Journal of Integer Sequences, Vol. 6 (2003),
Article 03.2.7

Further Results on Derived Sequences

Kevin G. Hare[1] and Soroosh Yazdani[2]
Department of Mathematics
970 Evans Hall
University of California
Berkeley, CA 94720-3840
USA
kghare@math.berkeley.edu
syazdani@math.berkeley.edu

Abstract

In 2003 Cohen and Iannucci introduced a multiplicative arithmetic function D by assigning $D(p^a) = ap^{a-1}$ when p is a prime and a is a positive integer. They defined $D^0(n) = n$ and $D^k(n) = D(D^{k-1}(n))$ and they called $\{D^k(n)\}_{k=0}^{\infty}$ the derived sequence of n. This paper answers some open questions about the function D and its iterates. We show how to construct derived sequences of arbitrary cycle size, and we give examples for cycles of lengths up to 10. Given n, we give a method for computing m such that $D(m) = n$, up to a square free unitary factor.

1. Introduction and Results

Cohen and Iannucci [1] introduced a multiplicative arithmetic function D by assigning $D(p^a) = ap^{a-1}$ when p is a prime and a is a positive integer. They defined $D^0(n) = n$ and $D^k(n) = D(D^{k-1}(n))$ and they called $\{D^k(n)\}_{k=0}^{\infty}$ the derived sequence of n. Cohen and Iannucci showed that for all $n < 1.5 \times 10^{10}$ the derived sequences are bounded. Moreover, they showed that the set of n where the derived sequence of n is bounded has a density of at least 0.996. Bounded sequences effectively end in a cycle. Although Cohen and Iannucci found only cycles of lengths 1 to 6, and 8, they conjectured the existence of cycles of any order. This paper gives a constructive proof for the existence of cycles of any order.

Given n, an integer m such that $D(m) = n$ is referred to as a value of $D^{-1}(n)$, and m is called canonical if it has no square free unitary factor. (A factor d of n is unitary if

[1]Research of K. G. Hare supported, in part by NSERC of Canada, and by the Department of Mathematics, University of California, Berkeley.

[2]Research of S. Yazdani supported, in part by NSERC of Canada, and by the Department of Mathematics, University of California, Berkeley.

$\gcd(d, n/d) = 1$ and square free if $p^2 \nmid d$ for any prime p.) We give a method for computing canonical values of $D^{-1}(n)$ and we give an example where $D^{-1}(n)$ has at least 2^{7101} different canonical values.

2. Cycles of arbitrary order

We say that the derived sequence has a cycle of order $r > 0$ if for sufficiently large k we have $D^{k+r}(n) = D^k(n)$ and r is minimal.

For example, we see that the derived sequence of $n = 4$ is

$$\{2^2,\ 2^2,\ 2^2,\ \cdots\}$$

and hence this has a cycle of order 1. Considering the derived sequence of $n = 16$ gives

$$\{2^4,\ 2^5,\ 5\cdot 2^4,\ 2^5,\ 5\cdot 2^4,\ \cdots\}$$

and hence this has a cycle of order 2.

First we introduce some notation: Let $\bar{p} = [p_1, p_2, \cdots, p_k]$ and $\bar{a} = [a_1, a_2, \cdots, a_k]$. Then we use the notation

$$\bar{p}^{\bar{a}} := p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}.$$

Here we show how to create a cycle of arbitrary order. First we need a lemma:

Lemma 2.1. *Let k be odd. Let $\gcd(a, k)$ and $\gcd(b, k)$ be square free. Then there exists an n such that $a + kn$ and $b + kn$ are both square free.*

Proof. We do this by showing that the set of n with the property that $a + kn$ and $b + kn$ are square free has positive density. For a subset $U \subset \mathbb{N}$, let

$$\text{Density}(U) = \lim_{n\to\infty} \frac{\#\{x \in U : x < n\}}{n}.$$

For p prime, define:

$$R_p := \{n \in \mathbb{N} : a + kn \not\equiv 0 \pmod{p^2} \text{ and } b + kn \not\equiv 0 \pmod{p^2}\}$$

and $S_p = \text{Density}(R_p)$.

