PERFECT NUMBERS: AN ELEMENTARY INTRODUCTION

JOHN VOIGHT

Abstract. This serves as an elementary introduction to the history and theory surrounding even perfect numbers.

> One would be hard put to find a set of whole numbers with a more fascinating history and more elegant properties surrounded by greater depths of mystery—and more totally useless—than the perfect numbers.
>
> —Martin Gardner [2]

The number 6 is unique in that $6 = 1+2+3$, where 1, 2, and 3 are all of the proper divisors of 6. The number 28 also shares this property, for $28 = 1 + 2 + 4 + 7 + 14$. These "perfect" numbers have seen a great deal of mathematical study—indeed, many of the basic theorems of number theory stem from the investigation of the Greeks into the problem of perfect and Pythagorean numbers [16]. Moreover, it was while investigating these numbers that Fermat discovered the (little) theorem that bears his name and which forms the basis of a substantial part of the theory of numbers. Though it is rooted in ancient times, remarkably this subject remains very much alive today, harboring perhaps the "oldest unfinished project of mathematics" [17].

This paper surveys the history and elementary results concerning perfect numbers from the author's undergraduate thesis. The author would like to thank John Burke and Ken Ono for their advice and Gottfried Barthel and Steve Morris for helpful corrections.

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 number's 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:

Date: May 31, 1998; updated January 27, 2024.

> 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].

Saint Augustine (among others, including the early Hebrews) considered 6 to be a truly perfect number—God fashioned the Earth in precisely this many days (rather than at once) to signify the perfection of His work. Indeed, as recorded by Alcuin of York (who lived from 732 to 804 C.E.), the second origin was imperfect, as it arose from the deficient number $8 > 1+2+4$, this number counting the 8 souls in Noah's ark (Noah, his three sons, and their four wives, in *Genesis*, chapter 7) from which sprung the entire human race [8]. Philo Judeus, in the first century C.E., called 6 the most productive of all numbers, being the smallest perfect number.

Throughout the centuries that followed, various mathematicians carefully studied perfect numbers (see the continued extensive history given by Dickson [6] and also by Picutti [14]). Up to the time of Descartes and Fermat, a sizeable pool of important results—as well as much misinformation—had been collected.

2. Elementary Results

We now turn to some definitions and some elementary results.

Definition 1. The *sum of divisors* is the function $\sigma(n) = \sum_{d|n} d$, where d runs over the positive divisors of n including 1 and n itself.

For example, $\sigma(11) = 1 + 11 = 12$ and $\sigma(15) = 1 + 3 + 5 + 15 = 24$.

Definition 2. The number N is said to be *perfect* if $\sigma(N) = 2N$. When $\sigma(N) < 2N$, we say N is *deficient*; when $\sigma(N) > 2N$, we say N is *abundant*.

The definition of perfect is equivalent to saying that the sum of the *proper* (or aliquot) 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 σ is that it possesses some very special properties. First:

Proposition 3. $\sigma(mn) = \sigma(m)\sigma(n)$ *whenever* $\gcd(m, n) = 1$.

Proof. If d is a divisor of mn, then by unique factorization we can represent d uniquely as the product of a divisor of m and a divisor of n (since they have no common factors). That is, every term of $\sigma(mn)$ (the sum of all divisors of mn) occurs exactly once in the sum $\sigma(m)\sigma(n)$ (the product of all divisors of m and n). The converse is also true: every such product is a divisor of mn, so the sums must be the same.

This suffices to establish the proposition. It might be easier also just to appeal to the very special way in which σ is defined as a divisor sum (for the details consult [12]). □

Hence σ is completely determined when its value is known for every prime-power argument. (Such functions are, of course, the multiplicative functions.) This yields the very useful:

Theorem 4. *If $N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$ is a factorization of N into primes, then*

$$\sigma(N) = \prod_{i=1}^{k} (1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Proof. The only divisors of $p_i^{\alpha_i}$ are $1, p_i, p_i^2, \dots, p_i^{\alpha_i}$, so $\sigma(p_i^{\alpha_i}) = 1+p_i+p_i^2+\cdots+p_i^{\alpha_i}$. Recall the geometric series has the closed form

