

The Humble Sum of Remainders Function

Michael Z. Spivey
 Samford University
 Birmingham, Alabama 35229
 mzspivey@samford.edu

The sum of divisors function is one of the fundamental functions in elementary number theory. In this note, we shine a little light on one of its lesser-known relatives, the sum of remainders function. We do this by illustrating how straightforward variations of the sum of remainders can 1) provide an alternative characterization for perfect numbers, and 2) help provide a formula for sums of powers of the first n positive integers. Finally, we give a brief discussion of perhaps why the sum of remainders function, despite its usefulness, is less well known than the sum of divisors function.

Some notation is in order. The standard notation for the sum of divisors function is $\sigma(n)$:

$$\sigma(n) = \sum_{d|n} d.$$

We denote the sum of remainders function by $\rho(n)$, namely,

$$\rho(n) = \sum_{d=1}^n n \bmod d.$$

Sums of remainders and perfect numbers A *perfect number* is a number equal to the sum of its positive divisors excluding itself. Another way to express this is that perfect numbers are those such that $\sigma(n) = 2n$. The three smallest perfect numbers are 6, 28, and 496. Euclid proved that every number of the form $2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are prime, is perfect. Euler proved the converse, that numbers of this form are the only even perfect numbers [3, p. 59]. One of the famous unsolved problems in number theory is whether or not there are any odd perfect numbers.

To see the connection between the sum of remainders and perfect numbers, let's take a look at what $\rho(n)$ is actually adding up. A table of remainders for $n = 15$ is as follows:

divisor: d	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$15 \bmod d$	0	1	0	3	0	3	1	7	6	5	4	3	2	1

Two patterns are fairly immediate: There are zeros in the entries for which d divides n , and once past half of 15, the remainders count down from 7 (just under half of 15) to 1. Other than that, there does not appear to be much of a pattern.

However, if we juxtapose the remainders for several consecutive integers we start to see a pattern:

divisor: d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$1 \bmod d$	0														
$2 \bmod d$	0	0													
$3 \bmod d$	0	1	0												
$4 \bmod d$	0	0	1	0											
$5 \bmod d$	0	1	2	1	0										
$6 \bmod d$	0	0	0	2	1	0									
$7 \bmod d$	0	1	1	3	2	1	0								
$8 \bmod d$	0	0	2	0	3	2	1	0							
$9 \bmod d$	0	1	0	1	4	3	2	1	0						
$10 \bmod d$	0	0	1	2	0	4	3	2	1	0					
$11 \bmod d$	0	1	2	3	1	5	4	3	2	1	0				
$12 \bmod d$	0	0	0	0	2	0	5	4	3	2	1	0			
$13 \bmod d$	0	1	1	1	3	1	6	5	4	3	2	1	0		
$14 \bmod d$	0	0	2	2	4	2	0	6	5	4	3	2	1	0	
$15 \bmod d$	0	1	0	3	0	3	1	7	6	5	4	3	2	1	0
$16 \bmod d$	0	0	1	0	1	4	2	0	7	6	5	4	3	2	1
$17 \bmod d$	0	1	2	1	2	5	3	1	8	7	6	5	4	3	2
$18 \bmod d$	0	0	0	2	3	0	4	2	0	8	7	6	5	4	3

For fixed d and increasing n , $n \bmod d$ cycles from 0 to $d - 1$, hitting 0 at all the integers that d divides. This makes sense, of course, when you think about it.

In particular, if we compare $n \bmod d$ and $(n - 1) \bmod d$, we see that the difference between them is either 1, if d does not divide n , or $1 - d$, if d does divide n . In symbols, this becomes:

$$n \bmod d - (n - 1) \bmod d = \begin{cases} 1, & \text{if } d \nmid n, \\ 1 - d, & \text{if } d \mid n. \end{cases} \quad (1)$$

Now, define the *backward difference operator* ∇ by $\nabla f(n) = f(n) - f(n - 1)$. Then the connection between the sum of remainders and perfect numbers is the following:

THEOREM 1. n is perfect if and only if $\nabla \rho(n) = -1$.

