A RECURSIVELY DEFINED DIVISOR FUNCTION

MICHAEL D. MILLER
University of California, Los Angeles, California 90024

INTRODUCTION

In this paper, we shall investigate the properties of a recursively defined number-theoretic function γ, paying special attention to its fixed points. An elementary acquaintance with number theory and linear recurrence relations is all that is required of the reader.

Throughout the discussion, $p, q, r, s, t, p_1, p_2, \cdots$ will denote prime numbers.

THE FUNCTION γ

We define a function γ on the positive integers by setting $\gamma(1) = 1$, and for $N > 1$,

$$\gamma(N) = \sum_{d \mid N, d<N} \gamma(d).$$

Example 1:

(1) If p is prime, $\gamma(p) = 1$.

(2) $\gamma(4) = \gamma(1) + \gamma(2) = 2$.

(3) $\gamma(12) = \gamma(1) + \gamma(2) + \gamma(3) + \gamma(4) + \gamma(6) = \gamma(1) + \gamma(2) + \gamma(3) + [\gamma(1) + \gamma(2)] + [\gamma(1) + \gamma(2) + \gamma(3)] = 8.$

The following theorem clearly follows from the definition of γ.

Theorem 1. $\gamma(N)$ depends only on the structure of the prime factorization of N.

That is, if $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_h^{\alpha_h}$, $\gamma(N)$ is independent of the particular primes p_i, and depends only on the set $a_1, a_2, \cdots, a_h$ of exponents. For example, $\gamma(12) = \gamma(20) = \gamma(75)$ since 12, 20, and 75 are each of the form p^2q.

By actually determining the divisors of N, we obtain the following results:

N	$\gamma(N)$	N	$\gamma(N)$	N	$\gamma(N)$
p	1	p^4	8	p^4q	48
p^2	2	p^3q	20	p^3q^2	76
pq	3	p^2q^2	26	p^3qr	132
p^3	4	p^2qr	44	p^2q^2r	176
p^2q	8	$pqrs$	75	p^2qrs	308
pqr	13	p^5	16	$pqrst$	541

If $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_h^{\alpha_h}$, we define the *exponent* of N to be

$$\sum_{i=1}^{h} a_i .$$

We now derive expressions for $\gamma(N)$ in a few simple cases, and then proceed to determine the general form.

Theorem 2. $$\gamma(p^n) = 2^{n-1}.$$

Proof. For $n = 1$, the theorem clearly holds. Assume it true for $n = k$. Thus $\gamma(p^k) = 2^{k-1}$. Now,

$$\gamma(p^{k+1}) = \gamma(1) + \gamma(p) + \cdots + \gamma(p^k) = 2\gamma(p^k) = 2^k,$$

since

$$\gamma(1) + \gamma(p) + \cdots + \gamma(p^{k-1}) = \gamma(p^k).$$

Theorem 3. $$\gamma(p^n q) = (n+2)\cdot 2^{n-1}.$$

Proof. $\gamma(p^n q) = \gamma(1)+\gamma(p)+\cdots+\gamma(p^{n-1})+\gamma(q)+\gamma(pq)+\cdots+\gamma(p^{n-1}q)+\gamma(p^n) = 2\gamma(p^{n-1}q)+\gamma(p^n).$ Let $a_n = \gamma(p^n q)$. Then

$$a_n - 2a_{n-1} = \gamma(p^n) = 2^{n-1}.$$

We solve this linear recurrence (using the fact that $a_0 = 1$) to obtain the desired result.