If $p|k$ then S_p either equals 1, $1 - \frac{1}{p}$, or $1 - \frac{2}{p}$. (It is worth remarking here that if k is even, and we took $p = 2$ then $1 - \frac{2}{p} = 0$, and hence positive density is not necessarily shown.) If $p \nmid k$ then S_p either equals $1 - \frac{1}{p^2}$ or $1 - \frac{2}{p^2}$. Let

$$\begin{aligned} R &= \{n \in \mathbb{N} : a + kn \text{ and } b + kn \text{ are square free }\} \\ &= \bigcap_{p \text{ prime}} R_p. \end{aligned}$$

Then, we get that the density of R is

$$\begin{aligned} \prod_{p \text{ prime}} S_p &= \prod_{p|k} (S_p) \prod_{p\nmid k} (S_p) \\ &\geq \prod_{p|k} \left(1 - \frac{2}{p}\right) \prod_{p\nmid k} \left(1 - \frac{2}{p^2}\right). \end{aligned}$$

We see that the first product is positive, as there are only a finite number of primes p such that $p|k$. We see that the second infinite product is positive because $\sum \frac{2}{p^2}$ converges.

Thus we see that the density of n where $a+nk$ and $b+nk$ are both square free is positive, hence there exists at least one. $\square$

Theorem 2.1. *There exist cycles of every order.*

Proof. This result is proved by constructing a cycle of order k for arbitrary k. Pick $k>1$. Pick k distinct odd primes $p_1, \cdots, p_k$.

For $\bar{a} = [a_1, \cdots, a_k]$ let $\bar{a}_i = [a_1, \cdots, a_{i-1}, a_i + 1, a_{i+1}, \cdots, a_k]$. The goal is to find an $\bar{a}$ such that

$$D(\bar{p}^{\bar{a}_1}) = s_1 \cdot \bar{p}^{\bar{a}_2}$$

and in general

$$D(\bar{p}^{\bar{a}_i}) = s_i \cdot \bar{p}^{\bar{a}_{i+1}}$$

where $i+1$ is taken modulo k, and the s_i are square free coprime to $p_1 \cdot p_2 \cdots p_k$. Then for any i, $\bar{p}^{\bar{a}_i}$ gives a cycle of order k.

Note that if we find a_i such that

- a_i is square free,
- $a_i + 1$ is square free,
- $\gcd(a_i, p_i) = p_i$,
- $\gcd(a_i + 1, p_{i+1}) = p_{i+1}$,
- $\gcd(a_i, p_j) = 1$ for $j \neq i$,
- $\gcd(a_i + 1, p_j) = 1$ for $j \neq i+1$,
- $\gcd(a_i + 1, a_1 a_2 \cdots a_{i-1}) = 1$ for $i > 1$,
- $\gcd(a_i, a_1 a_2 \cdots a_{i-1}) = 1$ for $i > 1$,
- $\gcd(a_i, (a_1+1)(a_2+1)\cdots(a_{i-1}+1)) = 1$ for $i > 1$,

then $\bar{a} = [a_1, \cdots, a_k]$ has the desired property. It is worth noting here that the last two conditions require all of the a_i to be odd. To see that $\bar{a}$ has the desired property, note that

$$D(s_{i-1}\bar{p}^{\bar{a}_i}) = D(\bar{p}^{\bar{a}_i}) = a_1 a_2 \cdots (a_i+1) \cdots a_n \bar{p}^{\bar{a}_i - 1} = s_i \bar{p}^{a_{i+1}},$$

where the last equality follows from the properties of $\bar{a}$.

