Decomposition of Natural Numbers from Prime Objects

Junya Sebata

July 8, 2022

Abstract

We decompose natural numbers from structure which prime numbers have, as its starting point. With the decomposition, we can find a general law by categorization, which is in a power set and also in structure which prime numbers have, and we know that it limits the framework of structure about product and sum of natural numbers. In other words, $\sum_{k=1}^{n} \phi(k) \times [\frac{n}{k}] = \frac{n(n+1)}{2}$ holds, and it is equivalent to a basic formula of sum of divisors $\sum_{k|n} \phi(k) = n$.

1 Introduction

When we try to understand natural numbers, at first it might be a normal way to think about them from order or sum. In other words, it is a thinking flow like as sum comes from order, then product comes from sum, and prime numbers are defined. General methods to think natural numbers, which started from Peano axioms, have this flow of defining them from sum to product. But by this kind of definition in which sum and product are connected firmly and inseparably, it is difficult to analyze structures of natural numbers about product, especially, structures of natural numbers about prime numbers.

On the other hand, because of the great achievement of Galois or not, many of researches in algebra, although they separate sum and product, are mainly on the basis of group, and many of them deal with the theory of integer, that is, the style of inducing theories from the expansion of natural numbers. In contrast, there can be an attitude to understand natural numbers themselves by decomposing them fundamentally, and actually natural ways to think them is decomposition to smaller objects than monoid. Although there are many researches on these objects, attempts to seek various decomposition and reconstruction of natural numbers are scarce.

Inherently for any kind of object, methods of thinking object are multilateral, therefore, it is important to select a right way fit to a purpose for analyzing it. In this paper, for seeking structure of natural numbers especially which is centered on prime numbers, we decompose natural numbers from structure which prime numbers have, as its starting point.

As like as one view of the world that we think all material in the world are composed of combination of atoms, an idea that we think all natural numbers are composed of product combination of prime numbers is basic for understanding natural numbers, and this feature of them is significant enough to let it be independent from definition of sum. We describe this feature of product of natural numbers with monoid as its basis, on the other hand, we compose order and sum which started from Peano axioms as object, and we connect both of them by mapping on which distributive law holds. This is our composition for natural numbers. Actually we see that it is possible enough to reconstruct natural numbers again by selecting necessary parts from the previous two of discussions, Peano and Galois.

However we start our discussion from more general object, namely power set. The reason why is that a general law, theorem 2.1, which we find in a power set by categorization is same as and related to a general law, corollary 3.1, which we find in structure prime numbers have by categorization. Finally, we know that corollary 3.1 limits the framework of structure about product and sum of natural numbers.

In the result, we see that Euler's totient function and floor function satisfy corollary 5.1 in natural numbers which have the distinguished feature, well-order. It should be noted that the following seems composition of natural numbers, but not decomposition. However, before composition, naturally, there is decomposition.

2   A general law on power set

A denotes a countable set, and SUB_A denotes a subset of $2^A \times 2^A$. For $\forall (x, y) \in SUB_A$, $(x \backslash y, y \backslash x)$ is determined, therefore we can categorize SUB_A by $DP_A = \{(x \backslash y, y \backslash x) | (x, y) \in SUB_A\}$ of which duplications are excluded. In other words, we can classify SUB_A to categories $SUBcatDP_A = \{\alpha | \alpha = \{(x, y) | (x \backslash y, y \backslash x) = \beta\}, \beta \in DP_A\}$.

We can also uniquely identify an element $(x, y) \in \alpha$ in each category $\alpha \in SUBcatDP_A$ by $x \cap y$. Therefore we can categorize $SUBcatDP_A$ by $SUBcatCP_A = \{\gamma | \gamma = \{x \cap y | (x, y) \in \alpha\}, \alpha \in SUBcatDP_A\}$. In other words, we can classify $SUBcatDP_A$ to categories $SUBcatDPcatCP_A = \{\delta | \delta = \{\beta | \{x \cap y | (x, y) \in \alpha\} = \gamma\}, \gamma \in SUBcatCP_A\}$.