Before proceeding, it will be valuable to make the following observation. If $N = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\cdots\cdot p_h^{\alpha_h}$, then

$$\gamma(N) = \sum_{d|N, d<N} \gamma(d)$$

is a sum involving two types of terms: those involving divisors of N which have $p_1^{\alpha_1}$ as a factor, and those which do not. The sum of all terms of the latter type we recognize as $2\gamma(p_1^{\alpha_1-1}\cdot p_2^{\alpha_2}\cdot\cdots\cdot p_h^{\alpha_h})$. Each of the remaining terms is of the form $\gamma(p^n d)$, where d properly divides $p_2^{\alpha_2}\cdot\cdots\cdot p_h^{\alpha_h}$. Moreover, in each case, d has lower exponent than that of $N/p_1^{\alpha_1}$.

This observation leads us to a proof by induction on the exponent of N in order to find an expression for $\gamma(N)$. We first look at the following example.

Example 2. $$\gamma(p^n q^2) = 2\gamma(p^{n-1}q^2)+\gamma(p^n)+\gamma(p^n q).$$

Using Theorems 2 and 3, and letting $a_n = \gamma(p^n q^2)$, we rewrite this equation as

$$a_n - 2a_{n-1} = 2^{n-1} + (n+2)2^{n-1}.$$

Noting that $a_0 = \gamma(q^2) = 2$, we solve to find $a_n = (n^2+7n+8)2^{n-2}$.

Using this example and observation as motivation, we now derive the general form of $\gamma(N)$ for any N.

Theorem 4. Let

$$A_n = p_1^n\cdot p_2^{\alpha_2}\cdot\cdots\cdot p_h^{\alpha_h},$$

where $\alpha_2, \alpha_3, \cdots, \alpha_h$ are fixed. Then

$$\gamma(A_n) = P(n)\cdot 2^n,$$

where $P(n)$ is a polynomial in n of degree $e = \alpha_2 + \cdots + \alpha_h$ with positive leading coefficient.

Proof. We shall use induction on e. For $e = 0$, we have

$$A_n = p_1^n \quad \text{and} \quad \gamma(A_n) = 2^{n-1} = \tfrac{1}{2}\cdot 2^n$$

by Theorem 2. Now assume the theorem true for $e < k$, and look at $B_n = p_1^n\cdot C$, where C is of exponent k, and p_1 does not divide C. By an earlier observation,

$$\gamma(B_n) - 2\gamma(B_{n-1}) = \sum_{i=1}^{m} \gamma(p_1^n d_i),$$

where $d_1, d_2, \cdots, d_m$ are the proper divisors of C. Now each such proper divisor d_i of C in the summation is of exponent less than k. Thus, by the inductive hypothesis, we can rewrite the right-hand side as

$$\sum_{i=1}^{m} P_i(n)\cdot 2^n = P^*(n)\cdot 2^n,$$

where $P_i(n)$ is a polynomial of degree the exponent of d_i, and $P^*(n)$ is a polynomial of degree $k-1$ with positive leading coefficient.

Now let $a_n = \gamma(B_n)$. We thus have a non-homogeneous linear recurrence $a_n - 2a_{n-1} = P^*(n)\cdot 2^n$. We try a particular solution of the form $a_n = Q(n)\cdot 2^n$, where $Q(n)$ is a polynomial of degree k. Hence we need

$$Q(n)\cdot 2^n - 2Q(n-1)\cdot 2^{n-1} = P^*(n)\cdot 2^n,$$

or $Q(n) - Q(n-1) = P^*(n)$. This will always have a solution $Q(n)$, of degree k, with positive leading coefficient. Thus $Q(n)\cdot 2^n$ is indeed a particular solution to the above recurrence relation. The general solution is therefore

$$a_n = c\cdot 2^n + Q(n)\cdot 2^n = 2^n(c + Q(n)),$$

where c is a constant. The theorem is proved.

This theorem, although giving much information about the nature of the function γ, does not explicitly give us a formula from which we can calculate $\gamma(N)$ for various values of N. However, it does tell us that once we know $\gamma(p^n d)$ for d with exponent less than k, we can find $\gamma(p^n d^*)$ with d^* of exponent k by solving a relatively simple (yet most times tedious) difference equation.