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

which implies that $\sigma(p_i^{\alpha_i}) = (p_i^{\alpha_i+1} - 1)/(p_i - 1)$. Since σ is multiplicative,

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

as claimed. □

To give us just a little bit practice and feel for this formula for the sum of divisors, we prove the following two short lemmas. If $\eta \mid N$ it is clear that $\sigma(\eta) < \sigma(N)$, but an even stronger result holds:

Lemma 5. *If $\eta \mid N$, then*

$$\frac{\sigma(\eta)}{\eta} \leq \frac{\sigma(N)}{N},$$

where equality holds only if $\eta = N$.

Proof. Note that if $d \mid N$ then $kd = N$ for some k, so $k = (N/d) \mid N$. This argument works just as well in reverse, so we have that $d \mid N$ if and only if $(N/d) \mid N$, which implies that

$$\sigma(N) = \sum_{d|N} d = \sum_{d|N} \frac{N}{d} = N \sum_{d|N} \frac{1}{d}.$$

If η is a proper divisor of N, we have

$$\frac{\sigma(N)}{N} = \sum_{d|N} \frac{1}{d} > \sum_{d'|\eta} \frac{1}{d'} = \frac{\sigma(\eta)}{\eta}.$$

Otherwise, equality holds. □

For free, we also have:

Corollary 6. *If N is perfect, $\sum_{d|N} (1/d) = 2$.*

Proof. We just showed $d \mid N$ is equivalent to $(N/d) \mid N$, hence

$$\sum_{d|N} d = \sum_{d|N} \frac{N}{d} = N \sum_{d|N} \frac{1}{d} = 2N.$$

Cancelling N proves the corollary. □

We assume henceforth that the reader is familiar with congruence arithmetic and the fundamentals of group theory (consult [12] or [7] for some of the basics), of which we will use often use various facts without proof.

3. Even Perfect Numbers

The first individual to really categorize the perfect numbers was the Greek mathematician Euclid. He noticed that the first four perfect numbers are of a very specific form:

$$\begin{aligned} 6 &= 2^1(1+2) = 2 \cdot 3, \\ 28 &= 2^2(1+2+2^2) = 4 \cdot 7, \\ 496 &= 2^4(1+2+2^2+2^3+2^4) = 16 \cdot 31, \text{ and} \\ 8128 &= 2^6(1+2+\cdots+2^6) = 64 \cdot 127. \end{aligned}$$

Notice, though, that the numbers $90 = 2^3(1+2+2^2+2^3) = 8 \cdot 15$ and $2016 = 2^5(1+2+\cdots+2^5) = 32 \cdot 63$ are missing from this sequence. As Euclid pointed out, this is because $15 = 3 \cdot 5$ and $63 = 3^2 \cdot 7$ are both composite, whereas the numbers 3, 7, 31, 127 are all prime.

As it appears in Book IX, proposition 36 of his *Elements*, Euclid writes: "If as many numbers as we please beginning from an unit be set out continuously in double proportion, until the sum of all becomes prime, and if the sum multiplied into the last make some number, the product will be perfect."

We state this observation in a slightly more compact form:

Theorem 7 (Euclid)**.** *If $2^n - 1$ is prime, then $N = 2^{n-1}(2^n - 1)$ is perfect.*

Proof. Clearly the only prime divisors of N are $2^n - 1$ and 2. Since $2^n - 1$ occurs as a single prime, we have simply that $\sigma(2^n - 1) = \big(1 + (2^n - 1)\big) = 2^n$, and thus

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

So N is perfect. □

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, and 19—and, more brilliantly, conjectured the cases $n = 31$, 67, 127, 257. It took nearly two hundred years to test these numbers.

