K-ary convolutions: What we know

July 18, 2016

This is not a research paper. This is just explaining k-ary convolutions so we are all on the same page. I hope we can also agree on which direction to go, and explain that choice here, so that our interests don't diverge.

1 Introduction

Definition 1. d is a unitary divisor of n (denoted $d|_1 n$) if and only if $d|n$ and $(d, \frac{n}{d}) = 1$.

For a prime-power, p^a, its unitary divisors are 1 and p^a. For the product of prime-powers, $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, its unitary divisors are the products of any combination of the prime-powers it is composed of.

Definition 2. Let $(a, b)_1$ stand for the greatest common unitary divisor of a and b.

Definition 3. d is a biunitary divisor of n (denoted $d|_2 n$) if and only if $d|n$ and $(d, \frac{n}{d})_1 = 1$.

Note that since unitary divisors are so much more rare than divisors in general, having a common unitary divisor greater than 1 is much more rare. Therefore biunitary divisors are much more common than unitary ones.

We can generalize this notion to k-ary division.

Definition 4. d is a k-ary divisor of n (denoted $d|_k n$) if and only if $d|n$ and $(d, \frac{n}{d})_{k-1} = 1$. Let $(a, b)_k$ stand for the greatest common k-ary divisor of a and b.

Note that, the normal division is 0-ary division and normal GCD is the 0-ary GCD.

There is an oscilitory pattern. The more k-ary divisors, the less $(k+1)$-ary divisors, and vice versa.

2 Specific cases

Definition 5. Let $A_k(n)$ stand for the set of all k-ary divisors of n.

Theorem 1. *For all k, $\{1, n\} \subseteq A_k(n)$.*

Theorem 2. *For $p \in \mathbb{P}$, $A_0(p^a) = \{1, p, p^2, \ldots, p^a\}$*

Theorem 3. *For $p \in \mathbb{P}$, $A_1(p^a) = \{1, p^a\}$*

Theorem 4. *For $p \in \mathbb{P}$, $A_2(p^a) = \begin{cases} A_0(p^a) \setminus \{p^{a/2}\} & 2 \mid a \\ A_0(p^a) & 2 \nmid a \end{cases}$*

Proof. $A_1(p^{a-b}) = \{1, p^{a-b}\}$ and $p^b = \{1, p^b\}$, therefore the $A_1(p^{a-b}) \cap A_1(p^b) = \{1\}$ unless $a - b = b$, in which case $A_1(p^{a-b}) \cap A_1(p^b) = \{1, p^b\}$. □

Theorem 5. *For $p \in \mathbb{P}$, $A_3(p^a) = \begin{cases} \{1, p, p^2, p^3\} & a = 3 \\ \{1, p^2, p^4, p^6\} & a = 6 \\ A_1(p^a) & \textit{otherwise} \end{cases}$*

Proof. For $0 \leq a \leq 6$,the theorem can be verified computationally.

Otherwise $a > 6$. All divisor pairs of p^a are of the form p^{a-b} and p^b where $b \leq \lfloor \frac{a}{2} \rfloor$. I will show that these divisors are not 2-ary coprime unless $b = 0$, proving that $A_3(p^a) = \{1, p^a\}$

