On the decomposition of sets of consecutive integers

Junhao Fan

Abstract. In this paper, we study the decomposition of sets of consecutive integers, i.e., how to express the set $\{0, 1, \ldots, mn-1\}$ as the Minkovski sum of two sets, one with m terms and the other with n terms. First, we translate the problem into the language of polynomials. Then we use the properties of cyclotomic polynomials to determine the structure of all the solutions. Then, we deduce formulas for the number of such expressions. Finally, we give an algorithm to calculate the number of such expressions and analyze its computational complexity.

1 Introduction

Here is an interesting combinatorial problem:

Question 1.1. Let $X = (x_{ij})$ be an $m \times n$ matrix such that $\{x_{ij} | 1 \le i \le m, 1 \le j \le n\} = \{0, 1, \ldots, mn-1\}$. We can do the following operations on X: choose any row or column, add 1 or subtract 1 from each element in the chosen row or column. If A can be changed into a zero-matrix (with every entry zero) after finitely many operations, we say that A is "PERFECT". Now the question is how can we find all the "perfect" matrices? What can we say about the number of "perfect" matrices?

A first observation to be made is that the order of operations doesn't affect the outcome. Therefore, we can simply assume that the operations are carried out row by row, then column by column. Suppose all the operations on the ith row subtract a_i from each element in this row, while all the operations on the jth column subtract b_j from each element in this column, here $a_i, b_j \in \mathbb{Z}$ (when $a_i < 0$, it means adding $|a_i|$ to each element in the the ith row, the same for b_j).

We can thus represent any combination of operations by $(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n)$, an $(m+n)$-tuple of integers. If the operations change $X = (x_{ij})$ into a zero-matrix, we have the following equations: $a_i + b_j = x_{ij} (1 \le i \le m, 1 \le j \le n)$.

Furthermore, we notice that doing the operation of subtracting d form each element in a row for all rows is the same as doing the operation of subtracting d form each element in a column for all columns. Therefore, without loss of generosity, we may assume that no operation is done on the row and column containing the entry 0, i.e., there exists $a_{i_0} = b_{j_0} = 0$. Since $x_{ij} \ge 0$, we have $a_i = x_{ij_0} \ge 0$, $b_j = x_{i_0 j} \ge 0$ for every $1 \le i \le m$ and $1 \le j \le n$.

With these observations, we can restate the question as follows:

Question 1.2. Let A, B be two finite sets of integers such that $A + B = \{0, 1, \ldots, mn-1\}$, $|A| = m$, $|B| = n$, $minA = minB = 0$. Here $A + B = \{a + b \mid a \in A, b \in B\}$. What can we say about the structure of (A, B)? What about the number of pairs $(A.B)$?

Date: August, 2016

Key words and Phrases. Decomposition of sets. Cylotomic Polynomials. Combinatorial Enumeration.

The relation between the two questions is clear. The first parts of both questions are equivalent except that the tuples $(a_1, a_2, \ldots, a_m)$, $(b_1, b_2, \ldots, b_n)$ in Question 1.1 are ordered, while the sets A, B in Question 1.2 are not. So, if we write the answer to the second part of Question 1.1 as $G(m, n)$, the answer to the second part of Question 1.2 as $F(m, n)$, we have $G(m, n) = m! \cdot n! \cdot F(m, n)$.

So the combinatorial problem Question 1.1 is essentially a question on the decomposition of sets of consecutive integers. It gives us an interesting combinatorial model and makes it easier to visualize. In the rest of the paper, we will be answering Question 1.2. In Section 2, we will be dealing with the first part of the question, i.e, how to construct all the decompositions. In Section 3, we will be dealing with the second part of the question, i.e., what is the number of different decompositions?

Remark. For the set $\{i, i+1, \ldots, j-1\}$, we can construct its decomposition $A + B$ by first taking $A' + B$ to be the decomposition of $\{0, 1, \ldots, j-i-1\}$, then take $A' = A + i$. So we only need to answer Question 1.2.

To answer Question 1.2, we use the idea of generating function to capture the property of the Minkovski sum: $A + B = \{a + b \mid a \in A, b \in B\}$. Suppose $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$, we define

$$\begin{aligned} P(x) &= x^{a_1} + x^{a_2} + \ldots + x^{a_m}, \\ Q(x) &= x^{b_1} + x^{b_2} + \ldots + x^{b_m}. \end{aligned}$$

Therefore,

$$\begin{aligned} P(x)Q(x) &= (\sum_{i=1}^{m} x^{a_i})(\sum_{j=1}^{n} x^{b_j}) = \sum_{i,j} x^{a_i+b_j} \\ &= 1 + x + x^2 + \ldots + x^{mn-1} = \frac{x^{mn}-1}{x-1}. \end{aligned}$$

We are lead to study the following question, which is exactly the same as Question 1.2:

Question 1.3. $N \geq 2$, $N = mn$. How can we write $\frac{x^N-1}{x-1} = 1 + x + x^2 + \ldots + x^{N-1}$ as the product of two polynomials $P(x)$, $Q(x)$ with $\{0, 1\}$ coefficients such that $P(x)$ has m positive terms and $Q(x)$ has n positive terms? And in how many ways?

Since it is much more convenient to use the language of polynomials, we will stick to the narrative in Question 1.3.

For the first part of the question, our first guess is as follows:

To write $\frac{x^N-1}{x-1}$ as the product of two polynomials with $\{0, 1\}$ coefficients, we do the following steps.

(1) Choose any factorization of N, namely $N = p_1 \ldots p_k$, where p_i are primes, not necessarily distinct. Notice that the order of the primes matters here.

(2) We have the following equality:

$$\frac{x^N-1}{x-1} = \Phi_{p_1}(x)\Phi_{p_2}(x^{p_1})\Phi_{p_3}(x^{p_1 p_2}) \ldots \Phi_{p_k}(x^{p_1 \cdots p_{k-1}}).$$

Here $\Phi_p(x) = \frac{x^p-1}{x-1}$ is the pth cyclotomic polynomial.

(3) We divide all the cyclotomic polynomials $\Phi_{p_i}(x^{p_1 \cdots p_{i-1}})$ into two groups such that the product of indexes of cyclotomic polynomials in each of the two groups is m and n respectively. Take $P(x)$ and $Q(x)$ to be the product of polynomials in one of the two groups respectively.

It is quite obvious that $P(x)$ and $Q(x)$ obtained this way have $\{0,1\}$ coefficients, have m and n positive terms respectively and satisfy $P(x)Q(x) = \frac{x^N-1}{x-1}$. Furthermore, we find out that every pair of polynomials satisfying the condition in Question 1.3 can be obtained in this way. This will be proved in Section 2.

As for the second half of the question, we will deduce formulas for $F(m,n)$ and $H(N)$ in Section 3. Here $F(m,n)$, $mn = N$ is the number of pairs of polynomials satisfying the condition in Question 1.3 and $H(N)$ is the number of pairs of polynomials $(P(x), Q(x))$ with $\{0,1\}$ coefficients whose product is $\frac{x^N-1}{x-1}$, without the restriction on the number of terms in $P(x)$ and $Q(x)$.

2 Construction of the decomposition

In this section, we study the first part of Question 1.3 and give a rigorous proof of our main result Proposition 2.4 and Corollary 2.5.