Doing this for a few simple cases, we obtain the following results:

N	$\gamma(N)$
p^n	2^{n-1}
$p^n q$	$(n+2)\cdot 2^{n-1}$
$p^n q^2$	$\frac{n^2+7n+8}{2}\cdot 2^{n-1}$
$p^n q^3$	$\frac{n^3+15n^2+56n+48}{6}\cdot 2^{n-1}$
$p^n qr$	$(n^2+6n+6)\cdot 2^{n-1}$
$p^n q^2 r$	$\frac{n^3+13n^2+42n+32}{2}\cdot 2^{n-1}$
$p^n qrs$	$(n^3+12n^2+36n+26)\cdot 2^{n-1}$

Theorem 5. $\gamma(N)$ is odd if and only if N is a product of distinct primes.

Proof. Recall the definition of γ: $\gamma(1) = 1$, and

$$\gamma(N) = \sum_{d|N,d<N} \gamma(d)$$

for $N > 1$. We cannot directly apply the Mobius inversion formula to γ, since the latter equation does not hold for $N = 1$. We thus introduce an auxiliary function η defined as follows:

$$\eta(N) = \begin{cases} 1 \text{ if } N = 1 \\ 0 \text{ otherwise} \end{cases}.$$

Then, for all positive integers N, we have

$$\gamma(N) = \sum_{d|N,d<N} \gamma(d) + \eta(N), \quad \text{or} \quad 2[\gamma(N) - \eta(N)] = 2\sum_{d|N,d<N} \gamma(d) = \sum_{d|N} \gamma(d) - \eta(N).$$

Let $F(N) = 2\gamma(N) - \eta(N)$. We can now apply the Mobius inversion formula to $F(N)$ to find that

$$\gamma(N) = \sum_{d|N} \mu(N/d)F(d) = 2\sum_{d|N} \mu(N/d)\gamma(d) - \sum_{d|N} \mu(N/d)\eta(d) = 2\gamma(N) + 2\sum_{d|N,d<N} \mu(N/d)\gamma(d) - \mu(N).$$

From this, we deduce that

$$\gamma(N) = \mu(N) - 2\sum_{d|N,d<N} \mu(N/d)\gamma(d).$$

Clearly, $\gamma(N)$ is odd if and only if $\mu(N) \neq 0$, that is, if and only if N is a product of distinct primes.

SUPER-PERFECT NUMBERS

We will call a positive integer $N > 1$ *super-perfect* if $\gamma(N) = N$.

Theorem 6. p^n is never super-perfect.

Proof. In order for p^n to be super-perfect, we would need $p^n = 2^{n-1}$, by Theorem 2. This forces $p = 2$, and thus a contradiction.

The following theorem assures us of the existence of infinitely many super-perfect numbers.

Theorem 7. $p^n q$ is super-perfect if and only if $p = 2$ and $n + 2 = 2q$.

Proof. By Theorem 3, for p^nq to be super-perfect, we need $(n+2)2^{n-1} = p^nq$. If $n > 2$, we must then have $p = 2$, and after cancellation, we get $n+2 = 2q$, as required. For $n = 0, 1$, or 2, the equation leads to a contradiction.

Since p and q are distinct, the first q and n for which $n+2 = 2q$ are $q = 3$ and $n = 4$, which gives $2^4 \cdot 3 = 48$ as the first super-perfect number of this form. As it turns out, it is the only super-perfect number less than 1000.

q	n	$N = p^nq \quad (p = 2)$
3	4	48
5	8	1280
7	12	28672
11	20	11534336

Theorem 8. $N = p^nq^2$ is never super-perfect.

