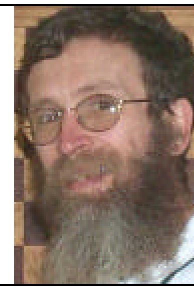
MAA Online

How Euler Did It

by Ed Sandifer



Odd Perfect Numbers

November 2006

The subject we now call "number theory" was not a very popular one in the 18th century. Euler wrote almost a hundred papers on the subject, but the first book to be published on the subject seems to be Legendre's *Essai sur la théorie des nombres*, [L] published during "*an* VI," the sixth year of the of the French Revolutionary calendar, known to the rest of the world as 1798. Gauss's great *Disquisitiones arithmeticae* [G] followed just three years later.

Of course, like many questions people ask in the history of mathematics, if you don't like the answer to a question, you can interpret the question a little differently and get a different answer. Euclid's books VII to IX, [E] for example, are devoted to what we now call number theory. Here we find such essential theorems as the Euclidean Algorithm for finding the greatest common divisor [Book VII prop. 2], the theorem that there are infinitely many prime numbers [Book IX prop. 20] and, as the climax to Book IX, the theorem that if a number of the form $2^n - 1$ is prime, then the number $2^{n-1}\left(2^n - 1\right)$ is what he (and we) call a *perfect* number. [Prop. 36]

A case could also be made that the rare and obscure book *Exercitationum mathematicarum libri quinque*, by Frans van Schooten, [S] published in 1656, was also a number theory book, since van Schooten wrote the book to explain how to find *amicable* numbers. That book did not have the impact van Schooten had hoped. People read his collected works of Viète and his Latin edition of Descartes' *Geometria*, but when they look at his *Exercitationum*, it is usually to read the appendix, *Tractatus de ratiocinis in aleae ludo*, by the young Christian Huygens, and a landmark in the history of probability. That, though, is a topic for another time and place.

It should be no surprise that a case could be made that Euler wrote, but never published, the first number theory textbook. It was a little-known manuscript, *Tractatus de numerorum doctrina capita sedecim quae supersunt*, "Tract on the doctrine of numbers, consisting of sixteen chapters." This is an unfinished first draft of part of what Euler apparently planned to be a textbook on number theory. He certainly did not intend it to be published in this form, and it was only published in 1849, 66 years after his death. We are not sure when Euler wrote it. He probably wrote it after 1756, because it contains results that he published around that time, and most Euler experts agree that he wrote it before he died in 1783, but it is difficult to be more specific than that. André Weil [W] has some thoughts on the subject.

As the title makes clear, the *Tractatus de numerorum* consists of sixteen chapters, the titles of which are listed below:

Ch 1 On the composition of numbers
Ch 2 On the divisors of numbers
Ch 3 On the number of divisors and their sum
Ch 4 On relatively prime numbers and composites
Ch 5 On remainders born of division
Ch 6 On the remainders arising from the division of a the terms of an arithmetic progression
Ch 7 On the remainders arising from the division of terms of a geometric progression
Ch 8 On the powers of numbers which are left by the division by a prime number
Ch. 9 On the divisors of numbers of the form $a^n \pm b^n$
Ch 10 On the remainders arising from the division of squares by prime numbers
Ch 11 On the remainders born of the division of cubes by prime numbers
Ch 12 On the remainders arising from the division of fourth powers (*biquadratorum*) by prime numbers
Ch 13 On the remainders arising from the division of fifth powers (*surdesolidorum* by prime numbers
Ch 14 On the remainders arising from the division of squares by composite numbers
Ch 15 On the divisors of numbers of the form $xx + yy$
Ch 16 On the divisors of numbers of the form $xx + 2yy$

From the titles of the chapters, it appears that Euler's major interest in starting to write this book is to study the prime divisors of certain binary forms. It is likely that he had planned more chapters, perhaps one titled "On the divisors of numbers of the form $xx + nyy$." Euler wrote papers on this and related topics in the 1740's and 1750's. We have devoted earlier columns to two of these papers, one in December 2005 and another in January 2006.

Gauss, [G] in contrast, clearly had different plans when he wrote his *Disquisitiones arithmeticae*. His table of contents shows that he thought that the highlights were the Quadratic Reciprocity Theorem in Chapter 4 and the construction of the 17-gon in Chapter 7. (His preface also suggests that he didn't do all he had planned, as he mentions the contents of a Chapter 8 that doesn't exist.) Alas, I haven't had the chance to study Legendre's book, [L] so I can only guess what he intended.

Back to Euler's book. Euler starts with quite elementary material, giving "definitions" of numbers, arithmetic sequences, multiples, prime numbers, and other basic objects. He takes special care to note that a number na is the nth multiple of the number a, and also the ath multiple of the number n, and that $an = na$. In paragraph 32 (of 586 paragraphs) He tells us that prime numbers are those "numbers that are not multiples of any other number," and includes 1 among the primes when he first lists them, but later in the manuscript, he never seems to treat 1 as a prime.[1] If Euler had ever made a second draft of this manuscript, this is the kind of detail that he certainly would have straightened out.