Question 2.1. $N \geq 2$. How can we write $\frac{x^N-1}{x-1} = 1 + x + x^2 + \ldots + x^{N-1}$ as the product of two polynomials $P(x)$, $Q(x)$ with $\{0,1\}$ coefficients such that $P(x)$ has m positive terms and $Q(x)$ has n positive terms?

It is helpful to remove the restriction on the number of positive terms at first. After we give Proposition 2.4, it is easy to add this further restriction as in Corollary 2.5.

We shall first look at some special cases:

Case. $N = p^\alpha$, p is a prime, $\alpha \in \mathbb{N}$.

$$\frac{x^{p^\alpha}-1}{x-1} = \frac{x^p-1}{x-1} \cdot \frac{x^{p^2}-1}{x^p-1} \cdot \ldots \cdot \frac{x^{p^\alpha}-1}{x^{p^{\alpha-1}}-1} = \Phi_p(x)\Phi_{p^2}(x)\ldots\Phi_{p^\alpha}(x)$$

Throughout the paper, $\Phi_n(x)$ is the nth cyclotomic polynomial.

Since $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$ for any $n \in \mathbb{Z}^+$, if $\frac{x^{p^\alpha}-1}{x-1} = P(x)Q(x)$, then we can divide these cyclotomic polynomials on the right hand side into two groups such that $P(x)$ is the product of the polynomials in one group and $Q(x)$ is the product of the polynomials in another group.

The product of any collection of polynomials on the right hand side of the equality above has $\{0,1\}$ coefficients, since for $I \subset \{1,2,\ldots,\alpha\}$, we have

$$\prod_{i\in I} \Phi_{p^i}(x) = \sum_j x^j.$$

Here, the summation runs over all j such that $j = \sum_{i\in I} e_i p^{i-1}, e_i \in \{0,1,\ldots,p-1\}$.

Therefore, polynomials $P(x)$ and $Q(x)$ with $\{0,1\}$ coefficients satisfy $\frac{x^{p^\alpha}-1}{x-1} = P(x)Q(x)$ if and only if there exists some partition I, J of $\{1,2,\ldots,\alpha\}$, i.e., $I \cup J = \{1,2,\ldots,\alpha\}$, $I \cap J = \varnothing$, such that

$$P(x) = \prod_{i\in I} \Phi_{p^i}(x),$$
$$Q(x) = \prod_{j\in J} \Phi_{p^j}(x).$$

The idea of using generating functions are extremely useful when N is a power of prime, since every irreducible factor of $\frac{x^{p^\alpha}-1}{x-1}$ has $\{0,1\}$ coefficients. But the problem becomes more complex when N has different prime factors.

Case. $N = 12$

$$\frac{x^{12}-1}{x-1} = \Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x)$$

In this case, $\Phi_6(x) = 1 - x + x^2$ and $\Phi_{12}(x) = 1 - x^2 + x^4$ do not have $\{0, 1\}$ coefficients.

If $\frac{x^{12}-1}{x-1} = P(x)Q(x)$, we can still divide these cyclotomic polynomials on the right hand side into two groups such that $P(x)$ is the product of the polynomials in one group and $Q(x)$ is the product of the polynomials in another group. The problem is that not every way of dividing these polynomials gives us $P(x)$ and $Q(x)$ with $\{0, 1\}$ coefficients.

For example,

$$\Phi_2(x)\Phi_{12}(x) = 1 + x - x^2 - x^3 + x^4 + x^5,$$
$$\Phi_3(x)\Phi_{12}(x) = 1 + x - x^3 + x^5 + x^6.$$

It is difficult to determine how can we divide the cyclotomic polynomials into two goups so that the product of each group has $\{0, 1\}$ coefficients. So we have to find more properties of $P(x)$ and $Q(x)$.

Lemma 2.2. For $N \geq 2$, if polynomials $P(x), Q(x)$ with $\{0, 1\}$ coefficients satisfy $\frac{x^N-1}{x-1} = P(x)Q(x)$, then there exists an integer $d \mid N, d > 1$ such that $\frac{x^d-1}{x-1} \mid P(x)$ and $\frac{P(x)(x-1)}{x^d-1}$ has $\{0, 1\}$ coefficients. (or $\frac{x^d-1}{x-1} \mid Q(x)$ and $\frac{Q(x)(x-1)}{x^d-1}$ has $\{0, 1\}$ coefficients.)

Proof. Suppose $P(x) = x^{a_1} + x^{a_2} + \ldots + x^{a_m}$, $Q(x) = x^{b_1} + x^{b_2} + \ldots + x^{b_n}$, $(0 = a_1 < a_2 < \ldots < a_m$, $0 = b_1 < b_2 < \ldots < b_n)$. Then, $\{a_i + b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\} = \{0, 1, \ldots, mn-1\}$.

Construct matrix $X = (x_{ij})$ such that $x_{ij} = a_i + b_j (1 \leq i \leq m, 1 \leq j \leq n)$. So $\{x_{ij}\} = \{0, 1, \ldots, mn-1\}$.

Notice that the entries in each row are in increasing order from left to right and the entries in each column are in increasing order from top to bottom.

Thus either $x_{12} = 1$ or $x_{21} = 1$. Without loss of generosity, we may assume that $x_{12} = 1$, thus $a_2 = 1$.

Suppose d is the smallest integer that is not in the first row of the matrix. Then $x_{1j} = j - 1, (1 \leq j \leq d)$ and $x_{21} = d$.

We want to show that the first row consists of blocks of d consecutive integers.

Suppose that this is true for the first kd $(k \geq 1)$ entries, i.e, $x_{1(id+j)} = x_{1(id+1)} + j - 1, (0 \leq i \leq k-1, 1 \leq j \leq d)$, while the next d entries are not consecutive integers, i.e, there exists an integer $1 \leq t < d$ such that $x_{1(kd+t+1)} > x_{1(kd+t)} + 1$. We may assume that t is the smallest integer satisfying this condition. Thus, $x_{1(kd+j)} = x_{1(kd+1)} + j - 1, (1 \leq j \leq t)$ but $x_{1(kd+t+1)} > x_{1(kd+t)} + 1$.

Since $x_{1(kd+1)} < x_{1(kd+t)} + 1 < x_{1(kd+t+1)}$, $x_{1(kd+t)} + 1$ must be somewhere in the matrix. Suppose $x_{i_0 j_0} = x_{1(kd+t)} + 1$.

(1) $j_0 > kd + t$

then we have $x_{i_0 j_0} \geq x_{1(kd+t+1)} > x_{1(kd+t)} + 1$, thus leading to a contradiction.

(2) $kd + 1 \leq j_0 \leq kd + t$

if $i_0 = 1$, we have $x_{i_0 j_0} \leq x_{1(kd+t)} < x_{1(kd+t)} + 1$, thus leading to a contradiction, if $i_0 \geq 2$, we have

$$\begin{aligned} x_{i_0 j_0} &\geq x_{2(kd+1)} = a_2 + b_{kd+1} \\ &= (a_2 + b_1) + (a_1 + b_{kd+1}) - (a_1 + b_1) \\ &= x_{21} + x_{1(kd+1)} = x_{1(kd+1)} + d \\ &= x_{1(kd+t)} + d - t + 1 \\ &> x_{1(kd+t)} + 1 \end{aligned}$$

thus leading to a contradiction.