From the above, SUB_A corresponds to $DP \times CP_A = \{(x', y') | (x', y') \in \delta_\gamma \times \gamma, \gamma \in SUBcatCP_A, \delta_\gamma \in SUBcatDPcatCP_A\}$ with one-to-one relation. Therefore the theorem below holds.

Theorem 2.1

$$\sum_{\gamma \in SUBcatCP_A, \ \delta_\gamma \in SUBcatDPcatCP_A} n(\delta_\gamma) \times n(\gamma) = n(SUB_A) \qquad (2.0.1)$$

We should note that the cases δ_γ includes $(\{\emptyset\}, \{\emptyset\})$ or $(\{\emptyset\}, y \backslash x)$, and γ includes $x \cap y = \{\emptyset\}$ are also counted up. Moreover, we note that even if $SUBcatCP_A$ remains duplications, the theorem above also holds, because the elements of DP_A have already been unique.

The following figure 1 will help us understand easily the complicated description of categories above. This figure is described with depending on the following consideration.

Thinking need object. We can not think with only one object, therefore at least two objects need. If two objects are no relation we can not think, therefore at least two objects and their relation need. In short, thinking need object and relation.

In addition, if object of which all the features are the same is one object, therefore to identify two objects need at least one different feature. In other words, identifying object need feature, and identifying object is done only by feature. With the consideration on the previous paragraph, to think all the features of an object need to think them as relation composed of an object and the object itself or other objects. Hence, object is relation composed of the object itself or other objects.

From the above, object is relation, and also relation is object. To describe our thought, object and relation, it is good to use the easiest and simplest geometric objects as being recognized. These are point and line. When we recognize something as object we use point, and when we recognize something as relation we use line. For example, we do not use a circle and points included in it for describing a set and elements, but use a line and points on it.

On a paper [1], readers can see the other concrete application example. In that paper [1], deformation of a famous algebraic formula thought in natural numbers is done by points, lines, and sets operation. It is interesting, because the deformation can also apply to the formula not only in natural numbers but finally in general. On [2], readers can see details of the philosophical consideration about object and relation above.

Next, we consider the case that new pairs ΔSUB_A are added into SUB_A. $\Delta SUBcatCP_A$ denotes categories corresponding to $SUBcatCP_A$, which are produced by ΔSUB_A, and also $\Delta SUBcatDPcatCP_A$ denotes categories corresponding to $SUBcatDPcatCP_A$. By these $\Delta SUBcatCP_A$ and $\Delta SUBcatDPcatCP_A$, ΔSUB_A corresponds to $\Delta DP \times CP_A = \{(x', y') | (x', y') \in \delta_\gamma \times \gamma, \gamma \in \Delta SUBcatCP_A, \delta_\gamma \in \Delta SUBcatDPcatCP_A\}$ with one-to-one relation.