Euler soon launches into a classification of numbers into the number of (not necessarily distinct) prime factors they have. Prime numbers are of the "first class." Squares and products of two primes are of the "second class," which includes numbers like 4, 6, 9, 10 and 14, but not numbers like 12. Since

[1] I tell my students that the notion of "prime number" came from the ancient Greeks, who did not regard 1 as a number at all. This interpretation survives in modern English usage in our use of the phrase "a number of …" If you ask me "How many sisters do you have?" and I reply, "I have a number of sisters," then you feel I have misled you with word games when you learn that I have only one sister. The phrase "a number of …" usually means "two or more," or even "three or more."

$12 = 2 \cdot 2 \cdot 3$, it is of the third class. He gives us the class (and prime factorization) of every number up to 100, and notes that 64 and 96 are the only numbers less than 100 of the sixth class.

We never do this today, but Euler, as usual, has a good reason and a good idea. He classifies the number of each class into *species*, according to the frequencies of the prime numbers in the prime factorization of a number. A number of the second class, for example, might be of the *first species*, having a form *pp*, like 4 or 9, or it might be of the *second species*, having form *pq*, like 6 or 15. Similarly, the species of the third class are p^3, $p^2 q$ and *pqr*. He surely recognizes, but does not mention, how the number of species of a class is related to the number of partitions of the class number.

We never see such a classification in modern approaches, though something similar occurs both when van Schooten [S] and when Euler do their analyses searching for amicable numbers. Here, though, it makes it easy for Euler to explain that the number of divisors of a number $n = p^l q^m r^n s^x$ will be $(l+1)(m+1)(n+1)(x+1)$. This function is called a *divisor function*[2] and is sometimes denoted either $d(n)$ or $s_o(n)$. [Anon]

From there, it is an easy transition to the topic of Euler's chapter 3, "On the number of divisors and their sum." Euler turns to the sum of the divisors of a number *n*, a sum he denotes using an integral sign, $\int n$, but we now denote either $t(n)$ or $s_1(n)$, the so called "Euler tau function." With Euler's preparation, it is easy for him to show that for powers of prime numbers, $\int p^n = \frac{p^{n+1}-1}{p-1}$, and if we know the prime factorization of a number to be $n = p^l q^m r^n s^x$, then $\int n = \int p^l \int q^m \int r^n \int s^x$.

Euler proves a couple of lemmas about this function, for example that $\int n > n$, and if $n = 1$, then $\int 1 = 1$. Euler is just a little bit confusing here in his use of the ">" sign. We never see Euler using a $\geq$ sign, and here it looks like maybe he should have. He also finds $\int n$ for all *n* up to 60.

Among his lemmas is that if $\frac{\int N}{N} = \frac{m}{n}$, with $\frac{m}{n}$ in lowest terms and *N* not equal to 1, then necessarily $m > n$ and $N = n$.

In paragraph 106 (still part of chapter 3) Euler defines a number *N* to be *perfect* if $\int N = 2N$. This is slightly different from the way Euclid [E] defines perfect numbers. For Euclid, *N* is perfect if it is exactly the sum of its divisors, (not twice that sum), but for Euclid, a number does not *divide* itself, because when you divide *N* into parts each of size *N*, you don't get any parts; you get the whole thing.

[2] *Wikipedia* [Anon] tells us that a *general divisor function* $s_x(n)$ is the sum of the *x*th powers of the divisors of *n*, and can be denoted by $s_x(n) = \sum_{d|n} d^x$.

Euler neglects to point out that among the examples he'd done in earlier paragraphs, he had shown that $\int 6 = 12$ and $\int 28 = 56$, so both 6 and 28 are perfect numbers. Perhaps he would have added this in a later draft of the manuscript, or maybe he expected his readers to notice that. Euler begins to look for perfect numbers.

First, he supposes that N is even, so that $N = 2^n A$, for some power of 2 and some odd number A. Then

$$2^{n+1}A = 2N = \int N = \int 2^n A = \left(2^{n+1} - 1\right)\int A,$$

which makes

$$\frac{\int A}{A} = \frac{2^{n+1}}{2^{n+1} - 1}.$$

On the right, we have a fraction where the numerator is only one more than the denominator, hence it is in lowest terms. By his lemma, $A = 2^{n+1} - 1$, so $\int A = 2^{n+1} = A + 1$ and A is prime. Hence, any *even* perfect number has the form $2^n A$ where $A = 2^{n+1} - 1$ and A is prime. This is the converse to Euclid's Book IX prop. 36, and is the first proof of the converse.

