DIVISORS AND PERFECT NUMBERS

1. Early History

The almost mystical regard for perfect numbers is as old as the mathematics concerning them. The Pythagoreans equated the perfect number 6 to marriage, health, and beauty on account of the integrity and agreement of its parts.

Around 100 c.e., Nicomachus noted that perfect numbers strike a harmony between the extremes of excess and deficiency (as when the sum of a numbers divisors is too large or small), and fall in the suitable order: 6, 28, 496, and 8128 are the only perfect numbers in the intervals between 1, 10, 100, 1000, 10000, and they end alternately in 6 and 8. Near the end of the twelfth century, Rabbi Josef b. Jehuda Ankin suggested that the careful study of perfect numbers was an essential part of healing the soul. Erycius Puteanus in 1640 quotes work assigning the perfect number 6 to Venus, formed from the triad (male, odd) and the dyad (female, even). Hrotsvit, a Benedictine in the Abbey of Gandersheim of Saxony and perhaps the earliest female German poet, listed the first four perfect numbers in her play Sapientia as early as the tenth century:

“We should not leave unmentioned the principal numbers . . . those which are called perfect numbers. These have parts which are neither larger nor smaller than the number itself, such as the number six, whose parts, three, two, and one, add up to exactly the same sum as the number itself. For the same reason twenty-eight, four hundred ninety-six, and eight thousand one hundred twenty-eight are called perfect numbers.”

2. Elementary Results

We first define the sum of divisors function \( \sigma(n) \). We will use \( \sum \) notation to denote a sum. For example,

\[
\sum_{j=1}^{4} j = 1 + 2 + 3 + 4 = 10,
\]

or

\[
\sum_{j \text{ even and less than 10}} 1 = 1 + 1 + 1 + 1 = 4.
\]

We also recall the notation \( d \mid n \) if \( d \) divides \( n \) without a remainder.

**Definition 2.1.** The sum of divisors function is the function

\[
\sigma(n) = \sum_{d \mid n} d,
\]

where \( d \) runs over the positive divisors of \( n \) including 1 and \( n \) itself.
Example 2.2. We have
\[ \sigma(11) = \sum_{d \mid 11} d. \]
Since the only divisors of 11 are 1 and 11, we have that
\[ \sum_{d \mid 11} d = 1 + 11. \]
Since 1 + 11 = 12, we have
\[ \sigma(11) = 12. \]

Definition 2.3. The number \( N \) is said to be perfect if \( \sigma(N) = 2N \). When \( \sigma(N) < 2N \), we say that \( N \) is deficient. If \( \sigma(N) > 2N \), we say that \( N \) is abundant.

The definition of perfect is equivalent to saying that the sum of the proper divisors of \( N \) is equal to \( N \) (we just do not add \( N \) itself to the sum). While this may seem more natural, the central reason for using the function \( \sigma \) is that it possesses some very special properties.

Definition 2.4. We say that a function \( f \) is multiplicative if for any integers \( m, n \) with \( \gcd(m, n) = 1 \), we have
\[ f(mn) = f(m)f(n). \]

Here is an example of a multiplicative function.

Example 2.5. The function \( \text{id}(n) = n \) is multiplicative. If we have integers \( m \) and \( n \) with \( \gcd(m, n) = 1 \), then
\[ \text{id}(mn) = mn = \text{id}(m)\text{id}(n). \]

We now show that \( \sigma(n) \) is a multiplicative function.

Proposition 2.6. The function \( \sigma(n) \) is multiplicative.

Before we do a full proof, we will work through an example. If \( m = 3 \) and \( n = 5 \), let’s try to show that \( \sigma(mn) = \sigma(m)\sigma(n) \). First, we know that the divisors of 3 are 1 and 3, and the divisors of 5 are 1 and 5. This confirms that \( \gcd(3, 5) = 1 \). Now, let’s look at \( mn \), which equals 15. Notice that the divisors of 15 are 1, 3, 5, and 15. These divisors are all obtained by multiplying a divisor of 3 by a divisor of 5. Now, we have
\[ \sigma(3)\sigma(5) = \left( \sum_{d \mid 3} d \right) \left( \sum_{d \mid 5} d \right) = (1 + 3)(1 + 5) = 1 + 3 + 5 + 15. \]
All of the terms on the far right are exactly the divisors of 15, and we got them merely by multiplying a divisor of 3 by a divisor of 5. Now, by the definition of \( \sigma(n) \), we have that
\[ \sigma(15) = \sum_{d \mid 15} d = 1 + 3 + 5 + 15. \]
Thus we have shown that \( \sigma(3)\sigma(5) = \sigma(15) = \sigma(3 \times 5) \). The key point is that if \( \gcd(m, n) = 1 \), then the all of the divisors of \( mn \) are the numbers you get when you multiply a divisor of \( m \) with a divisor of \( n \).
Proof. Suppose that \( \gcd(m, n) = 1 \). Then the only divisor \( d \) that \( m \) and \( n \) share is 1. We now list the divisors of \( m \) and \( n \). Say that the divisors of \( m \) are \( \{1, d_1, d_2, \ldots, d_u\} \) and the divisors of \( n \) are \( \{1, e_1, e_2, \ldots, e_v\} \). Then

\[
\sigma(m)\sigma(n) = \left(\sum_{i|m} i\right) \left(\sum_{j|n} j\right) = (1 + d_1 + d_2 + \cdots + d_u)(1 + e_1 + e_2 + \cdots + e_v).
\]