Proof. Summing up the left-hand side of the equation in (1) over d from 1 to $n - 1$ yields $\rho(n) - \rho(n - 1)$. The sum of the right-hand side of the equation in (1) over d from 1 to $n - 1$ can be split into the sum over those d that do not divide n and the sum over those that do. Setting the two expressions equal to each other yields

$$\begin{aligned} \rho(n) - \rho(n - 1) &= \sum_{d \nmid n} 1 + \sum_{d \mid n, d \neq n} (1 - d) = \sum_{d=1}^{n-1} 1 - \sum_{d \mid n, d \neq n} d \\ &= n - 1 - \sum_{d \mid n} d + n = 2n - 1 - \sigma(n). \end{aligned}$$

Since a number is perfect if and only if $\sigma(n) = 2n$, the theorem follows. \blacksquare

Theorem 1 is a surprisingly simple characterization of perfect numbers in terms of the sum of remainders. The theorem is proved by Cross [1] and by Lucas [8, p. 374]. (Cross's reference to p. 388 in Lucas is in error.)

The proof of Theorem 1 also implies simple characterizations of numbers that are close to being perfect. Define an *almost perfect* number to be a number n such that $\sigma(n) = 2n - 1$. Powers of 2 are almost perfect, but these are the only numbers known

to be almost perfect. Define a *quasi-perfect* number to be a number n such that $\sigma(n) = 2n + 1$. It is not known if there are any quasi-perfect numbers, but it is known that they must be odd squares [5]. Slight modifications of the proof of Theorem 1 then yield

COROLLARY 1. *We have the following:*

- n is almost perfect if and only if $\nabla\rho(n) = 0$.
- n is quasi-perfect if and only if $\nabla\rho(n) = -2$.

This can go on, of course, for other numbers that are close to being perfect.

There is another interesting corollary to Theorem 1. Calculus, as any freshman math major knows, involves derivatives and integrals of functions defined over real numbers. Calculus can also be done with discrete functions, functions defined over, say, the integers. In this case it is known as *finite calculus*. The discrete analog of the derivative is the *finite difference*:

$$\Delta f(n) = f(n+1) - f(n).$$

And the discrete analog of the antiderivative is the *antidifference*:

$$\Delta^{-1}f(n) \text{ is any function } F \text{ such that } \Delta F = f.$$

With finite calculus in mind, we see that the proof of Theorem 1 says that the finite difference of $\rho(n)$ is $2n + 1 - \sigma(n + 1)$, or, alternatively, that an antidifference of $\sigma(n)$ is $(n - 1)^2 - \rho(n - 1)$. Thus the ρ and σ functions are related to each other in a simple way via finite calculus. We are not aware of any other basic number-theoretic functions for which this is the case.

Sums of remainders and power sums For various integers k , the sums of k th powers of the first n positive integers, $1^k + 2^k + \cdots + n^k$, have got to be some of the most popular sums in all of mathematics. The study of these sums led Jakob Bernoulli to develop the numbers later named in his honor. In addition to formulas using these Bernoulli numbers, there are formulas involving Eulerian numbers and binomial coefficients, as well as Stirling numbers and binomial coefficients [10]. Many other papers have appeared on the subject [7, 9].

The promised formula for the power sum using remainders involves variations of both ρ and σ . Recall that the value of $\sigma(n)$ is determined by summing the divisors of n . Besides summing the divisors, however, we can also sum up powers of the divisors; that is, squares, cubes, or even any real powers. The standard notation is

$$\sigma_k(n) = \sum_{d|n} d^k.$$

Results concerning this function are scattered throughout Chapter X of Dickson [3]; other problems, some solved and some unsolved, appear in books by Dudley [4, p. 56] and Guy [5, pp. 102–105].

We could also sum powers of the remainders. However, for our purposes we need remainders that are *weighted* by powers of integers; namely, multiply $n \bmod d$ by d^k and then add up. This leads to the following definition:

$$\rho(n, k) = \sum_{d=1}^n d^k (n \bmod d).$$

Then the formula for the power sum in terms of $\sigma_k(n)$ and $\rho(n, k)$ is

THEOREM 2. For any real number k ,

$$1^k + 2^k + \cdots + n^k = \frac{1}{n} \left(\rho(n, k) + \sum_{i=1}^n \sigma_{k+1}(i) \right).$$

A nice property of Theorem 2 is that k can be any real number; most other formulas for the power sum restrict k to the nonnegative integers.

Two special cases of Theorem 2 are worth mentioning. If $k = 0$, we have the nice formula

$$n^2 = \rho(n) + \sum_{i=1}^n \sigma(i),$$

which appears in Lucas [8, p. 388]. This formula can also be derived easily from the proof of Theorem 1. In addition, the case $k = -1$ can be rewritten as

$$\sum_{i=1}^n \lfloor n/i \rfloor = \sum_{i=1}^n d(i),$$

where $d(i)$ gives the number of divisors of the integer i . This result is discussed in the proof of Theorem 320 in Hardy and Wright [6].