Now we turn to the results that give this column its title, Euler's work on odd perfect numbers. Suppose that N is an odd perfect number and that it factors to be $N = ABCD$etc. Euler implicitly assumes that these factors, A, B, C, D, etc. are powers of distinct primes, though he does not say so explicitly. Since N is odd, all of these factors must be odd, and since the prime factors are distinct, it must be that

$$2N = \int N = \int ABCD \text{ etc.} = \int A \int B \int C \int D \text{ etc.}$$

This number $2N$ is the double of an odd number, what Euler and Euclid called "oddly even" and we would call "congruent to 2 mod 4." Hence, it is divisible by 2 and not by 4, and so among its factors, $\int A$, $\int B$, $\int C$, etc., there must be one that is oddly even, and all the rest must be odd.

Suppose that one of them, say B, has $\int B$ odd, and that $B = p^n$. From what Euler did a long time ago, $\int p^n = \frac{p^{n+1} - 1}{p - 1} = p^n + p^{n-1} + \cdots + p^2 + p + 1$. Since p is odd, this is a sum of $n + 1$ odd numbers. The only way for that the sum to be odd is if $n + 1$ is odd, which forces n to be even. That means that B is an even power of a prime, so that B must be a perfect square.

Hence, all but one of A, B, C, etc., the factors of N, must be perfect squares, and the other one, suppose it is A, has $\int A$ oddly even.

What about this last factor $\int A$? Euler tells us that if we write $A = q^m$, then for $\int A$ to be oddly even, we must have q a prime number of the form $4n + 1$ and also m must be an odd number of the form $4\lambda + 1$. He doesn't tell us exactly why; probably he planned to add the details later. Perhaps we can fill in the gaps.

Odd prime numbers are either of the form $4n + 1$ or $4n + 3$. First, we will show that our number q cannot be of the form $4n + 3$. Suppose that $q = 4n + 3$. Then powers of q alternate between +1 (mod 4) and +3 (mod 4) (though Euler wouldn't use the "mod" notation to say this. That notation is due to Gauss in about 1800). Hence, $\int A = \int q^m = 1 + q + q^2 + \cdots + q^{m-1} + q^m$ is either 1 (mod 4) or 0 (mod 4), depending on whether m is even or odd, respectively. It is never 2 (mod 4), so $\int A$ is never oddly even.

On the other hand, if $q = 4n + 1$, then all powers of q are 1 (mod 4). Then $\int A = \int q^m = 1 + q + q^2 + \cdots + q^{m-1} + q^m$ (mod 4) is equal to the number of terms, that is $m + 1$. That is oddly even exactly when m is 1 (mod 4), or, as Euler said, m is of the form $4\lambda + 1$.

Euler summarizes his result saying that, "an odd perfect number will have the form $(4n+1)^{4l+1} PP$ where P is an odd number and $4n + 1$ is prime.

Since Euler's time, there have been a number of new results about odd perfect numbers, and there a web page devoted to the subject. [OP] The most striking of these is perhaps that there aren't any less than 10^{300}. It is remarkable that we know so much about them, but we still don't know if there are any.

References:

[Anon] Anon., "Divisor function," Wikipedia, http://en.wikipedia.org/wiki/Divisor_function, October 6, 2006.

[E] Euclid, *The Thirteen Books of Euclid's Elements*, 3 vols, translated from the text of Heiberg and annotated by Sir Thomas L. Heath, Cambridge University Press, 1908. Reprinterd by Dover, New York, in various editions.

[E792] Euler, Leonhard, Tractatus de numerorum doctrina capita sedecim quae supersunt, *Commentationes arithmeticae* **2**, 1849, pp. 503-575, reprinted in *Opera Omnia* Series I vol 5 p. 182-283. Available through The Euler Archive at www.EulerArchive.org.

[L] Legendre, Adrien Marie, *Essai sur la théorie des nombres*, Paris, Ches Duprat, an VI [1798]

[G] Gauss, Carl Friedrich, *Disquitiones arithmeticae*, translated by Arthur A. Clarke, Yale University Press, New Haven, 1966, revised by W. Waterhouse, et. al., Springer-Verlag, New York, 1986.

[G+W] Greathouse, Charles and Weisstein, Eric W. "Odd Perfect Number." From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/OddPerfectNumber.html

[OP] OddPerfect.org, October 8, 2006. Under development.

[S] Schooten, Frans van, *Exercitationum mathematicarum libri quinque*, Elsevier, 1656.

[W] Weil, André, *Number theory: an approach through history from Hamurapi to Legendre*, Birkhäuser, Boston, 1984.

Ed Sandifer (SandiferE@wcsu.edu) is Professor of Mathematics at Western Connecticut State University in Danbury, CT. He is an avid marathon runner, with 34 Boston Marathons on his shoes, and he is Secretary of The Euler Society (www.EulerSociety.org). His new book, *The Early Mathematics of Leonhard Euler*, will be published by the MAA in December, 2006, in advance of the celebrations of Euler's tercentennial in 2007.

How Euler Did It is updated each month.