(3) $j_0 \leq kd$

Notice that the first kd entries of each row consists of k blocks of d consecutive integers. If s is an entry in the first kd columns, and $s \in [s', s' + d]$ then either s' or $s' + d$ is also an entry in the first kd columns. However, $x_{1(kd+1)} < x_{1(kd+t)} + 1 < x_{1(kd+t+1)} < x_{1(kd+1)} + d = x_{2(kd+1)}$, and neither $x_{1(kd+1)}$ nor $x_{2(kd+1)}$ is in the first kd column, thus leading to a contradiction.

So we have proved that the first row consists of blocks of d consecutive integers, and so does each other row in the matrix.

Therefore $d|m$ and

$$\begin{aligned} P(x) &= x^{a_1} + x^{a_2} + \ldots + x^{a_m} \\ &= (1 + x + x^2 + \ldots + x^{d-1})(x^{a_1} + x^{a_{d+1}} + x^{a_{2d+1}} + \ldots + x^{a_{m-d+1}}) \end{aligned}$$

that is to say $\frac{x^d-1}{x-1} \mid P(x)$ and $\frac{P(x)(x-1)}{x^d-1}$ has $\{0, 1\}$ coefficients. □

The following lemma allow us to continually factorizing $P(x)$ and $Q(x)$ into products of polynomials with $\{0, 1\}$ coefficients according to Lemma 2.2.

Lemma 2.3. $N \geq 2$. If polynomials $P(x) = x^{a_1} + x^{a_2} + \ldots + x^{a_m}$, $Q(x) = x^{b_1} + x^{b_2} + \ldots + x^{b_n}$, $(0 = a_1 < a_2 < \ldots < a_m,\ 0 = b_1 < b_2 < \ldots < b_n)$ satisfy $\frac{x^N-1}{x^d-1} = P(x)Q(x)$, $(d \mid N)$, then we have $d|a_i$ for every $1 \leq i \leq m$ and $d|b_j$ for every $1 \leq j \leq n$.

Proof. The proof is straightforward. Since $P(x)Q(x) = \sum_{(i,j)} x^{a_i+b_j}$, we have $d \mid a_i + b_j$ for every (i, j). Taking $i = 0$ or $j = 0$, we have $d \mid a_i$ for every $1 \leq i \leq m$ and $d \mid b_j$ for every $1 \leq j \leq n$. □

Notice that if $d = p_1 \ldots p_l$, where p_i are primes, not necessarily distinct, then

$$\frac{x^d - 1}{x - 1} = \prod_{i=1}^{l} \Phi_{p_i}(x^{p_1 \cdots p_{i-1}}).$$

By Lemma 2.2 and Lemma 2.3, we can break down $P(x)$ and $Q(x)$ into products of $\Phi_p(x^t)$.

Proposition 2.4. $N \geq 2$. Polynomials $P(x), Q(x)$ with $\{0, 1\}$ coefficients satisfy $\frac{x^N-1}{x-1} = P(x)Q(x)$ if and only if

$$\begin{aligned} P(x) &= \prod_{i \in I} \Phi_{p_i}(x^{p_1 \cdots p_{i-1}}), \\ Q(x) &= \prod_{j \in J} \Phi_{p_j}(x^{p_1 \cdots p_{j-1}}), \end{aligned}$$

where $N = p_1 \ldots p_k$, and the p_i are primes, not necessarily distinct, and I, J are any partition of $\{1, 2, \ldots, k\}$, i.e., $I \cup J = \{1, 2, \ldots, k\}$, $I \cap J = \varnothing$.

Proof. First we prove that if

$$P(x)=\prod_{i\in I}\Phi_{p_i}(x^{p_1\cdots p_{i-1}}),\ \ Q(x)=\prod_{j\in J}\Phi_{p_j}(x^{p_1\cdots p_{j-1}}).$$

then $P(x),Q(x)$ have $\{0,1\}$ coefficients and satisfy $\frac{x^N-1}{x-1}=P(x)Q(x)$.

We only need to prove that $P(x)$ has $\{0,1\}$ coefficients, the proof for $Q(x)$ is exactly the same.

Suppose $I=\{i_1,i_2,\dots,i_s\}$ we have

$$P(x)=\prod_{t=1}^{s}\Phi_{p_{i_t}}(x^{p_1\cdots p_{i_t-1}})=\sum_j x^j.$$

Here, the summation runs over all j such that $j=\sum_t e_{i_t}\cdot p_1\dots p_{i_t-1}, e_{i_t}\in\{0,1,\dots,p_{i_t}-1\}$.

Now we only need to show that the terms in the summation are distinct, if

$$\sum_{t=1}^{s}e_{i_t}\cdot p_1\dots p_{i_t-1}=\sum_{t=1}^{s}f_{i_t}\cdot p_1\dots p_{i_t-1}.$$

and there exists integer $1\le t\le s$ such that $e_{i_t}\ne f_{i_t}$

Suppose t_0 is the smallest integer such that $e_{i_{t_0}}\ne f_{i_{t_0}}$,we have

$$\sum_{t=1}^{s}e_{i_t}\cdot p_1\dots p_{i_t-1}\not\equiv\sum_{t=1}^{s}f_{i_t}\cdot p_1\dots p_{i_t-1}\ (\textbf{mod}\ p_1\dots p_{i_{t_0}}).$$

thus leading to a contradiction.

Therefore, $P(x)$ has $\{0,1\}$ coefficients, so does $Q(x)$.

The second statement is obvious, since

$$P(x)Q(x)=\prod_{i=1}^{k}\Phi_{p_i}(x^{p_1\cdots p_{i-1}})=\frac{x^N-1}{x-1}.$$

Next we prove that if polynomials $P(x),Q(x)$ have $\{0,1\}$ coefficients and $\frac{x^N-1}{x-1}=P(x)Q(x)$ then

$$P(x)=\prod_{i\in I}\Phi_{p_i}(x^{p_1\cdots p_{i-1}}),\ \ Q(x)=\prod_{j\in J}\Phi_{p_j}(x^{p_1\cdots p_{j-1}}),$$

for some order of prime factorization of N, $N=p_1\dots p_k$, and some partition I, J of $\{1,2,\dots,k\}$.

If $N=p_1\dots p_k$, p_i primes, not necessarily distinct, define $\Omega(N)=k$ for $N>1$ and $\Omega(1)=0$.

We prove the statement by induction on $\Omega(N)$.

If $\Omega(N)=1$, the case is trivial.

If the statement holds for all N such that $\Omega(N)<k$, we need to prove that it also holds for all N such that $\Omega(N)=k$.

Let $N=p_1\dots p_k$. By Lemma 2.2, then there exists an integer $d\mid N, d>1$ such that $\frac{x^d-1}{x-1}\mid P(x)$ and $\frac{P(x)(x-1)}{x^d-1}$ has $\{0,1\}$ coefficients. (or $\frac{x^d-1}{x-1}\mid Q(x)$ and $\frac{Q(x)(x-1)}{x^d-1}$ has $\{0,1\}$ coefficients.)