If we expand the product, we get the sum of all of the combinations we can get of taking a divisor of \( m \) and multiplying it by a divisor of \( n \). Therefore, all of the numbers in the sum we get by expanding the product are divisors of \( mn \). We now need to check that these are all of the divisors of \( mn \). But since \( \gcd(m, n) = 1 \), we have that any divisor of \( mn \) can be written as a divisor of \( m \) times a divisor of \( n \), so our sum has all of the divisors of \( mn \). Thus

\[(1 + d_1 + d_2 + \cdots + d_u)(1 + e_1 + e_2 + \cdots + e_v) = \sigma(mn).\]

Thus \( \sigma(mn) = \sigma(m)\sigma(n) \), just as we hoped.

\[\square\]

**Exercise 2.7.** Define the function \( \mathbb{1}(n) \) by

\[\mathbb{1}(n) = 1 \quad \text{for all integers } n.\]

Show that \( \mathbb{1}(n) \) is a multiplicative function.

**Exercise 2.8.** Define the function \( \sigma_0(n) \) by

\[\sigma_0(n) = \sum_{d|n} 1.\]

(Note that this definition is very similar to the definition of \( \sigma(n) \).) Show that \( \sigma_0(n) \) is a multiplicative function.

**Exercise 2.9.** (1) Define the function \( \sigma_2(n) \) by

\[\sigma_2(n) = \sum_{d|n} d^2.\]

Show that \( \sigma_2(n) \) is a multiplicative function. (Hint: Use the same sort of argument that showed that \( \sigma(n) \) is multiplicative.)

(2) What if I define

\[\sigma_3(n) = \sum_{d|n} d^3?\]

What about

\[\sigma_r(n) = \sum_{d|n} d^r.\]

Are these functions multiplicative? (Hint: Use the same sort of argument that showed that \( \sigma(n) \) is multiplicative.)

Because \( \sigma(n) \) is multiplicative, this allows us to figure out any value of \( \sigma(n) \) as long as we know what \( \sigma(n) \) is at a prime power. Before we do that, we give an identity that will help with some of the arithmetic.
Proposition 2.10. If $x \neq 1$ is a real number, then

$$\sum_{i=0}^{k} x^i = 1 + x + x^2 + x^3 + \cdots + x^{k-1} + x^k = \frac{x^{k+1} - 1}{x - 1}.$$  

Proof. We have

$$(1 + x + x^2 + x^3 + \cdots + x^{k-1} + x^k)(x - 1)$$

$$= x(1 + x + x^2 + x^3 + \cdots + x^{k-1} + x^k) - (1 + x^2 + x^3 + \cdots + x^{k-1} + x^k)$$

$$= (x + x^2 + x^3 + \cdots + x^{k+1}) - (1 + x^2 + x^3 + \cdots + x^{k-1} + x^k)$$

$$= x^{k+1} + (x + x^2 + x^3 + \cdots + x^k) - (x + x^2 + x^3 + \cdots + x^{k-1} + x^k) - 1$$

$$= x^{k+1} + 0 - 1$$

$$= x^{k+1} - 1.$$  

Since

$$(1 + x + x^2 + x^3 + \cdots + x^{k-1} + x^k)(x - 1) = x^{k+1} - 1,$$

we can divide both sides by $x - 1$ to get

$$1 + x + x^2 + x^3 + \cdots + x^{k-1} + x^k = \frac{x^{k+1} - 1}{x - 1}.$$  

□

We can use this to get a nice formula for $\sigma(p^\alpha)$, where $p$ is prime and $\alpha$ is a positive integer.

Exercise 2.11. (1) Compute $\sigma(49)$. Note that $49 = 7^2$.

(2) Compute $\sigma(16)$. Note that $16 = 2^4$.

(3) Let $p$ be prime and let $\alpha$ be a positive integer. Show that

$$\sigma(p^\alpha) = 1 + p + p^2 + p^3 + \cdots + p^{\alpha-1} + p^\alpha.$$  

(4) Using Proposition 2.10, show that

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}.$$  

We will now compute $\sigma(12)$. We know that $12 = 3 \times 4$, and $\gcd(3, 4) = 1$. Thus

$$\sigma(12) = \sigma(3)\sigma(4).$$  

Now, using Exercise 2.11, we have that

$$\sigma(3) = \sigma(3^1) = \frac{3^2 - 1}{3 - 1} = 4$$

and

$$\sigma(4) = \sigma(2^2) = \frac{2^3 - 1}{2 - 1} = 7.$$  

Thus $\sigma(12) = 28$.