There is one important criterion that hones in on the primality of Mersenne numbers:

Proposition 8 (Cataldi-Fermat)**.** *If $2^n - 1$ is prime, then n itself is prime.*

Proof. Note from before, $x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$. Suppose we can write $n = rs$, where $r, s > 1$. Then

$$2^n - 1 = (2^r)^s - 1 = (2^r - 1)\big((2^r)^{s-1} + \cdots + 2^r + 1\big)$$

so that $(2^r - 1) \mid (2^n - 1)$ which is prime, a contradiction. □

Note that the converse is not true—the number $2^{11} - 1 = 2047 = 23 \cdot 89$, for instance.

Must all perfect numbers be of Euclid's type? Leonard Euler, in a posthumous paper, proved that every *even* perfect number is of this type. Many ingenious proofs of this fact exist.

Theorem 9 (Euler)**.** *If N is an even perfect number, then N can be written in the form $N = 2^{n-1}(2^n - 1)$, where $2^n - 1$ is prime.*

Proof. The first proof is Euler's own [6]. Let $N = 2^{n-1}m$ be perfect, where m is odd; since 2 does not divide m, it is relatively prime to 2^{n-1}, and

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

N is perfect so $\sigma(N) = 2N = 2(2^{n-1}m) = 2^n m$, and with the above, $2^n m = (2^n - 1)\sigma(m)$.

Let $s = \sigma(m)$. We then have $m = (2^n - 1)(s/2^n)$; since 2^n does not divide $2^n - 1$, it must divide s (because m is an integer), so that $m = (2^n - 1)q$ for some $q = s/2^n$. If $q = 1$, we have a number of Euclid's type, for then $m = 2^n - 1$ and $s = \sigma(m) = 2^n = (2^n - 1) + 1 = m + 1$. Since $\sigma(m)$ is the sum of all of the divisors of m, $m = 2^n - 1$ must be a prime, and $N = 2^{n-1}m = 2^{n-1}(2^n - 1)$.

If $q > 1$, we retotal the sum of the divisors of $m = (2^n - 1)q$. The factors of m then include 1, q, $2^n - 1$, and m itself, so that

$$s = \sigma(m) \geq 1 + q + (2^n - 1) + (2^n - 1)q = \big((2^n - 1) + 1\big)(q + 1) = 2^n(q + 1).$$

But this implies

$$\frac{m}{s} \leq \frac{(2^n - 1)q}{2^n(q + 1)} = \left(\frac{2^n - 1}{2^n}\right)\left(\frac{q}{q + 1}\right) < \frac{2^n - 1}{2^n},$$

an impossibility, for we have previously established equality: $\sigma(N) = 2^n m = (2^n - 1)s$ implies that $m/s = (2^n - 1)/2^n$. □

Proof 2. A second, simpler proof is given by Dickson [5]. From $2^n m = (2^n - 1)\sigma(m)$ we note

$$\sigma(m) = \frac{2^n m}{2^n - 1} = \frac{\big((2^n - 1) + 1\big)m}{2^n - 1} = m + \frac{m}{2^n - 1}.$$

Since both $\sigma(m)$ and m are integers, so too must $d = m/(2^n - 1)$ be an integer. Thus $(2^n - 1) \mid m$ and consequently d itself divides m.

But $\sigma(m) = m + m/(2^n - 1) = m + d$ is the sum of *all* of the divisors of m. How can this be? Certainly 1 divides m, so are forced to conclude that $d = 1$; if this were not the case, then we would have $\sigma(m) = m + d + 1$, a contradiction. Therefore, $m = 2^n - 1$, and in partiular, m has no other positive divisors other than one and itself, so $2^n - 1$ is prime. □

Proof 3. A third proof is given by McDaniel [10]. Since $2^n m = (2^n - 1)\sigma(m)$, every prime divisor of $2^n - 1$ must also divide m (for it is odd and cannot divide 2^n). So suppose p^α divides $2^n - 1$ with p prime.