Without loss of generosity, assume $\frac{x^d-1}{x-1}\mid P(x)$ and $\frac{P(x)(x-1)}{x^d-1}$ has $\{0,1\}$ coefficients. We may further assume that $d=p_1\dots p_l$ for some $1\le l\le k$.

Let $P_1(x) = \frac{P(x)(x-1)}{x^d-1}$, then $P_1(x)Q(x) = \frac{x^N-1}{x^d-1}$.

By Lemma 2.3, there exists polynomials $P'(x)$ and $Q'(x)$ with $\{0,1\}$ coefficients such that $P'(x^d) = P_1(x)$, $Q'(x^d) = Q(x)$.

Thus we have

$$P'(x^d)Q'(x^d) = \frac{x^N-1}{x^d-1} = \frac{(x^d)^{\frac{N}{d}}-1}{(x^d)-1}.$$

Therefore,

$$P'(x)Q'(x) = \frac{x^{\frac{N}{d}}-1}{x-1}.$$

Since $\Omega(\frac{N}{d}) = k-l < k$, by our assumption, there exists some order of prime factorization of $\frac{N}{d}$, $\frac{N}{d} = q_1 \dots q_{k-l}$ and some partition I', J' of $\{1,2,\dots,k-l\}$ such that

$$P'(x) = \prod_{i\in I'} \Phi_{q_i}(x^{q_1\cdots q_{i-1}}),\ \ Q'(x) = \prod_{j\in J'} \Phi_{q_j}(x^{q_1\cdots q_{j-1}}),$$

Thus we have

$$\begin{aligned} P(x) &= \frac{x^d-1}{x-1} \cdot \prod_{i\in I'} \Phi_{q_i}((x^d)^{q_1\cdots q_{i-1}}), \\ &= \prod_{i=1}^{l} \Phi_{p_i}(x^{p_1\cdots p_{i-1}}) \prod_{i\in I'} \Phi_{q_i}(x^{p_1\cdots p_l q_1\cdots q_{i-1}}) \\ Q(x) &= \prod_{j\in J'} \Phi_{q_i}(x^{p_1\cdots p_l q_1\cdots q_{j-1}}), \end{aligned}$$

Since $\frac{N}{d} = q_1 \dots q_{k-l} = p_{l+1} \dots p_k$, $q_1, \dots, q_{k-l}$ is just a permutation of $p_{l+1}, \dots, p_k$, there exists a permutation σ of $\{l+1, l+2, \dots, k\}$ such that $q_r = p_{\sigma(l+r)}$ for $1 \le r \le k-l$.

Then

$$P(x) = \prod_{i\in I} \Phi_{p_i}(x^{p_1\cdots p_{i-1}}),\ \ Q(x) = \prod_{j\in J} \Phi_{p_j}(x^{p_1\cdots p_{j-1}}),$$

for the factorization $N = p_1 \dots p_l p_{\sigma(l+1)} \dots p_{\sigma(k)}$ and the partition I, J of $\{1,2,\dots,k\}$, in which $I = \{1,\dots,l\} \cup \{\sigma(l+i) \mid i \in I'\}$, $J = \{\sigma(l+j) \mid j \in J'\}$.

We have thus completed the induction. ☐

Corollary 2.5. $N \ge 2$. Polynomials $P(x), Q(x)$ with $\{0,1\}$ coefficients have m and n positive terms respectively and satisfy $\frac{x^N-1}{x-1} = P(x)Q(x)$ if and only if

$$\begin{aligned} P(x) &= \prod_{i\in I} \Phi_{p_i}(x^{p_1\cdots p_{i-1}}), \\ Q(x) &= \prod_{j\in J} \Phi_{p_j}(x^{p_1\cdots p_{j-1}}), \end{aligned}$$

where $N = p_1 \dots p_k$, and the p_i are primes, not necessarily distinct, and I, J are any partition of $\{1,2,\dots,k\}$, i.e., $I \cup J = \{1,2,\dots,k\}$, $I \cap J = \varnothing$ such that $\prod_{i\in I} p_i = m$ and $\prod_{j\in J} p_j = n$.

This completes our classification as well as the construction of the decompositions of sets of consecutive integers.

3 Enumeration of the decomposition

Definition 3.1. $N \geq 2$. Define $H(N)$ to be the number of pairs of polynomials $(P(x), Q(x))$ with $\{0,1\}$ coefficients satisfying $\frac{x^N-1}{x-1} = P(x)Q(x)$.

Definition 3.2. Define $F(m,n)$ to be the number of pairs of polynomials $(P(x), Q(x))$ with $\{0,1\}$ coefficients satisfying $\frac{x^N-1}{x-1} = P(x)Q(x)$ and that $P(x)$ and $Q(x)$ has m and n terms respectively.

In this section, our aim is to give a satisfactory answer to the following question based on Proposition 2.4:

Question 3.3. Find $H(N)$ $(N \geq 2)$ and $F(m,n)$.

We have the following relationship between $H(N)$ and $F(m,n)$ as an immediate result of their definitions.

Proposition 3.4. $N \geq 2$. $H(N) = \sum_{d|N} F(d, \frac{N}{d})$.

Notice that in Proposition 2.4, different factorizations of N may result in the same $P(x)$ and $Q(x)$.

For example, when $N = 12$, let $N = p_1p_2p_3$. Take one factorization to be $p_1 = p_3 = 2, p_2 = 3$, with partition $I = \{1,2\}, J = \{3\}$. Then we have $P(x) = \Phi_2(x)\Phi_3(x^2)$, $Q(x) = \Phi_2(x^6)$. Take the other factorization to be $p_1 = 3, p_2 = p_3 = 2$, with the same partition $I = \{1,2\}, J = \{3\}$. Then we have $P(x) = \Phi_3(x)\Phi_2(x^3)$, $Q(x) = \Phi_2(x^6)$.

Since $\Phi_2(x)\Phi_3(x^2) = \Phi_6(x) = \Phi_3(x)\Phi_2(x^3)$, the factorizations have the same $P(x)$ and $Q(x)$.

The following corollary of Proposition 2.4 helps us to compute $H(N)$ and $F(m,n)$:

Corollary 3.5. $N \geq 2$. Polynomials $P(x), Q(x)$ with $\{0,1\}$ coefficients satisfy $\frac{x^N-1}{x-1} = P(x)Q(x)$ if and only if there exists a unique sequence of integers $d_1, d_2 \ldots, d_s > 1$ such that $N = d_1d_2 \ldots d_s$ and exactly one of the following holds:

$$P(x) = \prod_{2\nmid t} \frac{x^{d_1\ldots d_t}-1}{x^{d_1\ldots d_{t-1}}-1}, \ Q(x) = \prod_{2|t} \frac{x^{d_1\ldots d_t}-1}{x^{d_1\ldots d_{t-1}}-1}, \tag{1}$$

or

$$P(x) = \prod_{2|t} \frac{x^{d_1\ldots d_t}-1}{x^{d_1\ldots d_{t-1}}-1}, \ Q(x) = \prod_{2\nmid t} \frac{x^{d_1\ldots d_i t}-1}{x^{d_1\ldots d_{t-1}}-1}. \tag{2}$$

Proof. First, if such sequence of integers exists, then we can simply expand d_t into product of primes, and by Proposition 2.4, we know that $P(x), Q(x)$ have $\{0,1\}$ coefficients and satisfy $\frac{x^N-1}{x-1} = P(x)Q(x)$.