The one-to-one correspondence of SUB_A and $DP \times CP_A$ is equivalent to the one-to-one correspondence of ΔSUB_A and $\Delta DP \times CP_A$, because if we take a difference of the former it becomes the latter and if we take a sum of the latter it becomes the former. Therefore, the next theorem is proved.
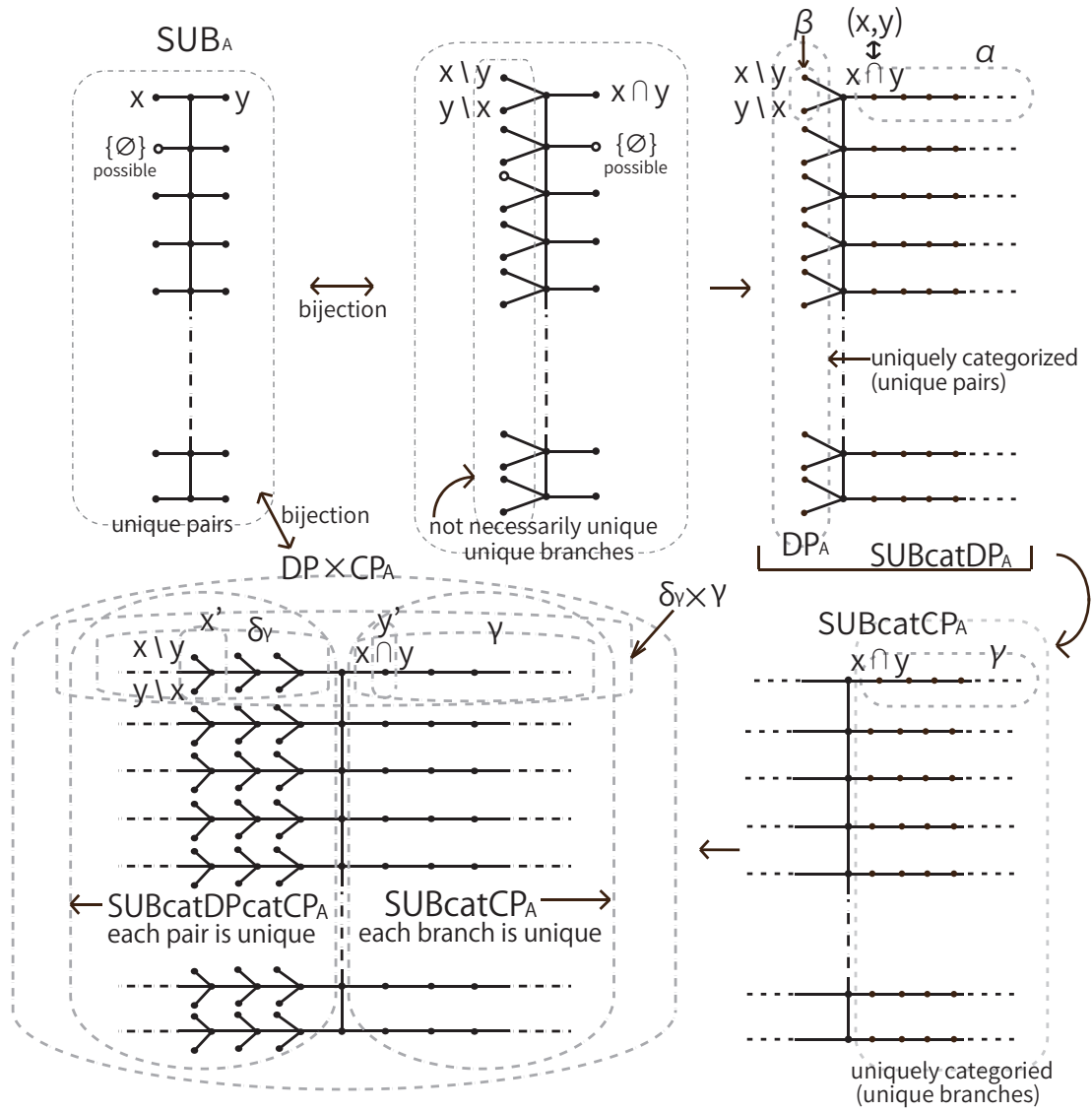
Figure 1: Points and Lines

Theorem 2.2

$$\sum_{\gamma \in SUBcatCP_A,\ \delta_\gamma \in SUBcatDPcatCP_A} \quad n(\delta_\gamma) \times n(\gamma) = n(SUB_A) \tag{2.0.2}$$

$$\Leftrightarrow$$

$$\sum_{\gamma \in \Delta SUBcatCP_A,\ \delta_\gamma \in \Delta SUBcatDPcatCP_A} \quad n(\delta_\gamma) \times n(\gamma) = n(\Delta SUB_A) \tag{2.0.3}$$

It is clear that the ratio between $n(\delta_\gamma)$ and $n(\gamma)$ is different by a power set structure SUB_A has. On objects dealt within the chapter 5, following conditions are satisfied. The one condition is for $\forall x, y \in sub2^A = \{x | (x, y) \in SUB_A\}$, $x \cap y \in sub2^A$ and $x \backslash y, y \backslash x \in sub2^A$. The other one is for $\forall x \in sub2^A$, $y \subset x \Rightarrow y \in sub2^A$. However, they do not need to prove theorem 2.1 and theorem 2.2. Therefore, they are omitted.

