4.4: Perfect, Mersenne, and Fermat Numbers

Integers with certain properties were studied extensively over the centuries. We present some examples of such integers and prove theorems related to these integers and their properties.

We start by defining perfect numbers.

A positive integer \(n\) is called a perfect number if \(\sigma(n)=2n\).

In other words, a perfect number is a positive integer which is the sum of its proper divisors.

The first perfect number is 6, since \(\sigma(6)=12\). You can also view this as \((6=1+2+3)\). The second perfect number is 28, since \(\sigma(28)=56\) or \((28=1+2+4+7+14)\).

The following theorem tells us which even positive integers are perfect.

The positive integer \(n\) is an even perfect number if and only if \(n=2^{l-1}(2^l-1),\) where \(l\) is an integer such that \(l\geq 2\) and \(2^l-1\) is prime.

We show first that if \(n=2^{l-1}(2^l-1)\) where \(l\) is an integer such that \(l\geq 2\) and \(2^l-1\) is prime then \(n\) is perfect. Notice that \(2^l-1\) is odd and thus \((2^l-1,2^l-1)=1\). Also, notice that \(\sigma\) is a multiplicative function and thus \(\sigma(n)=\sigma(2^{l-1})\sigma(2^l-1).\) Notice that \(\sigma(2^{l-1})=2^l-1\) and since \(2^l-1\) is prime we get \(\sigma(2^l-1)=2^l.\) Thus \(\sigma(n)=2n.\) We now prove the converse. Suppose that \(n\) is a perfect number. Let \(n=2^rs,\) where \(r\) and \(s\) are positive integers and \(s\) is odd. Since \((2^r,s)=1\), we get \(\sigma(n)=\sigma(2^r)\sigma(s)=2^r(r+1)s.\) Since \(n\) is perfect, we get \(\sigma(2^r(r+1)s)=2^{r+1}s.\) Notice now that \((2^r(r+1)s=1)\) and thus \(2^{r+1}\mid \sigma(s).\) Therefore there exists an integer \(q\) such
that \( \sigma(s) = 2^{r+1}q \). As a result, we have \( [(2^{r}+1)2^{r+1}q = 2^{r+1}s] \) and thus we get \( [(2^{r}+1)q = s] \) so we get that \( q \mid s \). We add \( q \) to both sides of the above equation and we get \( [s+q = (2^{r}+1)q + q = 2^{r+1}q = \sigma(s)] \). We have to show now that \( q = 1 \). Notice that if \( q \neq 1 \), then \( q \) will have three divisors and thus \( \sigma(q) = 1 + q + q \). Hence \( q = 1 \) and as a result \( q = 2^{r}+1 \). Also notice that \( \sigma(s) = s+1 \). This shows that \( q \) is prime since the only divisors of \( q \) are \( 1 \) and \( q \). As a result, \([n=2^r(2^{r+1}-1)],\) where \([(2^r+1)] \) is prime.

In theorem 50, we see that to determine even perfect numbers, we need to find primes of the form \( 2^{r-1} \). It is still unknown whether there are odd perfect numbers or not.

If \( 2^{r-1} \) is prime where \( r \) is a positive integer, then \( r \) must be prime.

Suppose that \( r \) is composite, that is \( r = st \) where \( 1 < s < t \). Thus after factoring, we get that \( 2^{st-1} = (2^s-1)(2^{s(t-1)}+2^{s(t-2)}+...+2^s+1) \). Notice that the two factors above are both greater than 1. Thus \( 2^{st-1} \) is not prime. This is a contradiction.

The above theorem motivates the definition of interesting numbers called Mersenne numbers.

Let \( r \) be a positive integer. An integer of the form \( M_r = 2^{r-1} \) is called the \( r \)th Mersenne number; if \( r \) is prime then \( M_r = 2^{r-1} \) is called the \( r \)th Mersenne prime.

\( M_3 = 2^3 - 1 = 7 \) is the third Mersenne prime.

We prove a theorem that help decide whether Mersenne numbers are prime.

Divisors of \( M_p = 2^{p-1} \) for prime \( p \) is of the form \( 2mp+1 \), where \( m \) is a positive integer.