By Lemma 5,

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

Hence,

$$1 = \frac{\sigma(N)}{2N} = \frac{\sigma(2^{n-1})\sigma(m)}{2^n m} \geq \frac{(2^n - 1)(1 + p)}{2^n p} = 1 + \frac{(2^n - 1) - p}{2^n p}.$$

This is only satisfied when the fraction on the right is zero, so that $p = 2^n - 1$, $\alpha = 1$ and $m = p$, hence N is of Euclid's type. □

Proof 4. A similar proof is provided by Cohen [4]. Again we start with $2^n m = (2^n - 1)\sigma(m)$, where $2^n - 1 \mid m$. We then write

$$\frac{\sigma(m)}{m} = \frac{2^n}{2^n - 1}.$$

From the previous lemma,

$$\frac{2^n}{2^n - 1} = \frac{\sigma(m)}{m} > \frac{\sigma(2^n - 1)}{2^n - 1} \geq \frac{1 + (2^n - 1)}{2^n - 1} = \frac{2^n}{2^n - 1}.$$

To sustain equality throughout this expression, we must have $2^n - 1 = m$ and $\sigma(m) = 1 + (2^n - 1) = 1 + m$, or $m = 2^n - 1$ is prime. □

Proof 5. A fifth proof is given by Carmichael [3]. Let $N = 2^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = 2^{\alpha_1} \prod_{i=2}^{k} p_i^{\alpha_i}$. Then

$$\begin{aligned}\frac{\sigma(N)}{2N} &= \frac{1}{2}\left(\frac{\sigma(2^{\alpha_1})}{2^{\alpha_1}}\right)\prod_{i=2}^{k}(\sigma(p_i^{\alpha_i})p_i^{\alpha_i}) \\ &= \left(2^{\alpha_1+1} - 12^{\alpha_1+1}\right)\prod_{i=2}^{k}\left(1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}p_i^{\alpha_i}\right) = 1.\end{aligned}$$

Write $d = 2^{\alpha_1+1} - 1$. Rearranging and dropping terms on the right, we have

$$\frac{2^{\alpha_1+1}}{2^{\alpha_1+1} - 1} = \frac{d+1}{d} = 1 + \frac{1}{d} \geq \prod_{i=2}^{k}\left(\frac{p_i^{\alpha_i - 1} + p_i^{\alpha_i}}{p_i^{\alpha_i}}\right) = \prod_{i=2}^{k}\left(1 + \frac{1}{p_i}\right).$$

Note that $\sigma(N) = d\prod_{i=2}^{k}\sigma(p_i^{\alpha_i}) = 2N = 2^{\alpha_1+1}\prod_{i=2}^{k} p_i^{\alpha_i}$. Immediately, then, some p_i must divide d, for the right-hand side has been completely factored into primes and d is odd. If p_i is an aliquot divisor, then $p_i < d$ and $1 + 1/p_i$ will exceed the left side of the inequality. Hence $p_i = d$. But with that, if $k > 2$, the inequality is again exceeded, so $k = 2$. Likewise, $\alpha_2 = 1$ and we have a number of Euclid's type. □

Proof 6. As if that weren't enough, a sixth and final proof is given by Knopfmacher [9]. Very familiar now, we have

$$\sigma(N) = (2^{\alpha_1+1} - 1)\prod_{i=2}^{k}(1 + p_i + \cdots + p_i^{\alpha_i}) = 2N = 2^{\alpha_1+1}\prod_{i=2}^{k} p_i^{\alpha_i}.$$

Since $2^{\alpha_1+1} - 1$ cannot divide 2, it divides N, and we may write

$$2^{\alpha_1+1} - 1 = p_2^{\gamma_2} p_3^{\gamma_3} \ldots p_k^{\gamma_k} = \prod_{i=2}^{k} p_i^{\gamma_i}.$$

It follows that

$$\frac{2N}{2^{\alpha_1+1} - 1} = 2^{\alpha_1+1}\prod_{i=2}^{k}\frac{p_i^{\alpha_i}}{\prod_{i=2}^{k} p_i^{\gamma_i}} = 2^{\alpha_1+1}\prod_{i=2}^{k} p_i^{\alpha_i - \gamma_i} = \prod_{i=2}^{k}(1 + p_i + \cdots + p_i^{\alpha_i})$$

and therefore

$$2^{\alpha_1+1}\prod_{i=2}^{k} p_i^{\alpha_i-\gamma_i} = \left(1+\prod_{i=2}^{k} p_i^{\gamma_i}\right)\prod_{i=2}^{k} p_i^{\alpha_i-\gamma_i} = \prod_{i=2}^{k}(1+p_i+\cdots+p_i^{\alpha_i})$$

so

$$p_2^{\alpha_2-\gamma_2}p_3^{\alpha_3-\gamma_3}\cdots p_k^{\alpha_k-\gamma_k}+p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k} = (1+p_2+\cdots+p_2^{\alpha_2})\cdots(1+p_k+\cdots+p_k^{\alpha_k}).$$