3 Abstraction of product of prime numbers

B denotes a countable set, it has an identity element, and commutative product satisfying associative law is defined on it. We think the case that the result of product is uniquely different by the elements in the product, the result of product without an identity is not included in B, and C denotes a set of which elements are elements of B and of the result of product of B. C does not necessarily include the product of the infinite number of elements.

SUB_B denotes a subset of $C \times C$. For $\forall (x, y) \in SUB_B$, $(x \backslash y, y \backslash x)$ is determined, therefore we can categorize SUB_B by $DP_B = \{(x \backslash y, y \backslash x) | (x, y) \in SUB_B\}$ of which duplications are excluded. In other words, we can classify SUB_B to categories $SUBcatDP_B = \{\alpha | \alpha = \{(x, y) | (x \backslash y, y \backslash x) = \beta\}, \beta \in DP_B\}$.

We can also uniquely identify an element $(x, y) \in \alpha$ in each category $\alpha \in SUBcatDP_B$ by $gcd(x, y)$. Therefore we can categorize $SUBcatDP_B$ by $SUBcatCP_B = \{\gamma | \gamma = \{gcd(x, y) | (x, y) \in \alpha\}, \alpha \in SUBcatDP_B\}$. In other words, we can classify $SUBcatDP_B$ to categories $SUBcatDPcatCP_B = \{\delta | \delta = \{\beta | \{gcd(x, y) | (x, y) \in \alpha\} = \gamma\}, \gamma \in SUBcatCP_B\}$.

From the above, SUB_B corresponds to $DP \times CP_B = \{(x', y') | (x', y') \in \delta_\gamma \times \gamma, \gamma \in SUBcatCP_B, \delta_\gamma \in SUBcatDPcatCP_B\}$ with one-to-one relation.

Therefore the corollary below holds by the consideration above, which is the same as the consideration of theorem 2.1.

Corollary 3.1

$$\sum_{\gamma \in SUBcatCP_B, \delta_\gamma \in SUBcatDPcatCP_B} n(\delta_\gamma) \times n(\gamma) = n(SUB_B) \tag{3.0.4}$$

We should note that the cases δ_γ includes $(1, 1)$ or $(1, y \backslash x)$, and γ includes $gcd(x, y) = 1$ are also counted up. Moreover, we note that even if $SUBcatCP_B$ remains duplications, the theorem above also holds, because the elements of DP_B have already been unique.

The following corollary also holds by the same consideration of theorem 2.2.

Corollary 3.2

$$\sum_{\gamma \in SUBcatCP_B, \delta_\gamma \in SUBcatDPcatCP_B} \quad n(\delta_\gamma) \times n(\gamma) = n(SUB_B) \tag{3.0.5}$$

$$\Leftrightarrow$$

$$\sum_{\gamma \in \Delta SUBcatCP_B, \delta_\gamma \in \Delta SUBcatDPcatCP_B} \quad n(\delta_\gamma) \times n(\gamma) = n(\Delta SUB_B) \tag{3.0.6}$$

Here, to understand the relationship between the previous chapter and this chapter, we consider about appropriate f, A, $sub'2^A \subset 2^A$ which would satisfy a surjective map $f : sub'2^A \to C$ for C. First, for some $x \in B$ which is not an identity, we fix n on the maximum number of $x^n | y$ in all $y \in C$. We make the subset and the elements $D_x = a_1, a_2, \ldots, a_n$ in A, corresponding to x^n. We also make A as all the elements of A, which is not a zero element, categorized in either $\forall D_x$. If we select appropriate $sub'2^A$, we can make a surjective map $f : sub'2^A \to C$ by the operation for an element of $sub'2^A$, which transfers a zero element to an identity element and the others with ignoring any index numbers and taking a product of these elements. By this consideration, we can confirm the existence of f, A, $sub'2^A$ satisfying the condition above.