Let \( p \) be a prime dividing \( M_p = 2^{p-1} \). By Fermat’s theorem, we know that \( p \mid (2^{p-1} - 1) \). Also, it is easy to see that \( (2^p - 1, 2^{p-1} - 1) = 2^{(p, p-1)} - 1 \). Since \( p \) is a common divisor of \( 2^{p-1} \) and \( 2^{p-1} - 1 \) and thus not relatively prime. Hence \( (p, p-1) = p \). Hence \( (p, p-1) = p \) and thus there exists a positive integer \( k \) such that \( (p, p-1) = kp \). Since \( p \) is odd, then \( k \) is even and thus \( k = 2m \). Hence \( (p, k) = (kp+1, 2mp+1) \). Because any divisor of \( M_p \) is a product of prime divisors of \( M_p \), each prime divisor of \( M_p \) is of the form \( 2mp+1 \) and the result follows.

\( M_{23} = 2^{23} - 1 \) is divisible by \( 47 = 46k+1 \). We know this by trial and error and thus looking at all primes of the form \( 46k+1 \) that are less than \( \sqrt{M_{23}} \).

We now define Fermat numbers and prove some theorems about the properties of these numbers.

Integers of the form \( F_n = 2^{2^n} + 1 \) are called Fermat numbers.

Fermat conjectured that these integers are primes but it turned out that this is not true. Notice that \( F_0 = 3 \), \( F_1 = 5 \), \( F_2 = 17 \), \( F_3 = 257 \) and \( F_4 = 65537 \) while \( F_5 \) is composite. It turned out the \( F_5 \) is divisible by \( 641 \). We now present a couple of theorems about the properties of these numbers.

UC Davis ChemWiki is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License.
For all positive integers \( n \), we have \([F_0F_1F_2...F_{n-1}=F_n-2]\)

We will prove this theorem by induction. For \( n=1 \), the above identity is true. Suppose now that \([F_0F_1F_2...F_{n-1}=F_n-2]\) holds. We claim that \([F_0F_1F_2...F_{n}=F_{n+1}-2]\) Notice that
\([F_0F_1F_2...F_{n}=(F_n-2)F_n=(2^{2^n}-1)(2^{2^n}+1)=2^{2^{n+1}}-1=F_{n+1}-2]\)

Using Theorem 53, we prove that Fermat numbers are relatively prime.

Let \( s \neq t \) be nonnegative integers. Then \((F_s,F_t)=1\).

Assume without loss of generality that \( s<t \). Thus by Theorem 52, we have \([F_0F_1F_2...F_s...F_{t-1}=F_t-2]\) Assume now that there is a common divisor \( (d) \) of \((F_s) \) and \((F_t) \). thus we see that \( (d) \) divides \([F_t-F_0F_1F_2...F_s...F_{t-1}=2]\). Thus \( (d=1) \) or \( (d=2) \). But since \( (F_t) \) is odd for all \( t \). We have \( (d=1) \). Thus \( (F_s) \) and \( (F_t) \) are relatively prime.

**Exercises**

1. Find the six smallest even perfect numbers.
2. Find the eighth perfect number.
3. Find a factor of \((2^{1001}-1)\).
4. We say \( (n) \) is abundant if \( (\sigma(n)>2n) \). Prove that if \( (n=2^{m-1}(2^m-1)) \) where \( (m) \) is a positive integer such that \((2^m-1) \) is composite, then \( (n) \) is abundant.
5. Show that there are infinitely many even abundant numbers.
6. Show that there are infinitely many odd abundant numbers.
7. Determine whether \( (M_{(11)}) \) is prime.
8. Determine whether \( (M_{(29)}) \) is prime.
9. Find all primes of the form \((2^{2^n}+5)\) where \( (n) \) is a nonnegative integer.

**Contributors and Attributions**

- Dr. Wissam Raji, Ph.D., of the American University in Beirut. His work was selected by the Saylor Foundation’s [Open Textbook Challenge](https://www.saylor.org) for public release under a Creative Commons Attribution (CC BY) license.