorem states that the only possibly divisors must have the form $2k(11) + 1 = 22k + 1$ for $k \in \mathbb{Z}^+$. These are 23, 45 and we can stop checking there since $\sqrt{2047} \approx 45.24$ and so any larger divisor must have a smaller co-divisor. Then we see that $2047 \div 23 = 89$ and so it’s not prime.

**Example:** Consider $p = 13$ which gives us $2^{13} - 1 = 8191$. This theorem states that the only possibly divisors must have the form $2k(13) + 1 = 26k + 1$ for $k \in \mathbb{Z}^+$. These are 27, 53, 79 and we can stop checking there since $\sqrt{8191} \approx 90.50$ and so any larger divisor must have a smaller co-divisor. Since none of these work we know that 8191 is prime.

**Note:** In reality we don’t need to check 27 since if 27 divided 8191 then so would 3 and 9 and neither of these have the right form.

**Proof:** Omitted. The proof is not long but depends on a lengthly and obscure lemma related to the Euclidean Algorithm. \( \Box \)