By f, A, $sub'2^A$ above, we can make a surjective map g onto SUB_B with taking appropriate SUB_A. Since SUB_A corresponds to $DP \times CP_A$ with one-to-one relation and SUB_B also corresponds to $DP \times CP_B$ with one-to-one relation, there exits a surjective map from $DP \times CP_A$ to $DP \times CP_B$ with this surjective map g. It can be also said a surjective map from the one-to-one relation between SUB_A and $DP \times CP_A$ to the one-to-one relation between SUB_B and $DP \times CP_B$. From these, we can always confirm the existence of a power set of theorem 2.1 to which corollary 3.1 corresponds as above.

However we should note that corollary 3.1 is not directly led from theorem 2.1 in this paper. It is not more than the fact that corollary 3.1 is proved by the same logical proof as theorem 2.1. It is not clear that a surjective map from $DP \times CP_A$ to $DP \times CP_B$, which needs to confirm the existence of the one-to-one relation between SUB_B and $DP \times CP_B$ in corollary 3.1, can naturally defined by f. We go ahead with remaining this point for the unsolved problem on this paper.

We can apply the content on this chapter to natural numbers with dealing a set of prime numbers as B. In that case, we can know that a new natural number $n++$ arises or being produced necessarily by either an element $x \in C \wedge x \le n$ times one element of B, but not an identity element. For starting to think about this feature, it is good for us to compare natural numbers to the next two extreme examples. The one is the case that B has only one element except an identity element, or the other one is the case of $SUB_B = B \times B$. Corollaries of this chapter hold surely on these two examples, also any composition of B, C, SUB_B, and any increment of ΔSUB_B. At each case, we can know that the ratio between $n(\delta_\gamma)$ and $n(\gamma)$ is different by their composition and increment.

4 Construction of natural numbers

D denotes a countable set, and total order holds on it. We think the case that $n(D) = n(C)$ holds, therefore a bijective mapping $h : C \to D$ exists. In addition, we define sum on D, which is closed, satisfies associative law, and is commutative. We think the case that for any elements a, b, c in D, distributive law $h(h^{-1}(a+b)h^{-1}(c)) = h(h^{-1}(a)h^{-1}(c)) + h(h^{-1}(b)h^{-1}(c))$ with h and C holds. In addition, we think the case that D has the minimum element d_1, and for any element a in D and its next element b on the order, $b = a + d_1$ holds.

In short, product is not defined directly on D, but the relation which can be thought as product is constructed by C and h. In addition to it, we should note that any x in D can be described as the sum $x = d_1 + d_1 + \cdots + d_1$, which uses only d_1, and the number of terms d_1 is unique for each element x.

We put index numbers $1, 2, \cdots, n-1, n \in N$ on elements in D along with the order, and $m_x \in N$ denotes the index number of $x \in D$. First, if an identity element e in C satisfies $d_1 \ne a = h(e)$, $h^{-1}(a) = e$ holds. For $h^{-1}(a)h^{-1}(a) = ee = e$, we substitute $a = d_1 + d_1 + \cdots + d_1$, which is the $m_a \ge 2$ times sum of d_1, in it. We apply distributive law repeatedly to the left side of $h(h^{-1}(d_1 + d_1 + \cdots + d_1)h^{-1}(d_1 + d_1 + \cdots + d_1)) = h(e)$, and it becomes the m_a^2 times sum of $h(h^{-1}(d_1)h^{-1}(d_1))$. Although the index number of $h(h^{-1}(d_1)h^{-1}(d_1))$ is any number, the index number of the left side is larger than m_a. There exists b which satisfies $a \ne b = h(e)$ and $m_b > m_a$. This contradicts that h is a mapping. Therefore an identity element e in C satisfies $d_1 = h(e)$.