Before we prove Theorem 2, though, we need to define the *indicator function* $1_{\{p\}}$ for the statement p . This is given by the following:

$$1_{\{p\}} = \begin{cases} 1, & \text{if } p \text{ is true,} \\ 0, & \text{if } p \text{ is false.} \end{cases}$$

Let us proceed to prove Theorem 2.

Proof. The division algorithm tells us that, for any integers n and d , $n = dq_d + r_d$, where q_d is the quotient and r_d is the remainder when n is divided by d . Multiplying both sides of this equation by d^k and summing over d from 1 to n yields the following:

$$\begin{aligned} n \sum_{d=1}^n d^k &= \sum_{d=1}^n (d^{k+1} q_d + d^k r_d) \\ &= \sum_{d=1}^n d^{k+1} q_d + \rho(n, k). \end{aligned} \tag{2}$$

At this point we can start to see the formula becoming clear. All that remains is to show that $\sum_{d=1}^n d^{k+1} q_d = \sum_{i=1}^n \sigma_{k+1}(i)$. To see this, we need the fact that q_d counts the number of integers between 1 and n that d divides evenly. For example, 37 divided by 7 leaves a quotient of 5; this is because 7 divides exactly five integers between 1 and 37: 7, 14, 21, 28, and 35. Therefore,

$$\begin{aligned} \sum_{d=1}^n d^{k+1} q_d &= \sum_{d=1}^n d^{k+1} \sum_{i=1}^n 1_{\{d|i\}} = \sum_{i=1}^n \sum_{d=1}^n d^{k+1} 1_{\{d|i\}} \\ &= \sum_{i=1}^n \sum_{d|i} d^{k+1} = \sum_{i=1}^n \sigma_{k+1}(i). \end{aligned}$$

Substituting this expression into (2) and dividing both sides of the equation by n yields the formula.

Some limitations of the sum of remainders function With these uses of the sum of remainders function, why is it so little known relative to the sum of divisors function? While some of the answer may be historical, much of it also lies in the fact that ρ does not have some of the nice properties that σ has, properties that σ shares with other well-known arithmetical functions.

For example, ρ is not multiplicative, whereas σ is. Multiplicative arithmetical functions f are those that are not identically zero and that have the property that $f(mn) = f(m)f(n)$ whenever m and n are relatively prime. This property means that the values of multiplicative functions are completely determined by their behavior on the primes. It is easy to see that ρ is not multiplicative; for example, $\rho(2) = 0$, but not every even number n has $\rho(n) = 0$. Dudley [4, p. 54] gives a proof that σ is multiplicative.

Another nice property that σ has but ρ does not is that σ is a unit in the standard ring of arithmetical functions. (Recall that the units in a ring are the elements that have multiplicative inverses.) In a recent article in this MAGAZINE, Delaney [2] characterizes the units in this ring. He also gives a formula for σ as the Dirichlet product of two simple functions, and one can use his subsequent discussion to construct the inverse of σ . Again, it is easy to see that ρ has no inverse. The multiplicative identity in the ring is the indicator function $1(n) = I_{\{n=1\}}$, and since $\rho(1) = 0$, ρ can have no inverse. (Further details on the ring of arithmetical functions can be found in Delaney's paper [2].)

Final remarks We have seen that the sum of remainders function ρ can provide a simple alternative characterization for perfect numbers, and, in conjunction with a variation of the sum of divisors function, give a new formula for sums of powers. We have also seen that the sum of remainders function does not have two nice properties that many more well-known arithmetical functions do have, namely, ρ is not multiplicative, and ρ is not a unit in the standard ring of arithmetical functions.

The interested reader may enjoy framing his own questions concerning the sum of remainders function. There is not a lot of literature available on the subject.

REFERENCES

1. James T. Cross, A note on almost perfect numbers, this MAGAZINE, **47** (1974), 230–231.
2. James E. Delaney, Groups of arithmetical functions, this MAGAZINE, **78** (2005), 83–95.
3. Leonard E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1952.
4. Underwood Dudley, *Elementary Number Theory*, W. H. Freeman, New York, 2nd ed., 1978.
5. Richard K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 3rd ed., 2004.
6. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 5th ed., 1979.
7. Donald E. Knuth, Johann Faulhaber and sums of powers, *Mathematics of Computation*, **61** (1993), 277–294.
8. Édouard Lucas, *Théorie des Nombres*, Gauthier-Villars, Paris, 1891.
9. Robert W. Owens, Sums of powers of integers, this MAGAZINE, **65** (1992), 38–40.
10. Kenneth H. Rosen, ed., *Handbook of Discrete and Combinatorial Mathematics*, CRC Press, Boca Raton, FL, 2000.