Next, we prove that for every $P(x), Q(x)$, we can find a sequence so that (1) or (2) holds.

Since we have

$$\begin{aligned}\prod_{l=i+1}^{j} \Phi_{p_l}(x^{p_{i+1}\ldots p_{l-1}}) &= 1 + x + x^2 + \ldots + x^{p_{i+1}\ldots p_j - 1} \\ &= \frac{x^{p_{i+1}\ldots p_j}-1}{x-1},\end{aligned}$$

taking $x = x^{p_1 \cdots p_i}$, we have

$$\prod_{l=i+1}^{j} \Phi_{p_l}(x^{p_1 \cdots p_{l-1}}) = \frac{x^{p_1 \cdots p_j} - 1}{x^{p_1 \cdots p_i} - 1}. \tag{3}$$

Without loss of generosity, we may assume that $\Phi_{p_1}(x) \mid P(x)$. In this case, we prove that $P(x)$ and $Q(x)$ satisfy (1), while in the other case, $P(x)$ and $Q(x)$ satisfy (2).

Let i_1 be the largest integer such that

$$\prod_{l=1}^{i_1} \Phi_{p_l}(x^{p_1 \cdots p_{l-1}}) \mid P(x).$$

Then $\Phi_{p_{i_1+1}}(x^{p_1 \cdots p_{i_1}}) \nmid P(x)$, therefore $\Phi_{p_{i_1+1}}(x^{p_1 \cdots p_{i_1}}) \mid Q(x)$.

Let i_2 be the largest integer such that

$$\prod_{l=i_1+1}^{i_2} \Phi_{p_l}(x^{p_1 \cdots p_{l-1}}) \mid Q(x).$$

Then $\Phi_{p_{i_2+1}}(x^{p_1 \cdots p_{i_2}}) \nmid Q(x)$, therefore $\Phi_{p_{i_2+1}}(x^{p_1 \cdots p_{i_2}}) \mid P(x)$.

We can continue this process until $i_s = k$. Now we have a sequence $i_0 = 0 < i_1 < \ldots < i_s = k$ such that

$$\prod_{l=i_t+1}^{i_{t+1}} \Phi_{p_l}(x^{p_1 \cdots p_{l-1}})2 \mid P(x) \ (2 \mid t), \quad \prod_{l=i_t+1}^{i_{t+1}} \Phi_{p_l}(x^{p_1 \cdots p_{l-1}})2 \mid Q(x) \ (2 \nmid t).$$

Let $d_t = p_{i_{t-1}+1} \ldots p_{i_t}$ for $1 \le t \le s$, then by (3),

$$\prod_{l=i_{t-1}+1}^{i_t} \Phi_{p_l}(x^{p_1 \cdots p_{l-1}}) = \frac{x^{p_1 \cdots p_{i_t}} - 1}{x^{p_1 \cdots p_{i_{t-1}}} - 1} = \frac{x^{d_1 \ldots d_t} - 1}{x^{d_1 \ldots d_{t-1}} - 1}.$$

Therefore $N = d_1 d_2 \ldots d_s$, and

$$P(x) = \prod_{2 \nmid t} \frac{x^{d_1 \ldots d_t} - 1}{x^{d_1 \ldots d_{t-1}} - 1}, \ Q(x) = \prod_{2 \mid t} \frac{x^{d_1 \ldots d_t} - 1}{x^{d_1 \ldots d_{t-1}} - 1}.$$

Finally, we prove the uniqueness of the sequence.

If we have two distinct sequences $d_1, d_2 \ldots, d_s > 1$ and $d'_1, d'_2 \ldots, d'_{s'} > 1$ such that $N = d_1 d_2 \ldots d_s = d'_1 d'_2 \ldots d'_{s'}$ and

$$P(x) = \prod_{2 \nmid t} \frac{x^{d_1 \ldots d_t} - 1}{x^{d_1 \ldots d_{t-1}} - 1}, \ Q(x) = \prod_{2 \mid t} \frac{x^{d_1 \ldots d_t} - 1}{x^{d_1 \ldots d_{t-1}} - 1}.$$

$$P'(x) = \prod_{2 \nmid t} \frac{x^{d'_1 \ldots d'_t} - 1}{x^{d'_1 \ldots d'_{t-1}} - 1}, \ Q'(x) = \prod_{2 \mid t} \frac{x^{d'_1 \ldots d'_t} - 1}{x^{d'_1 \ldots d'_{t-1}} - 1}.$$

Let t be the smallest integer such that $d_t \neq d'_t$. Without loss of generosity, we may assume that $d_t > d'_t$

(1) $2 \nmid t$, then $P(x)$ has the term $x^{d'_1 d'_2 \ldots d'_t}$, but $P'(x)$ hasn't. So $P(x) \neq P'(x)$.

(2) $2 \mid t$, then $Q(x)$ has the term $x^{d'_1 d'_2 \ldots d'_t}$, but $Q'(x)$ hasn't. So $Q(x) \neq Q'(x)$.

Therefore, we have proved the uniqueness of the sequence $d_1, d_2 \ldots, d_s$ corresponding to $P(x), Q(x)$. $\square$

By corollary 3.5, every sequence of integers $d_1, d_2 \dots, d_s > 1$ such that $N = d_1 d_2 \dots d_s$ corresponds to exactly two pairs of polynomials $(P(x), Q(x))$ and each $(P(x), Q(x))$ only corresponds to exactly one sequence. So the number of $(P(x), Q(x))$ is twice the number of sequences $d_1, d_2 \dots, d_s$.

Definition 3.6. Define $\widetilde{\Delta}(N) := \{(d_1, \dots, d_s) \mid s \in \mathbb{Z}^+, d_1, d_2, \dots, d_s > 1, N = d_1 d_2 \dots d_s\}$ for $N \geq 2$ and $\widetilde{\Delta}(1) := \{()\}$, in which the only element is the empty sequence.

$H(1)$ is not defined. For the sake of convenience, we define $H(1) = 2$. Then we have,

Corollary 3.7. For $N \in \mathbb{Z}^+$, $H(N) = 2|\widetilde{\Delta}(N)|$.

Proposition 3.8. $|\widetilde{\Delta}(N)| = \sum_{d|N, d<N} |\widetilde{\Delta}(d)|$.

Proof. It is obvious that $\widetilde{\Delta}(N)$ are disjoint.

Let $X = \bigcup_{d|N, d<N} \widetilde{\Delta}(d)$, then $|X| = \sum_{d|N, d<N} |\widetilde{\Delta}(d)|$.

Define map $f : \widetilde{\Delta}(N) \to X$ by $(d_1, d_2, \dots, d_s) \mapsto (d_1, d_2, \dots, d_{s-1})$. It is injective and surjective, therefore bijective. So we have $|\widetilde{\Delta}(N)| = |X|$, thus $|\widetilde{\Delta}(N)| = \sum_{d|N, d<N} |\widetilde{\Delta}(d)|$. $\square$

Therefore $H(N) = \sum_{d|N, d<N} H(d)$. We have thus obtained the recurrence formula for $H(N)$.