Next if h does not distribute elements of B, but not an identity element, to the elements in D of which index numbers are prime numbers in the index set N, for $a \in D$ which satisfies $a = h(x)$ of $\exists x \in B \wedge x \ne e$, the index number m_a is not a prime number. There exist $b, c \in D$ which are not d_1 and satisfy $m_a = m_b m_c$. We think about $h(h^{-1}(b)h^{-1}(c))$, and substitute $b = d_1 + d_1 + \cdots + d_1$ which is the m_b times sum of d_1 and $c = d_1 + d_1 + \cdots + d_1$ which is the m_c times sum of d_1 into it. By repeatedly applying distributive law, $h(h^{-1}(b)h^{-1}(c)) = d_1 + d_1 + \cdots + d_1$ which is the $m_b m_c$ times sum of d_1 holds. The right side is a, and $h^{-1}(b)h^{-1}(c) = h^{-1}(a) = x$ holds. This contradicts that $x \in B$ is indivisible without an identity element.

On the other hand, if h distributes an element in C, but not in B, to an element a in D of which index number is a prime number in the index set N, there exist $\exists b, c \in D$, but not d_1, and $h(h^{-1}(b)h^{-1}(c)) = a$ holds. With thinking as the above, $m_b m_c = m_a$ holds and this contradicts that m_a is a prime number.

Therefore, h must distribute elements in B, but not an identity element, to the elements in D of which index numbers are prime numbers in the index set N, and also we need elements in B, but not an identity element, which are distributed to them, all the prime elements in D. In short, B corresponds to elements in D of which index numbers are 1 or prime numbers with

one-to-one relation by h. Distribution of h from each element in B, but not an identity element, to each element in D of which index number is a prime number is arbitrary. However if we fix the restricted distribution of B, h distributes C to D uniquely because of the same consideration as the above and uniqueness of prime factorization. On the contrary, the decomposition of each element of D which corresponds to the product decomposition of each element of C by B with h^{-1} and h accords with prime factorization in the index set N. In short, if we fix the restricted distribution of B, h is fixed uniquely and we can consider (C, h, D) equally as natural numbers N.

From the above, we should note the fact that we can consider (C, h, D) as the definition of natural numbers with excluding the index set N. Therefore, the one result from the consideration on Chapter 2, the proposition that object is relation, can be applied to even natural numbers which seem difficult to be decomposed. In short, from one point of view even natural numbers can be said that their entity is the relation h between the independent objects C and D.

Since conceptions of natural numbers are varied, it is the interesting fact that we can decompose natural numbers into two objects completely, however, it is not more than that. In addition, if even one condition of them (C, h, D) is lacking or added, they are not natural numbers, but similar objects. It is important to consider the cases in which we change the conditions of (C, h, D), but the connection between the next chapter gets fade, therefore, we do not discuss about that. This point remains also for the problem on this paper.

5   Euler's totient function and floor function

We apply the consideration on the chapter 3, abstraction of product of prime numbers, to the natural numbers (C, h, D) on the previous chapter, and we think about the case $SUB_B = \{(x, y) | n \geq m_{h(x)+h(y)}\}$.

For $n > 1$ and each unique $\beta \in DP_B$, we set k as

$$k = m_{h(x \setminus y)} + m_{h(y \setminus x)}.$$

k satisfies $k = 2, 3, \cdots, n$.

We set each $\gamma \in SUBcatCP_B$ as

$$SUBcatCP_B = \{\gamma_k | \gamma_k = \{gcd(x, y) | n \geq m_{h(gcd(x,y))} \cdot k\}, k = 2, 3, \cdots, n\}$$

corresponding to each k with one-to-one relation. $\gamma_k \in SUBcatCP_B$ are not necessarily unique. We have already pointed out the fact that it is no problem to define $SUBcatCP_B$ like this in theorem 2.1 and corollary 3.1. The reason is that the elements of DP_B are unique.

Therefore, each $\delta_{\gamma_k} \in SUBcatDPcatCP_B$ corresponds to all the relatively prime numbers of pairs $\{(m_{h(x \setminus y)}, m_{h(y \setminus x)}) | m_{h(x \setminus y)} + m_{h(y \setminus x)} = k\}$ being obtained from the previous $k = m_{h(x \setminus y)} + m_{h(y \setminus x)}$ with fixing k.