We now show how if you have a number $N$ with prime factorization

$$N = p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i},$$

then you can compute $\sigma(N)$ exactly. (Here, $\prod_{i=1}^{k}$ means the same thing as $\sum_{i=1}^{k}$, except that now we’re taking a product instead of a sum.)
Theorem 2.12. If $N$ has prime factorization

$$N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i},$$

then

$$\sigma(N) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$ 

Proof. We first write

$$\sigma(N) = \sigma\left(\prod_{i=1}^{k} p_i^{a_i}\right).$$

Because $\sigma(n)$ is multiplicative, we can write

$$\sigma\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \sigma(p_k^{a_k}) \sigma\left(\prod_{i=1}^{k-1} p_i^{a_i}\right).$$

Repeating this over and over, we eventually get

$$\sigma\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} \sigma(p_i^{a_i}).$$

Using Exercise 2.11, we then have that

$$\sigma\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1},$$

just as we hoped. \qed

Now that we can compute $\sigma(n)$ exactly, we can compute the first few perfect numbers. Recall that a number $N$ is perfect if we have $\sigma(N) = 2N$.

Exercise 2.13. Show that 6 and 28 are perfect numbers.

It turns out to be the case that the first 4 perfect numbers are

$$6 = 1 + 2 + 3,$$
$$28 = 1 + 2 + 4 + 7 + 14,$$
$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248,$$
$$8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064.$$

Each of these numbers can be written in a special form:

$$6 = 2^1(1 + 2) = 2 \cdot 3,$$
$$28 = 2^2(1 + 2 + 2^2) = 4 \cdot 7,$$
$$496 = 2^4(1 + 2 + 2^2 + 2^3 + 2^4) = 16 \cdot 31,$$
$$8128 = 2^6(1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6) = 64 \cdot 127.$$

Notice, though, that the numbers

$$90 = 2^3(1 + 2 + 2^2 + 2^3) = 8 \cdot 15 \quad \text{and} \quad 2016 = 2^5(1 + 2 + 2^2 + 2^3 + 2^4 + 2^5) = 32 \cdot 63$$
are not on our list of the first few perfect numbers. As Euclid pointed out, this is because $15 = 3 \cdot 5$ and $63 = 3^2 \cdot 7$ are not prime numbers, whereas $3, 7, 31, \text{ and } 127$ are all prime.

**Theorem 2.14** (Euclid). If $2^n - 1$ is prime, then $N = 2^{n-1}(2^n - 1)$ is perfect.

**Proof.** If $2^n - 1$, then the only prime divisors of $N = 2^{n-1}(2^n - 1)$ are $2$ and $2^n - 1$. Since $2^n - 1$ occurs as a single prime, we have simply stated that

$$\sigma(2^n - 1) = 1 + (2^n - 1) = 2^n.$$ 

Therefore,

$$\sigma(N) = \sigma(2^{n-1})\sigma(2^n - 1) = \left(\frac{2^n - 1}{2 - 1}\right)2^n = 2^n(2^n - 1) = 2N.$$ 

Therefore, $N$ is perfect. \qed

The task of finding perfect numbers, then, is intimately linked with finding primes of the form $2^n - 1$. Such numbers are referred to as **Mersenne primes**, after the seventeenth century monk Marin Mersenne, a colleague of Descartes, Fermat, and Pascal. He is credited with investigating these unique primes as early as 1644. Mersenne knew that $2^{n-1}$ is prime for $n = 2, 3, 5, 11, 13, 17, \text{ and } 19$ and, more brilliantly, conjectured the cases $n = 31, 67, 127, 257$. It took nearly two hundred years to test these numbers.

We now show a way to determine if a Mersenne number is prime.

**Proposition 2.15.** If $2^n - 1$ is prime, then $n$ is also prime.

**Proof.** In the proof of Proposition 2.10, we showed that

$$(1 + x + x^2 + x^3 + \cdots + x^{k-1} + x^k)(x - 1) = x^{k+1} - 1.$$ 

Now, suppose to the contrary that we can write $n = rs$ with $r, s > 1$. Then

$$2^n - 1 = (2^r)^s - 1 = (2^r - 1)((2^r)^{s-1} + \ldots + 2^r + 1).$$ 

Therefore,

$$(2^r - 1) \mid (2^n - 1).$$ 

But we claimed that $2^n - 1$ is prime, so that means that $1$ is the only divisor of $2^n - 1$ other than $2^n - 1$ itself. Thus $2^r - 1 = 1$. This can only mean that $r = 0$, but we said earlier that $r > 1$. This gives us a contradiction. Therefore, the assumption that we can write $n = rs$ with $r, s > 1$ is false. This means that $n$ is prime. \qed