Proposition 3.9. $H(N)$ is given by the recurrence formula

$$H(N) = \sum_{d|N, d<N} H(d), \ H(1) = 2.$$

Definition 3.10. For $N \geq 2$. Define $\Delta(N, k) := \{(d_1, \dots, d_k) \mid d_1, \dots, d_k > 1, N = d_1 d_2 \dots d_k\}$ and $D_k(N) := |\Delta(N, k+1)|$.

Definition 3.11. For $N \geq 2$. Define $\delta(N, k) := \{(d_1, \dots, d_k) \mid d_1, \dots, d_k \in \mathbb{Z}^+, N = d_1 d_2 \dots d_k\}$ and $d_k(N) := |\delta(N, k+1)|$.

We first compute $d_k(N)$, then give a formula for $D_k(N)$ based on $d_k(N)$, and finally give a formula for $H(N)$.

Proposition 3.12. If $N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, where $\alpha_i \geq 1$ and p_i are distinct primes, then

$$d_k(N) = \prod_{i=1}^{s} \binom{\alpha_i + k}{k}.$$

Proof. First, we prove that $d_k(N)$ is multiplicative.

If $N = mn$ and $gcd(m, n) = 1$. Define a map $f : \delta(N, k+1) \to \delta(m, k+1) \times \delta(n, k+1)$by $(d_1, \dots, d_{k+1}) \mapsto [(gcd(d_1, m), \dots, gcd(d_{k+1}, m)), (gcd(d_1, n), \dots, gcd(d_{k+1}, n))]$. It is easy to check that f is bijective, thus $d_k(N) = d_k(m) d_k(n)$.

Next, we prove that $d_k(p^\alpha) = \binom{\alpha + k}{k}$.

Notice that $d_k(p^\alpha)$ is equal to the number of ways to put α objects into k boxes and empty boxes are allowed, which is known to be $\binom{\alpha + k}{k}$.

Therefore we have

$$d_k(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}) = \prod_{i=1}^{s} \binom{\alpha_i + k}{k}.$$

$\square$

Proposition 3.13. For $N \geq 2$,

$$D_k(N) = \sum_{i=0}^{k} (-1)^i \binom{k+1}{i} d_{k-i}(N).$$

Proof. Define $X_j = \{(d_1, \ldots, d_{k+1}) \in \delta \mid d_j = 1\} \subset \delta(N,k)$ for every $1 \leq j \leq k+1$. Then $\Delta(N,k) = \delta(N,k) - \bigcup_j X_j$.

Note that

$$|\bigcap_{1\leq t\leq s} X_{j_t}| = |\{(d_1, \ldots, d_{k+1}) \in \delta(N,k) \mid d_{j_1} = \ldots = d_{j_s} = 1\}| = d_{k-s}(N).$$

According to the inclusion-exclusion principle,

$$\begin{aligned} |\bigcup_j X_j| &= \sum_j |X_j| - \sum_{j_1,j_2} |X_{j_1} \cap X_{j_2}| + \ldots + (-1)^k |\bigcap_j X_j| \\ &= \binom{k+1}{1} d_{k-1}(N) - \binom{k+1}{2} d_{k-2}(N) + \ldots + \binom{k+1}{k} d_0(N) \\ &= \sum_{i=1}^{k} (-1)^{i-1} \binom{k+1}{i} d_{k-i}(N). \end{aligned}$$

Therefore

$$D_k(N) = d_k(N) - |\bigcup_j X_j| = \sum_{i=0}^{k} (-1)^i \binom{k+1}{i} d_{k-i}(N).$$

□

Proposition 3.14. If $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, let $A_0 = \alpha_1 + \alpha_2 + \ldots + \alpha_s$.

$$H(N) = 2 \sum_{k=0}^{A_0} \sum_{i=0}^{k} (-1)^i \binom{k+1}{i} d_{k-i}(N).$$

Proof. According to the Definition 3.6 and 3.10, we have $\widetilde{\Delta}(N) = \bigcup_{k=0}^{A_0} \Delta(N,k)$.

Since $\Delta(N,k)$ are disjoint, we have $|\widetilde{\Delta}(N)| = \sum_{k=0}^{A_0} D_k(N)$.

By Corollary 3.7 and Proposition 3.13,

$$\begin{aligned} H(N) = 2|\widetilde{\Delta}(N)| &= 2 \sum_{k=0}^{A_0} D_k(N) \\ &= 2 \sum_{k=0}^{A_0} \sum_{i=0}^{k} (-1)^i \binom{k+1}{i} d_{k-i}(N). \end{aligned}$$

□

Corollary 3.15. Under the assumption of proposition 3.14, for any integer $A \geq A_0$,

$$H(N) = 2 \sum_{k=0}^{A} \sum_{i=0}^{k} (-1)^i \binom{k+1}{i} d_{k-i}(N).$$

Proof. Notice that when $k > A_0$, $\Delta(N,k) = \varnothing$, thus $D_k(N) = 0$.

So we have

$$\begin{aligned} H(N) &= 2\sum_{k=0}^{A_0} D_k(N) = 2\sum_{k=0}^{A} D_k(N) \\ &= 2\sum_{k=0}^{A}\sum_{i=0}^{k}(-1)^i\binom{k+1}{i}d_{k-i}(N). \end{aligned}$$

□

Next, we give formulas for $F(m,n)$.

Definition 3.16. For $m \geq 2$ or $n \geq 2$, define $T(m,n)$ to be the set of sequences $(d_1,\ldots,d_s)$ such that $s \in \mathbb{Z}^+$, $d_1, d_2, \ldots, d_s > 1$, $m = \prod_{2\nmid i} d_i, n = \prod_{2|i} d_i$ or $m = \prod_{2|i} d_i, n = \prod_{2\nmid i} d_i$. Define $T(1,1) := \{()\}$, in which the only element is the empty sequence.

The following equality results from Corollary 3.5.

Corollary 3.17. $F(m,n) = |T(m,n)|$.

In order to have a more intuitive understanding of $T(m,n)$. We construct a representation of $T(m,n)$ by a certain type of lattice walking on $\mathbb{Z}^2$.

Consider the path from $(1,1)$ to (m,n) along the lines $x = k$ or $y = k$, where $k \in \mathbb{Z}$. For every step, one can only walks along the positive direction of x-axis so that the x-coordinate of the endpoint is a multiplier of the x-coordinate of the initial point or along the positive direction of y-axis so that the y-coordinate of the endpoint is a multiplier of the y-coordinate of the initial point. Furthermore, one must take turns going in the x-direction and the x-direction, i.e., two adjacent steps can't be in the same direction. We say a path from $(1,1)$ to (m,n) is a "arithmetical path" if it satisfies the rules above.

Assume that the endpoint of the ith step is (x_i, y_i) and let $(x_0, y_0) = (1,1)$. Define a map from the set of paths just introduced to $T(m,n)$ by defining $d_i = x_i/x_{i-1}$ if the ith step is in the x-direction and $d_i = y_i/y_{i-1}$ if the ith step is in the y-direction. It is easy to check that the map thus defined is a bijection. Therefore, $F(m,n)$ is the number of arithmetical paths from $(1,1)$ to (m,n).

