6.9. Perfect Numbers, Mersenne Primes, Arithmetic Functions

Note. In this section, we consider the sum of the divisors of a positive integer, define perfect numbers, and discuss their history. We mention the Goldbach Conjecture, its history, and its connection to ETSU. We consider Mersenne primes and their history. We consider the Möbius function, the Möbius inversion formula, and Dirichlet convolution.

Definition. An *arithmetic function* is a function with domain $\mathbb{N}$. We take the codomain to be $\mathbb{R}$. For arithmetic function f and $n \in \mathbb{N}$ define $\sum_{d\,|\,n} f(d)$ as the sum of the values of f on the positive divisors of n. Arithmetic function f such that $f(n) \neq 0$ for at least one $n \in \mathbb{N}$ is *multiplicative* if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$.

Note. Theorem 6.59 (the "moreover" part) shows that Euler's φ function is multiplicative. The next result and its corollary illustrate the advantage of having a multiplicative function.

Theorem 6.85. Suppose f is a multiplicative function. Then

(i) $f(1) = 1$, and

(ii) if n has standard factorization $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, then

$$f(n) = \prod_{i=1}^{r} f\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} f(p_i^{\alpha_i}).$$

Note. Notice that we **cannot** carry the conclusion of Theorem 6.85 another step to conclude that $f(n) = \prod_{i=1}^{r} f(p_i^{\alpha_i}) = \prod_{i=1}^{r} f(p_i)^{\alpha_i}$, because $(p_i, p_i) = p_i \neq 1$ (so the definition of "multiplicative function" does not even apply to $p_i^{\alpha_i}$).

Corollary 6.86. A multiplicative function is completely determined by its value on prime powers.

Definition 6.87. For $n \in \mathbb{N}$, define $\sigma(n)$ to be the sum of the positive divisors of n. That is, $\sigma(n) = \sum_{d \mid n} d$.

Example 6.88. Some values of σ are: $\sigma(1) = 1$, $\sigma(5) = 1 + 5 = 6$, and $\sigma(6) = 1+2+3+6 = 12$. If p is prime then $\sigma(p) = p+1$ and $\sigma(p^\alpha) = 1+p+p^2+\cdots+p^\alpha$ for all $\alpha \in \mathbb{N}$. We can also show that $\sigma(28) = 56$, $\sigma(496) = 992$, and $\sigma(8{,}128) = 16{,}256$.

Theorem 6.89. σ is a multiplicative function.

Corollary 6.90. If $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ then $\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$.

Note. Gerstein makes an insightful observation on page 337: "Some of the most intriguing topics in number theory relate to the mysterious interaction between multiplication and addition." He lists as an example the Goldbach Conjecture which claims that every even integer greater than or equal to 4 can be written as a sum of two primes. "Primes" involve multiplication in the sense that every integer is (plus or minus) a *product* of primes, yet it concerns writing numbers as a *sum*.

Note. The Wikipedia Goldbach's Conjecture website is thorough. These comments are based on that website. On June 7, 1742 the German mathematician Christian Goldbach (March 18, 1690–November 20, 1764) write a letter to Leonhard Euler (April 15, 1707–September 18, 1783)). As a parenthetic note, we seem to keep encountering Euler in this chapter. This is because he is a towering figure in number theory (and several other areas of mathematics). He was born about 300 years ago, and the project of organizing his collected works is still ongoing! More details are in my online presentation Leonard Euler - Happy 300th Birthday!. Returning to the Goldbach/Euler correspondence, Euler replied on June 30 observing that Goldbach's ideas would follow from the fact that every positive even integer greater than 2 can be written as the sum of two primes; an idea that Euler believed to be "completely certain," though he did not have a proof (the original statements were somewhat different, since 1 was considered prime at the time). Numerical studies have confirmed Golbach's Conjecture up to 4×10^{18}, according to the Goldbach conjecture verification website maintained by Tomás Oliveira e Silva (accessed 2/28/2022), but it remain unproved. Goldbach's Weak Conjecture (also called the Ternary Goldbach Conjecture) claims that every odd number greater than 5 can be expressed as the sum of three (not necessarily distinct) primes. This conjecture has an ETSU connection. In 2013, Harald Helfgott proposed a proof that was accepted for publication in *Annals of Mathematics Studies* (in 2015), but which has apparently not yet appeared. A Google search indicates that the latest available work on this is from 2015 and is available on arXiv.org: The Ternary Goldbach Problem (this is a 327 page document; accessed 2/28/2022). The ETSU connection is that Harald Helgott is the son of former ETSU Department of Mathematics and Statistics faculty members Drs. Edith Seier and Michel Helfgott (both retired in the late 2010s).

Note. Another (commonly studied) idea relating the interaction between multiplication and addition is the following.

Definition 6.91. An integer $n > 1$ is *perfect* if $n = \sum_{d\,|\,n, d<n} d$, or equivalently if $\sigma(n) = 2n$.