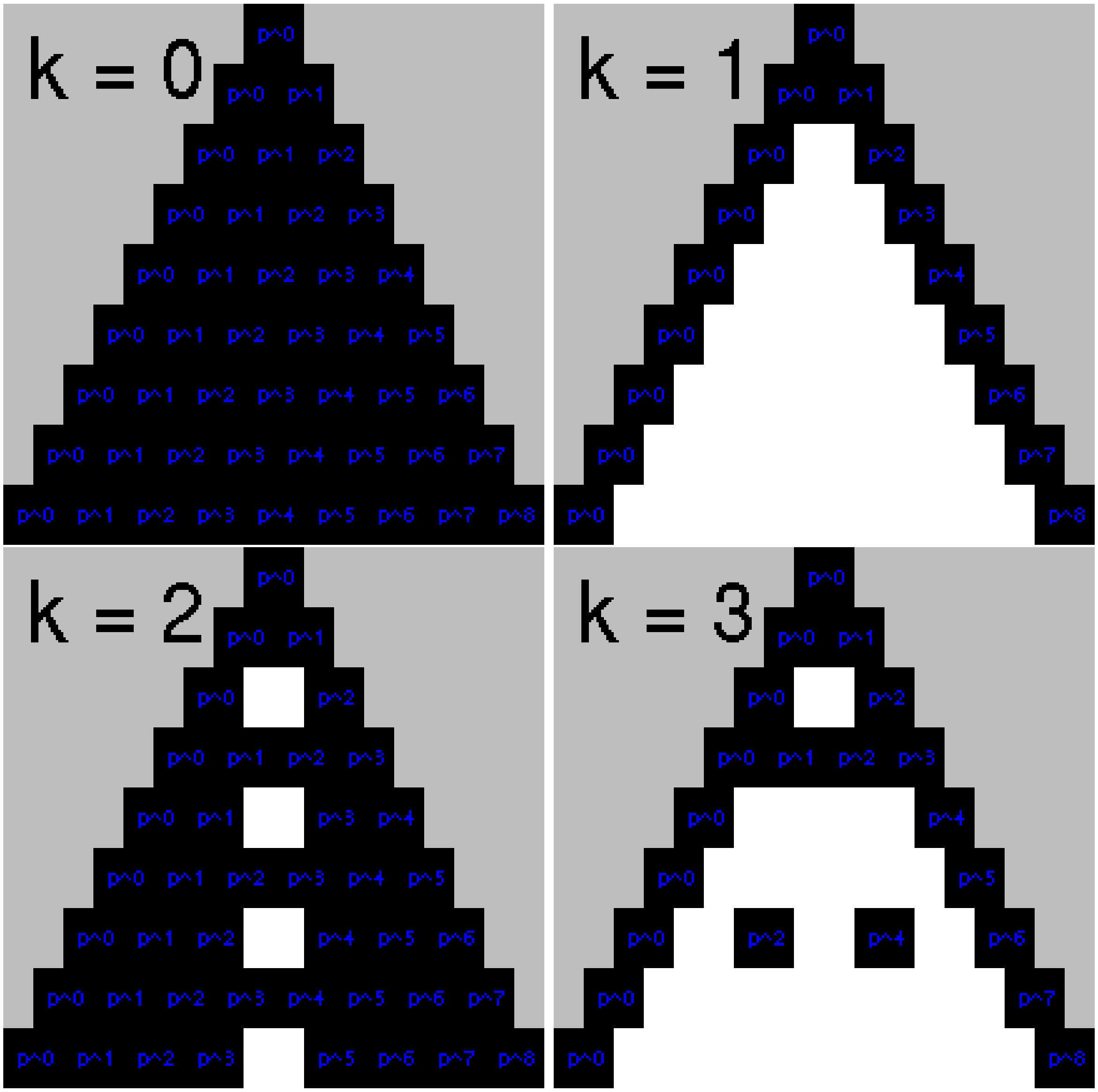
- If $b > 2$, then $p \in A_2(p^{a-b})$ and $p \in A_2(p^b)$ so $(p^{a-b}, p^b)_2 \geq p \neq 1$.
- If $b = 2$, then $p^2 \in A_2(p^b)$ and $p^2 \in A_2(p^{a-b})$ since $a > 6$, so $(p^b, p^{a-b})_2 = p^2 \neq 1$.
- If $b = 1$, then $p \in A_2(p^b)$ and $p \in A_2(p^{b-a})$, so $(p^b, p^{a-b})_2 = p \neq 1$.