Proof. From Example 2, we know that

$$\gamma(p^nq^2) = (n^2+7n+8)\cdot 2^{n-2}.$$

Assume that

$$p^nq^2 = (n^2+7n+8)\cdot 2^{n-2}.$$

For $n > 4$, this forces $p = 2$, which leads to $(2q)^2 = n^2+7n+8$. However, we clearly have the inequality

$$(n+3)^2 < n^2+7n+8 < (n+4)^2 \quad \text{for} \quad n > 4.$$

Thus no solution exists in this case. If $n = 0, 1, 2, 3$, or 4, we get $p^nq^2 = 2, 8, 26, 76, 208$, respectively, none of which are possible.

The following theorems are stated without proof, for the proofs follow the same patterns as above.

Theorem 9. $N = p^nq^3$ is never super-perfect.

Theorem 10. $N = p^nqr$ is super-perfect if and only if $p = 2$, and $2qr = n^2+6n+6$.

q	r	n	$N = p^nqr \quad (p = 2)$
13	3	6	2496
37	3	12	454656
13	11	14	2342912
73	3	18	57409536

In all cases, we are faced with trying to find values for n which make a given polynomial in n have a certain prime factorization structure. This is, in general, a very difficult, and in most cases, an unsolved problem.

ODD SUPER-PERFECT NUMBERS

Recall from Theorem 5 that $\gamma(N)$ is odd only when N is a product of distinct primes. We now use various combinatorial methods to prove:

Theorem 11. There are no odd super-perfect numbers.

Proof. Suppose that $p_1, p_2, \cdots$ are distinct primes. Let $a_0 = 1$ and $a_i = \gamma(p_1p_2\cdot\cdots\cdot p_i)$, $i = 1, 2, \cdots$. Using Theorem 1 to consolidate terms, we find that

$$a_n = \binom{n}{0}a_0 + \binom{n}{1}a_1 + \cdots + \binom{n}{n-1}a_{n-1} = \sum_{i=0}^{n-1}\binom{n}{i}a_i.$$

Then

$$\frac{a_n}{n!} = \sum_{i=0}^{n-1}\frac{a_i}{i!(n-i)!}.$$

Let

$$b_n = \frac{a_n}{n!} \quad \text{and} \quad b(x) = \sum_{i=0}^{\infty} b_ix^i.$$

We thus have

$$b(x)\cdot e^x = \sum_{i=0}^{\infty} b_i x^i \cdot \sum_{j=0}^{\infty} \frac{x^j}{j!} = b_0 + \sum_{n=1}^{\infty} \sum_{i+j=n} \frac{b_i}{j!} x^n = b_0 + \sum_{n=1}^{\infty} \left(\sum_{i=0}^{n-1} \frac{b_i}{(n-i)!} + b_n \right) x^n = 2b(x) - b_0$$

But $a_0 = b_0 = 1$, so we solve to find that

$$b(x) = \frac{1}{2-e^x} = \tfrac{1}{2}\left(1 + \frac{e^x}{2} + \frac{e^{2x}}{4} + \frac{e^{3x}}{8} + \cdots\right).$$

We now expand each term in the infinite sum in powers of x, and then collect coefficients to obtain

$$b(x) = \tfrac{1}{2} \sum_{n=0}^{\infty} \sum_{i=0}^{\infty} \frac{i^n}{2^i n!} x^n \qquad (0^0 = 1).$$

Thus

$$b_n = \tfrac{1}{2} \sum_{i=0}^{\infty} \frac{i^n}{2^i n!} \quad \text{and} \quad a_n = \tfrac{1}{2} \sum_{i=0}^{\infty} \frac{i^n}{2^i}.$$

In order to proceed, we need the following lemma.

Lemma. For fixed k,

$$f_k(x) = \sum_{n=0}^{\infty} n^k x^n$$

converges for $|x| < 1$, and is equal to

$$\frac{P_k(x)}{(1-x)^{k+1}},$$

where $P_k(x)$ is a monic polynomial of degree k with non-negative coefficients.

