A multiplicative variant arithmetic derivation

István Kovács Dániel Soltész

December 28, 2013

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad f(n) := \prod_{i=1}^{k} \alpha_i p_i^{\alpha_i - 1}$$

Let us denote the k-th iterate of this function by

$$f^{(k)}(n) := \underbrace{f(\ldots f(f}_{k \text{ times}}(n))\ldots).$$

We say that a k-tuple of distinct positive integers $(n_1, \ldots, n_k)$ is a k-cycle if and only if $f(n_i) = n_{i+1}$ and the indices are understood modulo k.

1 Elementary properties of the derivation

These claims help us to develop an understanding of the behavior of the derivation. The first six properties are immediate consequences of the definition. For the seventh and eighth, we also present their proofs.

Claim 1. *f is a multiplicative but not a totally multiplicative arithmetic function.*

While the usual Arithmetic derivative preserves the Leibnitz rule, the "nice property" of our derivative is that it is multiplicative.

Claim 2. *$f(n)$ can be expressed in terms of the radical and the number of divisors function:*

$$f(n) := \left(\prod_{i=1}^{k} \alpha_i\right)\left(\prod_{i=1}^{k} p_i^{\alpha_i - 1}\right) = d\left(\frac{n}{rad(n)}\right)\frac{n}{rad(n)}$$

From this it follows that $f(n) = o(n^{1+\varepsilon})$ for any $\varepsilon > 0$.

Claim 3. *$\prod_i p_i = \prod_i \alpha_i$ if and only if $f(n) = n$.*

This way from the prime decomposition of n it is easy to check if n is a 1-cycle. But we do not have similar conditions for n being in a k-cycle. Also note that for a k-cycle the product of all the exponents is equal to the product of all the primes.

Claim 4. *If p^k divides n then p^{k-1} divides $f(n)$.*

In other words the exponents can decrease by at most one.

Claim 5. *If $\alpha_i \equiv k_i \pmod p$ and $0 \leq k_i < p$ then $p^{\alpha_i - k_i}$ divides $f^{(m)}(n)$ for any m.*

Therefore the exponents of p_i can only decrease to the first multiple of p_i.

Claim 6. *For any n and square-free c, $(n,c)=1$ if and only if $f(nc)=f(n)$.*

This shows us that infinitely many numbers have the same derivative.

Claim 7. *(Mark Sapir [?]) For any K there is an $n\in\mathbb{N}$ such that $f^{(K)}(n)$ is not in a cycle.*

Proof. If there is an n such that $f^{(k)}(n)$ is not bounded, we are done. Otherwise for an arbitrary $n>K$ consider the sequence $a_n, a_{n-1},\dots,a_1, f(a_1),\ f^{(2)}(a_1),\ \dots, f^{(k)}(a_1)\dots$ where $a_n=n$ and $a_j=jf(a_{j+1})$. By assumption that for any integer the sequence is bounded, this sequence has only finitely many distinct elements. Thus we can choose p a prime larger than every element. Then by the definition of the sequence, for any $m\le n$ we have that $f^{(m)}(p^n)=a_{n-m+1}p^{n-m}$ thus for any $m<n$ we have that p divides $f^{(m)}(p^n)$ but for $m\ge n$, p des not divide $f^{(m)}(p^n)$ finishing the proof. □

Claim 8. *If there is a not bounded sequence $n_0,n_1,\dots,n_m,\dots$ and $f^{(m)}(n_0)=n_m$ then there are infinitely many primes which divide some element in this sequence.*

Proof. Suppose to the contrary that there are only finitely many primes dividing the sequence, also note that the same primes are the only prime divisors of the exponents too. We denote these primes by $p_1,\dots,p_k$. We define $\alpha_{i,m}$ by the prime factorization of $n_m=\prod_{i=1}^k p_i^{\alpha_{i,m}}$. An elementary upper bound for the growth of the exponents is

$$\alpha_{i,m+1}<\alpha_{i,m}+\sum_{j=1}^{k}\log_2(\alpha_{j,m})\le\alpha_{i,m}+\sum_{j=1}^{k}\log(\alpha_{j,m}).$$

The number of $\alpha<n$ such that the only prime divisors of α are $p_1,\dots,p_k$ is at most $c\log^k(n)$. Therefore for infinitely many n there is an interval $[n,n+n/(\log^k(n))]$ where every integer is divisible by a prime not in $\{p_1,\dots,p_k\}$. Choose an n larger than every $\alpha_{i,0}$ such that the interval $[n,n+n/(\log^k(n))]$ is as above and $n/(\log^k(n))>k\log(n)$. Then let l be the first integer such that for some j, $\alpha_{j,l}>n+n/(\log^k(n))$. Now by assumption $\alpha_{j,l-1}<n$ which contradicts the upper bound on the growth rate of the exponents. □

2 Proof of Theorem 1

Consider the exponents in an N-cycle. Observe that for any number in an N-cycle the product of the exponents of the odd primes can not be divisible by 4. Otherwise we could use Claim 4 and Claim 5 on the exponent of 2 to contradict the fact that the number is in an N-cycle. Thus any exponent can move at most three. Our construction of the N cycle uses exactly N primes with exponents larger than two. In each step only one exponent decreases, one increases and all the others remain the same.