We can solve for each a_i in order by the use of the Chinese remainder Theorem and Lemma 2.1. $\square$

In Table 1, $\bar{a}$ is given for cycles of sizes 2 to 10 for the first 10 primes. It should be noted that this construction does not give the smallest n where the derived sequence is of order k. For example, let $s_1 = 2 \cdot 7$ and $s_2 = 2 \cdot 23$ then $s_2 \cdot 3^{70} \cdot 5^5$ and $s_1 \cdot 3^{69} \cdot 5^6$ gives rise to a cycle of order two. The smallest cycle of order two is 2^5 and $5 \cdot 2^4$, which is considerably smaller.

Cycle Size	Primes									
	3	5	7	11	13	17	19	23	29	31
2	69	5								
3	129	265	77							
4	129	265	1561	1397						
5	309	265	1561	12661	221					
6	309	265	1561	12661	10777	1037				
7	309	1945	1561	12661	10777	15997	437			
8	309	1945	1561	12661	10777	15997	20653	1541		
9	309	1945	1561	12661	10777	15997	20653	4117	2117	
10	669	1945	4333	12661	10777	15997	20653	4117	6757	4061

TABLE 1. $\bar{a}$ that give rise to an various cycle sizes.

3. COMPUTING $D^{-1}(n)$.

By noticing that $D(s) = 1$ for all square free numbers s, we see that if we have $D(m) = n$ then $D(ms) = n$ for all square free factors s coprime to m. To eliminate these trivial alternate values to $D^{-1}(n)$, we introduce the definition:

Definition 3.1. *If $\bar{p}^{\bar{b}}$ has no square free components (i.e. $b_i \neq 1$ for all i) and $D(\bar{p}^{\bar{b}}) = n$ then we say that $\bar{p}^{\bar{b}}$ is a canonical value of $D^{-1}(n)$. We define $D_c(n)$ to be the set of all canonical values of $D^{-1}(n)$.*

To compute $D_c(n)$ we need the following lemma.

Lemma 3.1. *If $n = \bar{p}^{\bar{a}}$ and $D_c(n) \neq \emptyset$, then for every $k \in D_c(n)$ we have $k = \bar{p}^{\bar{b}}$. Furthermore $0 \leq b_i \leq a_i + 1$.*

Proof. This follows immediately by applying D to $\bar{p}^{\bar{b}}$. □

In particular an element of $D_c(n)$ cannot have prime factors that are not also factors of n.

Corollary 3.1. *Let p be a prime. Then $D_c(p^a) \neq \emptyset$ if and only if $a = p^k + k - 1$ for some k. Further $D_c(p^{p^k+k-1}) = \{p^{p^k}\}$.*

Corollary 3.2. *If s is an odd square free number, then $D_c(s) = \emptyset$.*

Given Lemma 3.1, it is an easy matter to determine $D_c(n)$. Simply compute $D(\bar{p}^{\bar{b}})$ where $0 \leq b_i \leq a_i + 1$ and $b_i \neq 1$, and check which ones work. For large exponents $\bar{b}$ this is not particularly efficient, but it suffices for $n < 10^7$.

We see from Corollary 3.1 and 3.2 that $D_c(n)$ is empty for some values n. Table 2 lists $D_c(n)$, if they are nonempty, for all $n \leq 100$. It is worth noting that, in the case of the first 100, there is a unique canonical value in $D_c(n)$. This is not true in general. The first example when $D_c(n)$ does not have a unique element is $108 = 2^2 \cdot 3^3$ for which we $D_c(108) = \{2^2 \cdot 3^3,\ 3^4\}$. The first six examples of multiple canonical values, less than 2000 are listed in Table 3.