Since $0 \le \gamma_i \le \alpha_i$ for all i, expanding the product on the right will yield each of the terms on the left. But there are the only two, which means that $\gamma_i = 0$ for all values of i except one; so then $k = 2$, and $\alpha_2 = 1$. The above equation then yields simply

$$p_2^{1-\gamma_2} + p_2 = 1 + p_2 \quad \text{or} \quad p_2^{1-\gamma_2} = 1,$$

so $\gamma_2 = 1$, and N is of Euclid's type as claimed. □

Even perfect numbers have a number of nice little properties. We say that a number is *triangular* if it can be arranged in triangular fashion, that is, one atop two atop three (and so on) arranged in a triangular lattice. While perfect numbers can be written in a geometric expression à la Euclid, they may also be derived from arithemetic progressions:

$$6 = 1+2+3, \quad 28 = 1+2+3+4+5+6+7, \quad 496 = 1+2+3+\cdots+31.$$

We state this result as follows:

Proposition 10. *If N is an even perfect number, then N is triangular.*

Proof. We have m triangular if $m = \sum_{i=1}^{k-1} i = 1+2+\cdots+k = (\frac{1}{2})k(k-1)$ for some k. But note that $N = 2^{n-1}(2^n-1) = (\frac{1}{2})2^n(2^n-1)$. □

We can also write any perfect number as the sum of cubes:

Proposition 11 ([1])**.** *If $N = 2^{n-1}(2^n-1) \neq 6$ is perfect, then $N = 1^3+3^3+\cdots+\left(2^{(n-1)/2}-1\right)^3$.*

Proof. Recall the formula

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4},$$

a fact which can be proved by induction. Let $m = 2^{(n-1)/2}$; we have then that

$$\begin{aligned}
1^3+3^3+\cdots+(2m-1)^3 &= \left(1^3+2^3+\cdots+(2m)^3\right) - \left(2^3+4^3+\cdots+(2m)^3\right) \\
&= \frac{(2m)^2(2m+1)^2}{4} - 2^3\frac{m^2(m+1)^2}{4} \\
&= m^2(2m+1)^2 - 2m^2(m+1)^2 \\
&= m^2(4m^2+4m+1-2m^2-4m-1) = m^2(2m^2-1).
\end{aligned}$$

By substituting for m we get the desired result. □

Perfect numbers have very unique representations. As first noted by Studnička, we have $6 = 110_2$, $28 = 11100_2$, $496 = 111110000_2$, and $8128 = 1111111000000_2$ written in binary; in general:

Proposition 12. *If $N = 2^{n-1}(2^n-1)$ is perfect and N is written in base 2, then it has $2n-1$ digits, the first n of which are unity and the last $n-1$ are zero.*

Proof. This follows immediately from how numbers are written in binary, by recalling that $2^p - 1 = 1 + 2 + \cdots + 2^{p-1}$. □

We also have the historically interesting fact:

Proposition 13. *Every even perfect number ends in either 6 or 8.*

Proof. Every prime greater than 2 is of the form $4m + 1$ or $4m + 3$. In the first case,

$$\begin{aligned} N &= 2^{n-1}(2^n - 1) = 2^{4m}(2^{4m+1} - 1) = 16^m(2 \cdot 16^m - 1) \equiv 6^m(2 \cdot 6^m - 1) \\ &\equiv 6(12 - 1) \equiv 6 \pmod{10}, \end{aligned}$$

since by induction it is clear that $6^m \equiv 6 \pmod{10}$ for all m. Similarly, in the second case,

$$N = 4 \cdot 16^m(8 \cdot 16^m - 1) \equiv 4 \cdot 6(8 \cdot 6 - 1) \equiv 4(8 - 1) \equiv 8 \pmod{10}.$$