Proof. The convergence part of the lemma follows immediately from the ratio test. For $k = 0$, we have

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x},$$

so the lemma holds. Assume it true for $k = s$. Thus

$$f_s(x) = \sum_{n=0}^{\infty} n^s x^n = \frac{P_s(x)}{(1-x)^{s+1}}.$$

Now

$$f_{s+1}(x) = x f_s'(x) = \sum_{n=0}^{\infty} n^{s+1} x^n = \frac{x(1-x)^{s+1} P_s'(x) + x(s+1)P_s(x)(1-x)^s}{(1-x)^{2s+2}} = \frac{x(1-x)P_s'(x) + x(s+1)P_s(x)}{(1-x)^{s+2}}.$$

It is straightforward to verify that the numerator is indeed a monic polynomial of degree $s+1$ with non-negative coefficients. The lemma follows.

Putting $x = \tfrac{1}{2}$ in the lemma, we find that

$$a_k = \tfrac{1}{2} \sum_{n=0}^{\infty} \frac{n^k}{2^n} = \frac{\tfrac{1}{2} P_k(\tfrac{1}{2})}{(\tfrac{1}{2})^{k+1}} = 2^k P_k(\tfrac{1}{2}).$$

Using the fact that $P_0(x) = 1 = 0!$, we can show (via a simple induction argument) that the sum of the coefficients of $P_k(x)$ is $k!$. Since $P_k(\tfrac{1}{2}) < P_k(1)$, we clearly have $a_k < 2^k k!$.

Comparing $2^k k!$ with the product

$$\prod_{i=1}^{k} p_i$$

of the first k odd primes, we see that $k = 1$ is the lowest k for which

$$2^k k! < \prod_{i=1}^{k} p_i .$$

But once this inequality holds for one k, it holds for all larger k. For by multiplying each side by $2(k+1)$, we get

$$2^{k+1}(k+1)! < \prod_{i=1}^{k} p_i \cdot 2(k+1) < \prod_{i=1}^{k+1} p_i ,$$

since $p_{k+1} > 2(k+1)$.

Therefore, for all k,

$$a_k < \prod_{i=1}^{k} p_i ,$$

and in particular, a_k is less than any product of k distinct odd primes. We conclude that no product of distinct odd primes can be super-perfect, and the theorem follows.

****

SIGNIFICANCE OF EVEN-ODDNESS OF A PRIME'S PENULTIMATE DIGIT

WILLIAM RAYMOND GRIFFIN
Dallas, Texas

By elementary algebra one may prove a remarkable relationship between a prime number's penultimate (next-to-last) digit's even-oddness property and whether or not the prime, p, is of the form $4n + 1$, or $p \equiv 1 \pmod 4$, or of the form $4n + 3$, or $p \equiv 3 \pmod 4$, where n is some positive integer.

The relationships are as follows:

A. Primes $\equiv 1 \pmod 4$
   (1) If the prime, p, is of the form $10k \pm 1$, k being some positive integer, then the penultimate digit is *even.*
   (2) If p is of the form $10k \pm 3$, then the penultimate digit is *odd.*

B. Primes $\equiv 3 \pmod 4$
   (1) If p is of the form $10k \pm 1$, then the penultimate digit is *odd.*
   (2) If p is of the form $10k \pm 3$, then the penultimate digit is *even.*

The beauty of these relationships is that, by inspection *alone,* one may instantly observe whether or not a prime number is $\equiv 1$, or $\equiv 3 \pmod 4$. These relationships are especially valuable for very large prime numbers—such as the larger Mersenne primes.

Thus, it is seen from inspection of the penultimate digits of the Mersenne primes, as given in [1], that all of the given primes are $\equiv 3 \pmod 4$. This holds true for *all* Mersenne primes, however large they may be, for, by adding and subtracting 4 from $M_p = 2^p - 1$ and re-arranging, we have

$$M_p = 2^p - 1 + 4 - 4 = 2^p - 4 + 3 = 4(2^{p-2} - 1) + 3 \equiv 3 \pmod 4.$$

[Continued on Page 208.]