We have the following results concerning the non-uniqueness of the canonical values in $D_c(n)$.

n	$D_c(n)$
$1 = 1$	$\{1 = 1\}$
$4 = 2^2$	$\{4 = 2^2\}$
$6 = 2 \cdot 3$	$\{9 = 3^2\}$
$10 = 2 \cdot 5$	$\{25 = 5^2\}$
$12 = 2^2 \cdot 3$	$\{8 = 2^3\}$
$14 = 2 \cdot 7$	$\{49 = 7^2\}$
$22 = 2 \cdot 11$	$\{121 = 11^2\}$
$24 = 2^3 \cdot 3$	$\{36 = 2^2 \cdot 3^2\}$
$26 = 2 \cdot 13$	$\{169 = 13^2\}$
$27 = 3^3$	$\{27 = 3^3\}$
$32 = 2^5$	$\{16 = 2^4\}$
$34 = 2 \cdot 17$	$\{289 = 17^2\}$
$38 = 2 \cdot 19$	$\{361 = 19^2\}$
$40 = 2^3 \cdot 5$	$\{100 = 2^2 \cdot 5^2\}$
$46 = 2 \cdot 23$	$\{529 = 23^2\}$
$56 = 2^3 \cdot 7$	$\{196 = 2^2 \cdot 7^2\}$
$58 = 2 \cdot 29$	$\{841 = 29^2\}$
$60 = 2^2 \cdot 3 \cdot 5$	$\{225 = 3^2 \cdot 5^2\}$
$62 = 2 \cdot 31$	$\{961 = 31^2\}$
$72 = 2^3 \cdot 3^2$	$\{72 = 2^3 \cdot 3^2\}$
$74 = 2 \cdot 37$	$\{1369 = 37^2\}$
$75 = 3 \cdot 5^2$	$\{125 = 5^3\}$
$80 = 2^4 \cdot 5$	$\{32 = 2^5\}$
$82 = 2 \cdot 41$	$\{1681 = 41^2\}$
$84 = 2^2 \cdot 3 \cdot 7$	$\{441 = 3^2 7^2\}$
$86 = 2 \cdot 43$	$\{1849 = 43^2\}$
$88 = 2^3 \cdot 11$	$\{484 = 2^2 \cdot 11^2\}$
$94 = 2 \cdot 47$	$\{2209 = 47^2\}$

TABLE 2. $D_c(n)$ for $n \leq 100$ when $D_c(n)$ is non-empty.

n	$D_c(n)$
$108 = 2^2 \cdot 3^3$	$\{81 = 3^4, 108 = 2^2 \cdot 3^3\}$
$192 = 2^6 \cdot 3$	$\{144 = 2^4 \cdot 3^2, 64 = 2^6\}$
$448 = 2^6 \cdot 7$	$\{784 = 2^4 \cdot 7^2, 128 = 2^7\}$
$1080 = 2^3 \cdot 3^3 \cdot 5$	$\{2025 = 3^4 \cdot 5^2, 2700 = 2^2 \cdot 3^3 \cdot 5^2\}$
$1512 = 2^3 \cdot 3^3 \cdot 7$	$\{3969 = 3^4 \cdot 7^2, 5292 = 2^2 \cdot 3^3 \cdot 7^2\}$
$1920 = 2^7 \cdot 3 \cdot 5$	$\{3600 = 2^4 \cdot 3^2 \cdot 5^2, 1600 = 2^6 \cdot 5^2\}$

TABLE 3. Examples of two different Canonical values, for $n \leq 2000$

Lemma 3.2. *If $m \in D_c(p+1)$, then $D_c((p+1)p^p)$ has at least two elements, namely $m \cdot p^p$ and p^{p+1}.*

Proof. One only needs to check that m is coprime to p, which follows from Lemma 3.1. □

Lemma 3.3. *If $D_c(n)$ and $D_c(m)$ have k and l elements in them, and for every $x \in D_c(n)$ and $y \in D_c(m)$ we have $\gcd(x,y) = 1$, then $D_c(nm)$ has at least kl elements.*

Proof. For $x \in D_c(n)$ and $y \in D_c(m)$, note that $D(xy) = D(x)D(y) = mn$, since x and y are coprime. □