Note. We see from the values of σ given in Example 6.88 that 6, 28, 496, and 8,128 are perfect numbers.

Remark 6.92. If positive integer n factors as $n = d \cdot e$ then $e = n/d$. So as d varies over all the divisors of n then e also varies over all divisors of n (we can think of divisors of n as coming in pairs (d, e) where $n = d \cdot e$). So for a perfect number n (for which $\sigma(n) = 2n$) we have

$$2n = \sigma(n) = \sum_{d \mid n} d = \sum_{d \mid n} \frac{n}{d} = n \sum_{d \mid n} \frac{1}{d},$$

so that $2 = \displaystyle\sum_{d \mid n} \frac{1}{d}$ (and conversely, if this last equality holds then n is perfect).

Note. We now consider some history of perfect numbers. The MacTutor History of Mathematics Archive's page on "Perfect Numbers" (on which most of this history is base; accessed 3/1/2022) mentions that is is not known as to when perfect numbers were first studied, but suggests that the Egyptians may have been aware of this idea (the page cites C. M. Taisbak's "Perfect numbers: A mathematical pun? An analysis of the last theorem in the ninth book of Euclid's Elements," *Centaurus* **20**(4), 269–275 (1976)). The page also mentions that Pythagoras took a mystical interest in perfect numbers. The first recorded mathematical result on perfect numbers appears around 300 BCE in Euclid's *Elements* in Book IX as Proposition 36: "If as many numbers as we please beginning from a unit are set out continuously in double proportion until the sum of all becomes prime, and if the sum multiplied into the last makes some number, then the product is perfect." In modern terminology, this translates into the claim: "If for some $k > 1$ we have $2^k - 1$ prime, then $2^{k-1}(2^k - 1)$ is a perfect number." We'll see below (Exercise 6.93) that the condition $2^k - 1$ is prime requires that k itself is prime. Around 100 CE Nichomachus of Gerasa (circa 60 CE–120 CE) in his *Introductio Arithmetica* (a foundational work in classical algebra) gives a classification of numbers based on the idea of perfect numbers. By adding up what was called the "aliquot parts" of a number (what we would call the divisors of the number, excluding the number itself), he classified numbers (i.e., positive integers) as *deficient* (when the sum of the aliquot parts is less than the number), *superabundant* (when the sum of the aliquot parts is greater than the number), and *perfect* (when the sum of the aliquot parts equals the number). This idea of some type of "balance" with perfect numbers has been taken up by some in the religious and mystical community (Nichomachus himself made some strange observations). Nichomachus made several claims about perfect numbers, but provided no proofs. Some of his claims are true, some are false, and some are still open problems. In particular, he claimed that there are infinitely many perfect numbers. This and his other claims are bold, given that there were only four perfect numbers known at the time: 6, 28, 496, and 8128.

Note. Islamic mathematician and astronomer Thabit ibn Qurra (836–901) in his *Treatise on Amicable Numbers* explored when numbers of the form $2^n p$ are perfect, where p is prime. Islamic mathematician Ibn al-Haytham (965–1039) gave a partial converse of Euclid's Proposition IX.36 in his *Treatise on Analysis and Synthesis*. Ismail ibn Ibrahim ibn Fallus (1194–1239) wrote a treatise in which he gave a table of ten numbers that he claimed were perfect; the first seven were correct, but the last three were not. The fifth perfect number (33,550,336) was rediscovered (the results of Fallus seem to be unknown at the time in central Europe) and included in a manuscript dated 1461. Another mansucript by the same author included both the fifth and sixth perfect numbers (the sixth perfect number is

8,589,869,056). The only thing known about the author of these manuscripts is that he lived in Florence. The German scholar Johan Regiomontanus (June 6, 1436–July 6, 1476) in 1461 included the fifth perfect number in a manuscript he wrote in 1461. In 1536, Hudalrichus Regius in his *Ultriusque Arithmetices* observed that $2^{11}-1 = 2047 = 23\cdot 89$ so that $2^{p-1}(2^p-1)$ is not a perfect number. That is, Regius has found the first prime p such that $2^{p-1}(2^p-1)$ is not perfect. he also showed that $2^{13}-1 = 8191$ is prime so that (by Euclid IX.36) $2^{12}(2^{13}-1) = 33{,}550{,}336$ is perfect (this is another "discovery" of the fifth perfect number).