Theorem 1. *For any $k\in\mathbb{N}$ there exists a k-cycle.*

First we describe our construction reducing the problem to the existence of integers with certain properties. Let $p_1,p_2\dots,p_N,c_1,c_2\dots,c_N,d_1,d_2,\dots,d_N$ be pairwise relatively prime odd integers such that the p_i are primes and the c_i,d_i are square-free such that:

$$p_{i+1}c_i-1=2p_id_i.$$

The elements of the cycle $(n_1,n_2,\dots,n_N)$ are in the the following form (the indices are modulo N):

$$n_i = p_i^{2p_id_i}\left(\prod_{\substack{j=1\\ j\neq i}}^{N} p_j^{p_{j+1}c_j}\right) 2d_{i-1}\left(\prod_{\substack{j=1\\ j\neq i-1}}^{N} c_j\right) \tag{1}$$

It is easy to check that $f(n_i) = n_{i+1}$. We finish the proof by showing the existence of suitable p_i, c_i and d_i.

Lemma 1. *For any N there exists $p_1, p_2, \ldots, p_N, c_1, c_2, \ldots, c_N, d_1, d_2, \ldots, d_N$ pairwise relatively prime odd integers such that p_i is prime and c_i, d_i is squarefree for all i and $p_{i+1}c_i - 1 = 2p_id_i$.*

Proof. Let $p_1, p_2, \ldots, p_N$ be arbitrary distinct odd primes. Suppose that we have c_i, d_i with the desired properties for $i < k$. We show that suitable c_k, d_k exists. Note that the same method can be used to obtain c_1 and d_1. Fix a large positive integer M. Let S_M denote the set of odd primes less than M which does not divide any p_i, c_i, d_i for $i < k$. Consider the following congruence systems

$$\begin{array}{rcrll}
x & \equiv & 2 & \mod 4 & \\
x & \equiv & 0 & \mod p_k & \\
x & \equiv & -1 & \mod p_{k+1} & \\
x & \equiv & 1 & \mod p_j & \text{for all } j \leq N, j \neq k \text{ and } j \neq k+1 \\
x & \equiv & 1 & \mod c_i & \text{for all } i < k \\
x & \equiv & 1 & \mod d_i & \text{for all } i < k \\
x & \equiv & r_s & \mod p_s^2 & \text{for all } p_s \in S_M
\end{array} \tag{2}$$

where every r_s varies over the set $\{1, \ldots, p_s^2 - 2\}$ independently of each other.

Let $\phi(n)$ denote the number of squarefree integers less than n and satisfying the first six congruence relations in (2). It is enough to show that $\phi(n)$ is positive for sufficiently large n since for x squarefree $d_k = x/(2p_k)$ and $c_k = (x+1)/p_{k+1}$ will satisfy the conditions. Note that the right hand side of the third fourth and fifth congruence ensures that the resulting numbers are relatively prime to all the previous c_i, d_i, the choice of 1 serves only this purpose. We wish to prove the positivity of $\phi(n)$ by showing that

$$\lim_{n\to\infty} \frac{\phi(n)}{n} = C > 0.$$

Let $\phi_M(n)$ denote the number of integers less than n and satisfying (2) for some possible choices of r_s. We approximate $\phi(n)$ by $\phi_M(n)$. Whenever n is a multiple of $4\prod_{i=1}^{N} p_i \prod_{j=1}^{k-1} c_j d_j \prod_{p_s\in S} p_s^2$ then by the Chinese remainder theorem

$$\frac{\phi_M(n)}{n} = \frac{1}{4}\prod_{i=1}^{N}\frac{1}{p_i}\prod_{j=1}^{k-1}\frac{1}{c_jd_j}\prod_{p_s\in S_M}\left(1-\frac{2}{p_s^2}\right)$$

holds. Thus for arbitrary n and a C' positive constant we have that

$$\begin{aligned}
\frac{\phi_M(n)}{n} &= \frac{1}{4}\prod_{i=1}^{N}\frac{1}{p_i}\prod_{j=1}^{k-1}\frac{1}{c_jd_j}\prod_{p_s\in S_M}\left(1-\frac{2}{p_s^2}\right) + O\left(\frac{1}{n}\right) \\
&= C'\prod_{\substack{p<M\\ p \text{ prime}}}\left(1-\frac{2}{p^2}\right) + O\left(\frac{1}{n}\right).
\end{aligned}$$

Now we estimate the error of the approximation. The number of $x < n$ such that x or $x+1$ is divisible by a square of a prime $p \geq M$ is at most $\frac{2n}{p^2}$. Thus

$$\frac{\phi_M(n) - \phi(n)}{n} \leq \sum_{\substack{p \geq M \\ p \text{ prime}}} \frac{2}{p^2} = O\left(\frac{1}{M \log M}\right)$$

and

$$\frac{\phi(n)}{n} \geq C' \prod_{\substack{p < M \\ p \text{ prime}}} \left(1 - \frac{2}{p^2}\right) + O\left(\frac{1}{n}\right) - O\left(\frac{1}{M \log M}\right)$$

finishes the proof for large enough M and $n \to \infty$ as the product converges to a positive constant as $M \to \infty$. □

Remarks: We can add any finite number of congruences to (2) if we maintain that the conditions of the Chinese remainder theorem are satisfied and that x is square-free with respect to the primes less than M. We also have to adjust S_M to the new congruences. From this it follows that there are infinitely many k cycles such that elements from distinct cycles are co-prime. Also note that the d_i need not be relatively prime to each other, but the assumption that they are simplifies the presentation of the proof.

Experimental obervations: We tested the first 100000 integers we observed that the vast majority of numbers fall into a cycle after four steps. We arrived to the conclusion that the numbers of the form $p_1^{p_2^{p_3}}$ tend to grow large and sometimes it takes several hundreds of thousands of derivations to get to a cycle. Although we know that arbitrarily large cycles exists, we only found examples of $1, 2$ and 4-cycles.