Example 1. *Notice that:*

$$D_c(3 \cdot 2 \cdot 5^5) = \{5^6,\ 5^5 \cdot 3^2\}$$

and

$$D_c(2 \cdot 7 \cdot 13^{13}) = \{13^{14},\ 7^2 \cdot 13^{13}\}.$$

Combining these together, either by Lemma 3.3, or by direct computation we get

$$\begin{aligned} D_c(2^2 \cdot 3 \cdot 5^5 \cdot 7 \cdot 13^{13}) &= \{13^{14} \cdot 5^6,\ 7^2 \cdot 13^{13} \cdot 5^6, \\ &\quad 13^{14} \cdot 3^2 \cdot 5^5,\ 7^2 \cdot 13^{13} \cdot 3^2 \cdot 5^5\}. \end{aligned}$$

It should be noted that Lemma 3.3 only shows that these four values are contained in $D_c(2^2 \cdot 3 \cdot 5^5 \cdot 7 \cdot 13^{13})$. Equality comes from direct computation.

In particular if p and $2p-1$ are both prime, then for $n = 2 \cdot p \cdot (2p-1)^{2p-1}$ we have $D_c(n)$ has at least 2 elements, namely $p^2 \cdot (2p-1)^{2p-1}$ and $(2p-1)^{2p}$. Primes with this property are similar to Sophie Germain primes, in which p and $2p+1$ must both be prime [2, 3]. It is not known if there are infinitely many Sophie Germain primes, and there do not appear to be any results of primes p where $2p-1$ is also prime. If anything is learned about primes of this form, then the following Theorem can be strengthened. In particular, if Dickson's Conjecture is true (see for instance page 180 of [4]), then there are an infinite number of primes p such that $2p-1$ is also prime. In this case, this Theorem can be strengthen, by replacing 2^{7101} with M an arbitrarily large number.

Theorem 3.1. *There exists an n such that $D_c(n)$ has at least 2^{7101} elements.*

Proof. A quick computation verifies that there are 7101 primes p less than a million, where $2p-1$ is also prime, and all of these terms are coprime. Let $P_i := 2p_i - 1$. By Lemma 3.2 we see that $D_c(2 \cdot p_i \cdot P_i^{P_i})$ has (at least) two elements, $P_i^{P_i+1}$ and $P_i^{P_i} \cdot p_i^2$. By Lemma 3.3 we see that if $n = \prod 2 \cdot p_i \cdot P_i^{P_i}$ then $D_c(n)$ has at least 2^{7101} elements. □

4. Conclusions

In Section 3 we considered primes p where $2p-1$ is also prime. An interesting observation is that, empirically, there appears to be the same number of these types of primes as there are of Sophie Germain primes.

In [1], Cohen and Iannucci conjectured the existence of n such that the derived sequence of n is unbounded. It would be interesting to know if this is in fact true or not.

It would also be interesting to explore the properties of the D function if it is extended in the natural way to rational numbers. For example: $D\left(\frac{16}{9}\right) = D\left(2^4 \cdot 3^{-2}\right) = 4 \cdot 2^3 \cdot (-2) \cdot 3^{-3} = -2^6 \cdot 3^{-3} = -\frac{64}{27}$ and $D(-1) = -1$.

5. Acknowledgment

We would like to thank the organizers of the West Coast Number Theory conference, where we were first introduced to this problem. We would also like to thank the referee for a number of very useful comments and suggestions.

References

[1] G. L. Cohen and D. E. Iannucci. Derived sequences. *J. Integer Seq.*, **6** (2003), Article 03.1.1.
[2] Harvey Dubner. Large Sophie Germain primes. *Math. Comp.*, **65** (1996), 393–396.
[3] Karl-Heinz Indlekofer and Antal Járai. Largest known twin primes and Sophie Germain primes. *Math. Comp.*, **68** (1999), 1317–1324.
[4] Paulo Ribenboim. *The Little Book of Big Primes*. Springer-Verlag, New York, 1991.

2000 *Mathematics Subject Classification*: Primary 11Y55; Secondary 11A25, 11B83.
Keywords: Arithmetic functions, multiplicative functions, cycles.

Received April 21, 2003; revised version received June 23, 2003. Published in *Journal of Integer Sequences*, July 9, 2003.

Return to Journal of Integer Sequences home page.