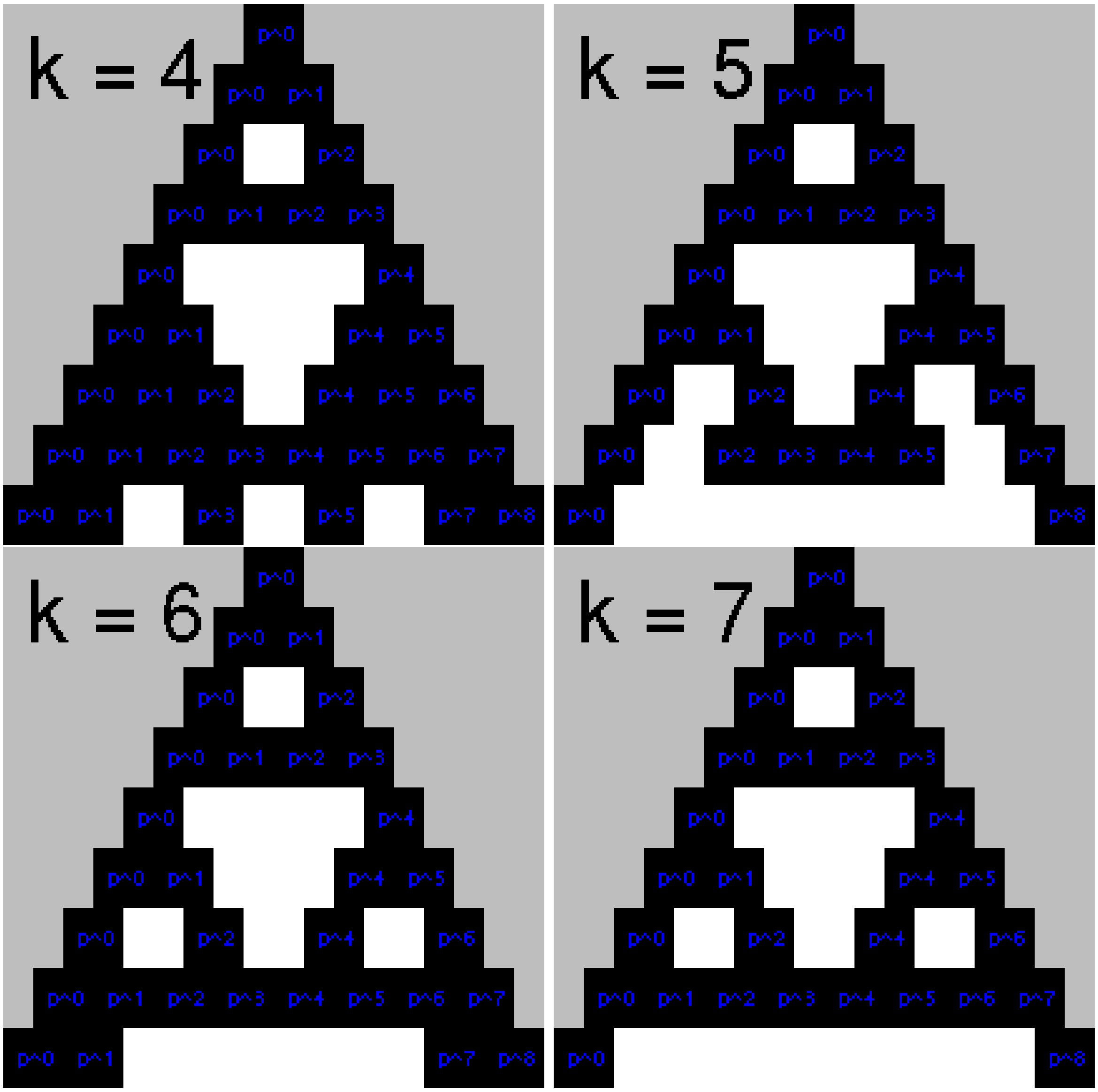
□

The rest are more complicated. Providing an easier way to compute these could be the subject of future research.

3 k-ary divisors

For even k, the k-ary divisors seem to be the same as the $(k-2)$-ary divisors with some elements removed. For odd k, the k-ary divisorss seem to be the same as the $(k-2)$-ary divisorss with some elements added n. Furthermore, if you go far enough, this odd-even oscilation converges to the infinitary divisors, with the odd k-ary divisors being a proper subset and the even k-ary divisors being a proper superset of the infinitary divisors.


k = 0
k = 1
k = 2
k = 3



Above are computer-generated visualizations where the n-th column of the k-th picture shows all of $A_k(p^n)$ highlighted in black. I will post code for this shortly.

4 Infinitary divisors

If you fix a and let k be sufficiently large, $A_k(p^a)$ remains constant when you increase k. Notice how in the $k = 5$ and beyond, the row ending in p^4 does not change. Neither do any of the rows above it.

Theorem 6 (Cohen). *For $k > y - 1$, $A_k(p^y) = A_{y-1}(p^y)$.*

Proof. (by induction)

Base case: when $y = 1$, $A_k(p) = \{1, p\} = A_0(p)$, from Theorem 1, and since there are no other possible divisors of p.

Inductive step: Assume for some y, $A_k(p^y) = A_{y-1}(p^y)$ for $k \geq y-1$. Then $A_{k+1}(p^{y+1}) = \{p^a \mid 1 < a < y \wedge (p^a, p^{y+1-a})_k = 1\} \cup \{1, p^{y+1}\}$. But for $1 < a < y$, the inductive hypothesis applies, so $A_k(p^a) = A_y(p^a) = A_{a-1}(p^a)$ and likewise for p^{y+1-a}. Therefore $(p^a, p^{y+1-a})_k = (p^a, p^{y+1-a})_y$. Therefore $\{p^a \mid 1 < a < y \wedge (p^a, p^{y+1-a})_k = 1\} = \{p^a \mid 1 < a < y \wedge (p^a, p^{y+1-a})_y = 1\}$. Thus $A_{k+1} = A_y(p^{y+1})$ for $k + 1 \geq y$, proving the inductive step.

□

This motivates the definition of 'infinitary divisors'.

Definition 6. $p^x|_\infty p^y$ if and only if $p^x|_{y-1}p^y$

Cohen proves many more facts about infinitary divisors.