Finally, if $n = 2$, $N = 6$, and so we have captured all the possibilities. □

Even perfect numbers exhibit another amazing property, first proven in 1844:

Proposition 14 (Wantzel)**.** *The iterative sum of the digits of an even perfect number (other than* 6*) is one.*

Proof. Let $N = 2^{n-1}(2^n - 1)$. The first claim we establish is that $N \equiv 1 \pmod 9$. Now $n \not\equiv 0 \pmod 3$, for then $3 \mid n$ so n is not prime ($N \neq 6$) and N is not perfect. Hence $N \equiv 1$ or 2 modulo 3. Suppose we have the first case, and $n = 3k + 1$ for some k. Now n is odd, so k is even and we could have written $n = 6k + 1$. Hence

$$N = 2^{6k}(2^{6k+1} - 1) = 64^k(2 \cdot 64^k - 1) \equiv (1)\big(2(1) - 1\big) = 1 \pmod 9.$$

In the second case, $n = 3k + 2$ for some k, so as n is not even, k is odd and $n = 6k + 5$. Thus,

$$N = 2^{6k+4}(2 \cdot 2^{6k+5} - 1) \equiv 16(1)\big(32(1) - 1\big) \equiv (-2)(-4 - 1) = 10 \equiv 1 \pmod 9.$$

The work is now done, for the iterative sum of the digits of a number is merely its congruence class mod 9. For if $N = a_r \ldots a_1 a_0$, where the a_i are digits, then the sum of digits is

$$\sum_{i=1}^{r} a_i 10^i \equiv \sum_{i=1}^{r} a_i 1^i = \sum_{i=1}^{r} a_i \pmod 9.$$

By iterating this sum we get the desired result. □

Historically, there are a number of problems that arise in the investigation of even perfect numbers. For instance, Fermat declared that if n is a prime, then $2^n - 2$ is divisble by $2n$. Of course, this immediately follows from the fact that $2^{n-1} \equiv 1$ modulo n if n is prime by Fermat's little theorem.

Fermat also showed that if n is prime, then $2^n - 1$ is divisible by no prime other than those of the form $2kn + 1$. If $q \mid (2^n - 1)$ for some prime $q \neq 2$, then $2^n \equiv 1$ modulo q. Since we have a power of 2 equal to 1, the identity, the order of 2 divides n; and since n is prime, we have the order just equal to n. But also $n \mid (q - 1)$, the order of the multiplicative group. q is odd so $q - 1$ is even and we have even better that $2n \mid (q - 1)$, or $2nk = q - 1$, and the result follows.

Lucas proved the following: if $p = 8m+7$ is a prime, then $2^{4m+3}-1$ is not. It can be shown that if $p \equiv 1$ or 7 modulo 8 then $2^{p-1} - 1$ is divisible by the same factors

as $2^{(p-1)/2}-1$. In the second case, we have $(p-1)/2=(8m+7-1)/2=4m+3$ so $2^{4m+3}-1$ by Fermat's little theorem is divisible by $p=8m+7$.

4. Mersenne Primes

From the previous section, we know that finding even perfect numbers reduces simply to finding primes of the form 2^n-1, where n is prime. As of 1998, there were 37 known Mersenne primes, summarized in the following table [2]:

Index	**Even Perfect Number**	**Number of Digits**	**Date**
1	6	1	–
2	28	2	–
3	496	3	–
4	8128	4	–
5	33550336	8	1461
6	8589869056	10	1603
7	$2^{18}(2^{19}-1)$	12	1603
8	$2^{30}(2^{31}-1)$	19	1753
9	$2^{60}(2^{61}-1)$	37	1883
10	$2^{88}(2^{89}-1)$	54	1911
11	$2^{106}(2^{107}-1)$	65	1914
12	$2^{126}(2^{127}-1)$	77	1876
13	$2^{520}(2^{521}-1)$	314	1952
14	$2^{606}(2^{607}-1)$	366	1952
	...		...
34	$2^{1257786}(2^{1257787}-1)$	757263	1996
35	$2^{1398268}(2^{1398269}-1)$	841842	1996
36	$2^{2976220}(2^{2976221}-1)$	895932	1997
37	$2^{3021376}(2^{3021377}-1)$	1819050	1998