Proposition 3.18. F(m,n) is given by the following recurrence formula

$$\begin{aligned} &F(m,n) = -[\sum_{d|m,d>1}\mu(d)F(\frac{m}{d},n) + \sum_{d|n,d>1}\mu(d)F(m,\frac{n}{d})], \\ &F(m,1) = F(1,n) = F(1,1) = 1. \end{aligned}$$

for $m \geq 2$ and $n \geq 2$. Here, $\mu(d)$ is the Möbius function.

Proof. Every arithmetical path from $(1,1)$ to (m,n) either passes $(m-1,n)$ or $(m,n-1)$.

We prove that the number of arithmetical paths passing $(m-1,n)$ is $-\sum_{d|m,d>1}\mu(d)F(\frac{m}{d},n)$.

For every path passing $(m-1,n)$, there exists a prime $p \mid m$ such that the path passes $(\frac{m}{p},n)$. Suppose $m = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, let X_i be the set of paths passing $(\frac{m}{p_i},n)$.

According to the inclusion-exclusion principle, the number of arithmetical paths passing the point $(m-1,n)$ is

$$\begin{aligned}
|\bigcup_i X_i| &= \sum_i |X_i| - \sum_{i_1,i_2} |X_{i_1} \cap X_{i_2}| + \ldots + (-1)^k |\bigcap_i X_i| \\
&= \sum_i F(\frac{m}{p_i}, n) - \sum_{i1,i2} F(\frac{m}{p_{i_1}p_{i_2}}, n) + \ldots + (-1)^k F(\frac{m}{p_{i_1}\ldots p_{i_k}}, n) \\
&= \sum_{d|m,d>1} [-\mu(d)] F(\frac{m}{d}, n) \\
&= -\sum_{d|m,d>1} \mu(d) F(\frac{m}{d}, n).
\end{aligned}$$

Similarly, we can prove that the number of arithmetical paths passing the point $(m,n-1)$ is $-\sum_{d|n,d>1}\mu(d)F(m,\frac{n}{d})$.

Therefore, for $m \geq 2$ and $n \geq 2$,

$$F(m,n) = -[\sum_{d|m,d>1} \mu(d)F(\frac{m}{d},n) + \sum_{d|n,d>1} \mu(d)F(m,\frac{n}{d})].$$

It is easy to check that $F(m,1) = F(1,n) = F(1,1) = 1$ for $m \geq 2$ and $n \geq 2$. □

Proposition 3.19. If m, n have prime factorization $m = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$, $n = q_1^{\beta_1}q_2^{\beta_2}\ldots q_t^{\beta_t}$, then $F(m,n)$ is equal to the coefficient of $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_s^{\alpha_s}y_1^{\beta_1}y_2^{\beta_2}\ldots y_t^{\beta_t}$ in the generating function

$$\frac{1}{\prod_{i=1}^{\infty}(1-x_i) + \prod_{i=1}^{\infty}(1-y_i) - 1}.$$

Proof. Let

$$g(x_1,x_2\ldots,y_1,y_2\ldots) = \sum F(p_{i_1}^{\alpha_{i_1}}\ldots p_{i_s}^{\alpha_{i_s}}, q_{j_1}^{\beta_{j_1}}\ldots q_{j_t}^{\beta_{j_t}}) x_{i_1}^{\alpha_{i_1}}\ldots x_{i_s}^{\alpha_{i_s}} y_{j_1}^{\beta_{j_1}}\ldots y_{j_t}^{\beta_{j_t}}. \tag{4}$$

Here the summation goes over all $(i_1,\ldots i_s, j_1,\ldots j_t)$ and $(\alpha_{i_1},\ldots,\alpha_{i_s},\beta_{j_1},\ldots,\beta_{j_t})$ in which $\alpha_{i_e} \in \mathbb{Z}^+$ and $\beta_{j_f} \in \mathbb{Z}^+$.

We prove that

$$g(x_1,x_2\ldots,y_1,y_2\ldots) = \frac{1}{\prod_{i=1}^{\infty}(1-x_i) + \prod_{i=1}^{\infty}(1-y_i) - 1}.$$

According to Proposition 3.18,

$$\begin{aligned}
F(p_{i_1}^{\alpha_{i_1}}\ldots p_{i_s}^{\alpha_{i_s}}, q_{j_1}^{\beta_{j_1}}\ldots q_{j_t}^{\beta_{j_t}}) &= F(\frac{m}{p_{i_1}},n) + F(\frac{m}{p_{i_2}},n) + \ldots + F(\frac{m}{p_{i_s}},n) \\
&- F(\frac{m}{p_{i_1}p_{i_2}},n) - F(\frac{m}{p_{i_1}p_{i_3}},n) - \ldots - F(\frac{m}{p_{i_{s-1}}p_{i_s}},n) \\
&+ \ldots \\
&+ F(m,\frac{n}{q_{j_1}}) + F(m,\frac{n}{q_{j_2}}) + \ldots + F(m,\frac{n}{q_{j_t}}) \\
&- F(m,\frac{n}{q_{j_1}q_{j_2}}) - F(m,\frac{n}{q_{j_1}q_{j_3}}) - \ldots - F(m,\frac{n}{q_{j_{t-1}}q_{j_t}}) \\
&+ \ldots
\end{aligned}$$

It is also easy to verify that

$$F(p_{i_1}^{\alpha_{i_1}}\dots p_{i_s}^{\alpha_{i_s}},1) = F(\frac{m}{p_{i_1}},1)+F(\frac{m}{p_{i_2}},1)+\dots+F(\frac{m}{p_{i_s}},1)$$
$$-F(\frac{m}{p_{i_1}p_{i_2}},1)-F(\frac{m}{p_{i_1}p_{i_3}},1)-\dots-F(\frac{m}{p_{i_{s-1}}p_{i_s}},1)+\dots$$

and

$$F(1,q_{j_1}^{\beta_{j_1}}\dots q_{j_t}^{\beta_{j_t}}) = F(1,\frac{n}{q_{j_1}})+F(1,\frac{n}{q_{j_2}})+\dots+F(1,\frac{n}{q_{j_t}})$$
$$-F(1,\frac{n}{q_{j_1}q_{j_2}})-F(1,\frac{n}{q_{j_1}q_{j_3}})-\dots-F(1,\frac{n}{q_{j_{t-1}}q_{j_t}})+\dots$$

Expanding $F(p_{i_1}^{\alpha_{i_1}}\dots p_{i_s}^{\alpha_{i_s}},q_{j_1}^{\beta_{j_1}}\dots q_{j_t}^{\beta_{j_t}})$ on the right hand side of (4), except $F(1,1)$, and then combining the term with the same $F(p_{i_1}^{\alpha_{i_1}}\dots p_{i_s}^{\alpha_{i_s}},q_{j_1}^{\beta_{j_1}}\dots q_{j_t}^{\beta_{j_t}})$, we get

$$\begin{aligned} &g(x_1\dots,y_1\dots) \\ &\quad = 1+g(x_1\dots,y_1\dots)(\sum_i x_i-\sum_{i_1,i_2}x_{i_1}x_{i_2}+\dots+\sum_j y_j-\sum_{j_1,j_2}x_{j_1}x_{j_2}+\dots) \\ &\quad = 1+g(x_1\dots,y_1\dots)[(1-\prod_{i=1}^{\infty}(1-x_i))+(1-\prod_{i=1}^{\infty}(1-y_i))]. \end{aligned}$$

Thus we have

$$g(x_1,x_2\dots,y_1,y_2\dots)=\frac{1}{\prod_{i=1}^{\infty}(1-x_i)+\prod_{i=1}^{\infty}(1-y_i)-1}.$$

□

We can also give a formula for $F(m,n)$ based on $D_k(N)$, which is defined in Definition 3.10, and can be computed according to Proposition 3.12 and Proposition 3.13.