Note. In 1603, Italian mathematician Pietro Cataldi (April 15, 1548–February 11, 1626) created a table of primes up to 750 and used it to find the sixth perfect number (again) and the seventh perfect number (namely, 137,438,691,328); he also made some false claims. In a letter to French monk and math enthusiast Marin Mersenne (September 8, 1588–September 1, 1648) in 1640, Fermat used his "Little Theorem" (Corollary 6.53) to show two of Cataldi's claims were wrong (he factored two numbers which Cataldi had claimed were prime). Fermat's letter inspired Mersenne to further explore prime numbers and perfect numbers. He published *Cogitata Physica Mathematica* in 1644 in which he claimed 2^p-1 is prime for several values of prime p; these prime numbers then yield perfect numbers $2^{p-1}(2^p-1)$ by Euclid IX.36. Primes of the form 2^p-1 are now known as *Mersenne primes.* In 1732 Euler was the next to give a new perfect number (the first in 125 years); he proved that $2^{30}(2^{31}-1) = 2{,}305{,}843{,}008{,}139{,}952{,}128$ is the eighth perfect number. In two manuscripts that Euler wrote but did not publish, he proved the converse of Euclid's Proposition IX.36. That is, he proved that every even perfect number is of the form $2^{p-1}(2^p-1)$ where p is prime and 2^p-1 is a Mersenne prime (our Theorem 6.94 below). Of course this does not give all even perfect numbers explicitly, since there are unanswered questions about Mersenne primes. Skipping ahead quite a bit, according to the Wikipedia page "List of Mersenne Primes and Perfect Numbers" (accessed 3/1/2022), there are 51 known Mersenne primes and perfect numbers. The largest known perfect number is $2^{p-1}(2^p-1)$ where $p = 82{,}589{,}933$, computed in late 2018; it has almost 50 million digits (more details can be found on the Great Internet Mersenne Prime Search (GIMPS) website) and $2^{82{,}589{,}933}-1$ presently (March 1, 2022) stands as the largest known prime number (it has almost 25 million digits).

Note. Some unsolved problems concerning perfect numbers and Mersenne primes include:

1. Are there infinitely many perfect numbers?
2. Are there infinitely many Mersenne primes?
3. Are there any odd perfect numbers?

According to Gerstein (see page 340), it is known that no odd perfect number exists that is less than 10^{300}. We now return to the presentation given in Gerstein.

Definition. A prime number of the form 2^p-1 with p prime is a *Mersenne prime*, denoted M_p.

Note. We may have p prime, yet 2^p not prime. This was observed in 1536 by Hudalrichus Regius, as mentioned above, who factored $2^{11} - 1$ as $2^{11} - 1 = 2047 = 23 \cdot 89$. One might consider numbers of the form $2^n - 1$ where n is *not* prime in the hopes of finding a prime number However, this will not work, as illustrated in the next result.

Exercise 6.93. Prove that if n is positive and composite, then $2^n - 1$ is not prime. That is, for $2^n - 1$ to be prime, it is necessary that n is prime.

Note. The next result is Euler's converse of Euclid's Book IX Proposition 36 (both mentioned above). The result is sometimes called the "Euclid-Euler Theorem."

Theorem 6.94. Euclid-Euler Theorem.
A positive even integer n is perfect if and only if there is a factorization $n = 2^{p-1}(2^p - 1)$ with p prime and $2^p - 1$ a Mersenne prime.

Note. The Euclid-Euler Theorem (Theorem 6.94) marks the high point of our exploration of number theory. We conclude this section by introduction two more arithmetic functions.

Definition. The *Möbius function* is the arithmetic function $\mu : \mathbb{N} \to \{0, 1, -1\}$ given by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ a product of } r \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

Notice that $\mu(n) = 0$ whenever n is divisible by the square of a prime; that is, whenever n is not *square-free*.

Note. The Möbius function is named for German topologist August Möbius (November 17, 1790–September 26, 1868). We'll prove the Möbius Inversion Formula (Theorem 6.97) below and from that we will again derive the formula for $\varphi(n)$ in terms of the standard factorization of n (in Theorem 6.99).

Lemma 6.96. Suppose $n \in \mathbb{N}$. Then $\displaystyle\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$

Theorem 6.97. Möbius-Inversion Formula.
Let f be an arithmetic function, and suppose $g(n) = \sum_{d \mid n} f(d)$ for all $n \in \mathbb{N}$. Then

$$f(n) = \sum_{d \mid n} \mu(d) g(n/d).$$

Note. We now turn our attention back to Euler's φ function and apply the Möbius-Inversion Formula to express $\varphi(n)$ in terms of the standard factorization of n. First, we need a lemma.

Lemma 6.98. If $n \in \mathbb{N}$, then $\displaystyle\sum_{d \mid n} \varphi(d) = n$.

Theorem 6.99.

(i) If n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

(ii) φ is multiplicative.

Note. Our final idea in this section lets us create new arithmetic functions from old ones.

Definition 6.100. If f and g are arithmetic functions, define

$$(f * g)(n) = \sum_{d \mid n} f(d) g(n/d) \text{ for all } n \in \mathbb{N}.$$

The function $f * g$ is the *Dirichlet convolution* of f and g.

Theorem 6.101. If f and g are multiplicative functions, then $f * g$ is multiplicative.

Revised: 4/24/2022