With each one of these primes, there is a story that goes with its discovery. For instance, Peter Barlow in his *Theory of Numbers* published in 1811, wrote about the eighth perfect number: "It is the greatest that will ever be discovered, for, as they are merely curious without being useful, it is not likely that any person will attempt to find one beyond it."

Quite to the contrary, the latest Mersenne prime was discovered on January 27, 1998 by Roland Clarkson, a 19-year-old student at California State University–Dominguez Hills. Roland used a 200 MHz Pentium computer part-time for 46 days to prove the number prime—he is just one of over 4000 volunteers world-wide participating in the Great Internet Mersenne Prime Search (GIMPS). Indeed, Scott Kurowski, the co-author of software Clarkson used to find this enormous prime, has offered a cash prize to the discoverer of the 38th Mersenne prime. The prize pool is $1.00 for every 1000 digits in the new prime or US $1,000.00, whichever is larger. He says, "If you have a desktop computer, we've got something for it to do between keystrokes and mouse clicks, and many more machines are needed for the next, even larger, prime." More information can be found about this grand quest at `http://www.mersenne.org/prime.htm` [11].

The Mersenne primes appear to be regularly distributed—"ballpark" estimates (meaning within thousands of orders of magnitude) can be given [15], but ultimately these numbers must be checked out one by one.

References

1. Syed Asadulla, *Even perfect numbers and their Euler's function*, Internat. J. Math. Math. Sci. **10** (1987), 409–412.
2. Stanley J. Bezuszka and Margaret J. Kenney, *Even perfect numbers: (update)*^{2}, Math. Teacher **90** (1997), 628–633.
3. R. D. Carmichael, *Multiply perfect numbers of four different primes*, Annals of Math. **8** (1906-1907), 149–158.
4. Graeme L. Cohen, *Even perfect numbers*, Math. Gaz. **65** (1981), 28–30.
5. L. E. Dickson, *Notes on the theory of numbers*, Amer. Math. Monthly **18** (1911), 109.
6. Leonard Eugene Dickson, *History of the theory of numbers, vol. 1*, pp. 3–33, Chelsea Pub. Co., New York, 1971.
7. I.N. Herstein, *Abstract algebra, 3rd ed.*, Prentice-Hall, Upper Saddle River, N.J., 1996.
8. David G. Kendall, *The scale of perfection*, J. Appl. Prob. **19A** (1982), 125–138.
9. J. Knopfmacher, *A note on perfect numbers*, Math. Gazette **44** (1960), 45.
10. Wayne L. McDaniel, *On the proof that all even perfect numbers are of Euclid's type*, Math. Mag. **48** (1975), 107–108.
11. *Mersenne prime search*, `http://www.mersenne.org/prime.htm`, 1998.
12. Ivan Morton Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An introduction to the theory of numbers, 5th ed.*, John Wiley & Sons, Inc., 1991.
13. Oystein Ore, *Number theory and its history*, pp. 91–100, McGraw-Hill, 1948.
14. Ettore Picutti, *Pour l'histoire des sept premiers nombres parfaits*, Historia Math. **16** (1989), 123–136.
15. Manfred R. Schroeder, *Where is the next Mersenne prime hiding?*, Math. Intelligencer **5** (1983), 31–33.
16. Daniel Shanks, *Solved and unsolved problems in number theory, 2nd ed.*, pp. 1–8, 12–15, 18–29, Chelsea Pub. Co., New York, 1978.
17. Stan Wagon, *Perfect numbers*, Math. Intelligencer **7** (1985), 66–68.

Email address: `jvoight@math.berkeley.edu`

Department of Mathematics, University of California, Berkeley