From the above, since $\gamma_k \in SUBcatCP_B$ is determined by each k, $n(\gamma_k) = [\frac{n}{k}]$ holds. Since $\delta_{\gamma_k} \in SUBcatDPcatCP_B$ corresponds to the relatively prime numbers of pairs which satisfy $k = m_{h(x \setminus y)} + m_{h(y \setminus x)}$, $n(\delta_{\gamma_k}) = \phi(k)$ holds.

Therefore, because of corollary 3.1 and the case $k = 1$ added afterward, the following holds.

Corollary 5.1

$$\sum_{k=1}^{n} \phi(k) \times [\frac{n}{k}] = n(SUB_B) + n = \frac{n(n+1)}{2} \tag{5.0.7}$$

We can easily confirm that the case $n = 1$ of the above also holds. Because of corollary 3.2, the following also holds.

Corollary 5.2

$$\sum_{k=1}^{n} \quad \phi(k) \times [\frac{n}{k}] = \frac{n(n+1)}{2} \tag{5.0.8}$$

$$\Leftrightarrow$$

$$\sum_{k|n} \quad \phi(k) = n \tag{5.0.9}$$

The second formula of the above is the well-known basic formula of sum of divisors. It holds, because taking difference between the first formula in the cases n and $n-1$, $[\frac{n}{k}] - [\frac{n-1}{k}]$ is 1 in the case $k|n$, and is 0 in the case not $k|n$.

6   Conclusions

Elements in a power set are objectified combinations of elements of a source set A. It is interesting that we can formulate the ordinary fact that theorem 2.1 holds among overlapped and joined parts of elements, pairs of relatively not overlapped and separated parts of elements, and pairs of all the elements in a power set.

On abstraction of product of prime numbers, we clarify the fact that the same law as the structure of a power set on the above holds in them, and also we can deeply consider their relationship. This structure also seems a commonly observed form in recognition of natural phenomena.

In addition, on the steps concretizing natural numbers from well-order and abstraction of sum, we can see the structure of the above, abstraction of product of prime numbers, pushed into the inside of natural numbers. Considering natural numbers from this point of view, theorem 2.1 holds from the first step of a power set, and on the second step of abstraction of product of prime numbers, the ratio between overlapped elements and pairs of not overlapped elements and the ratio of elements of the set B, which are primes, in the set C are not determined, however, we can see that they are determined by pushing C into D with h on the last step. Also the distribution of elements of the set B, which are primes, in the set D, in other words, distribution of prime numbers is determined by the same last step of pushing C into D.

The above is just one flow of deduction by consideration which assumes the free ratio between $n(\delta_\gamma)$ and $n(\gamma)$, and assumes premises SUB_A, SUB_B, and the decomposition of natural numbers (C, h, D). However, we have known that at least Euler's totient function and floor function which are deeply concerned to distribution of prime numbers on natural numbers satisfy corollary 5.1 which has its background on corollary 3.1 and theorem 2.1 derived from structure of a power set.

In this paper, we can conclude that we obtain the point of view to consider natural numbers, especially their distribution of prime numbers, with clearly connecting them to the general law about joined parts and pairs of separated parts on a power set by the decomposition of natural numbers (C, h, D).

7   Acknowledgments

References

[1] J. Sebata, *A simple condition of Fermat wiles theorem mainly led by combinatorics*, JP J. Algebra Number Theory Appl. 51(1) (2021), 55-75.

[2] J. Sebata, *Object and Relation, Relational Logic*, Why What How Learn [serial online], `http://www.linktracktool.com/what-why-study/object-relation.html` (accessed 2022-06-24) (in Japanese).

Junya Sebata
n061470@jcom.home.ne.jp

The LaTeX code written by Nik Gjonbalaj, which is distributed by CC BY 4.0, is used with modifications.