Proposition 3.20.

$$F(m,n)=\sum_{k=0}^{A}[2D_k(m)D_k(n)+D_{k+1}(m)D_k(n)+D_k(m)D_{k+1}(n)].$$

Here, $A=\min(\Omega(m),\Omega(n))$ where $\Omega(N)=\alpha_1+\alpha_2+\dots+\alpha_k$, if $N=p_1^{\alpha_1}\dots p_k^{\alpha_k}$.

Proof. For an arithmetical path, if the number of steps is even, suppose there are $2k$ steps. Then there are k steps in the x-direction and k steps in the y-direction.

Without loss of generosity, we first compute the number of paths starting with a step in the x-direction.

A step in the x-direction is determined by an integer $x_{end}/x_{initial}$, in which x_{end} and $x_{initial}$ are x-coordinates of the endpoint and initial point respectively. Suppose the integer thus defined for the k steps are $d_1,d_2,\dots,d_k$. We have $d_1,d_2,\dots,d_k>1$ and $m=d_1d_2\dots d_k$. Therefore, the number of different $(d_1,d_2,\dots,d_k)$ is $D_{k-1}(m)$.

Similarly, a step in the y-direction is determined by an integer $y_{end}/y_{initial}$, in which y_{end} and $y_{initial}$ are y-coordinates of the endpoint and initial point respectively. Suppose the integer thus defined for the k steps are $d'_1, d'_2, \ldots, d'_k$. Then the number of different $(d'_1, d'_2, \ldots, d'_k)$ is $D_{k-1}(n)$.

Since different paths have different tuples $(d_1, d_2, \ldots, d_k, d'_1, d'_2, \ldots, d'_k)$ and every tuple has a corresponding path, there is bijection between the paths and the tuples. Thus, the number of paths with $2k$ steps, starting with a step in the x-direction is $D_{k-1}(m)D_{k-1}(n)$.

Similarly, the number of paths with $2k$ steps, starting with a step in the y-direction is also $D_{k-1}(m)D_{k-1}(n)$.

With the same spirit, we can prove that the number of paths with $(2k+1)$ steps, starting with a step in the x-direction is $D_k(m)D_{k-1}(n)$ while the number of paths with $(2k+1)$ steps, starting with a step in the y-direction is also $D_{k-1}(m)D_k(n)$.

Therefore, we have

$$F(m,n) = \sum_{k=0}^{A} [2D_k(m)D_k(n) + D_{k+1}(m)D_k(n) + D_k(m)D_{k+1}(n)].$$

□

It is difficult to compute $D_k(N)$ by hand, while computing $d_k(N)$ is an easy task. So we will give a formula for $F(m,n)$ based on $d_k(N)$. First, we give the formula in some special cases.

Case. $m = p^s$, $n = q^t$, p, q primes, $s, t \in \mathbb{N}$.

$$F(m,n) = \binom{s+t}{s}.$$

Case. $m = p^s$, $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, p, p_i primes $s, \alpha_i \in \mathbb{N}$.

$$F(m,n) = d_s(n) = \prod_{i=1}^{k} \binom{s+\alpha_i}{s}.$$

Case. $m = p^s q$, p, q primes, $s, t \in \mathbb{N}$.

$$F(m,n) = (s+1)d_{s+1}(n) - sd_s(n).$$

Case. $m = p^s q^t$, p, q primes, $s, t \in \mathbb{N}$.

$$F(m,n) = \sum_{i=0}^{s+t} (-1)^i \binom{s+t-i}{s-i, t-i, i} d_{s+t-i}(n).$$

Case. $m = p^s q^t r$, p, q, r primes, $s, t \in \mathbb{N}$.

$$F(m,n) = \sum_{i=0}^{s+t+1} (-1)^i \frac{(s+t+1-i)!}{(s+1-i)!(t+1-i)!i!}((s+1)(t+1)-i)d_{s+t+1-i}(n).$$

Case. $m = p^s q^t r^2$, p, q, r primes, $s, t \in \mathbb{N}$.

$$F(m,n) = \sum_{i=0}^{s+t+2} (-1)^i \frac{(s+t+2-i)!}{(s+2-i)!(t+2-i)!i!}$$
$$((s+2)(s+1)(t+2)(t+1) - 4(s+i)(t+i) + 6i(i-1))d_{s+t+2-i}(n).$$

Case. $m = p_1^s p_2^s \dots p_k^s$, p_i primes, $s \in \mathbb{N}$.

$$F(m,n) = \sum_{i=s}^{ks} (-1)^{ks-i} T_k(i,s) d_i(n).$$

Here $T_k(n,m) = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} \binom{j}{m}^k$ or can be given by $\binom{n}{m}^k = \sum_{j=0}^{n} T_k(j,m) \binom{n}{j}$.

On OEIS, $T_3(n,m)$ is A262704; $T_4(n,m)$ is A262705; $T_5(n,m)$ is A262706.

Inspired by the form of the last case, we find the following beautiful formula.

Proposition 3.21. If $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, p_i primes $\alpha_i \in \mathbb{N}$. We define polynomial $f(x)$ to be $\prod_{i=1}^{k} \binom{x+\alpha_i}{\alpha_i}$ and let $A = \alpha_1 + \alpha_2 + \dots + \alpha_k$. Then

$$F(m,n) = \sum_{i=0}^{A} \sum_{j=0}^{i} (-1)^j \binom{i}{j} f(-j-1) d_i(n).$$

Proof. First, by Proposition 3.20, we know that for a fixed m, $F(m,n)$ can be written as the linear combination of $D_k(n)$ in which the coefficients don't depend on n. Together with Proposition 3.13, we know that $F(m,n)$ can be written as the linear combination of $d_k(n)$ in which the coefficients don't depend on n. Suppose that

$$F(m,n) = \sum_{i=0}^{\infty} C_i d_i(n).$$

Taking $n = p^s$, p prime, $s \in \mathbb{N}$, we have

$$F(m,n) = \sum_{i=0}^{\infty} C_i \binom{s+i}{i}.$$

On the other hand,

$$F(m,n) = \prod_{i=1}^{k} \binom{s+\alpha_i}{\alpha_i}$$

So for all $s \in \mathbb{N}$, we have

$$\prod_{i=1}^{k} \binom{s+\alpha_i}{\alpha_i} = \sum_{i=0}^{\infty} C_i \binom{s+i}{i}.$$

Dividing both side by s^A and let s tend to infinity, we have a positive constant on the left hand side, thus we should also have the same constant on the right hand side. Notice that for every $i < A$, $\lim_{s\to+\infty} s^{-A} \binom{s+i}{i} = 0$, while for every $i > A$, $\lim_{s\to+\infty} s^{-A} \binom{s+i}{i} = +\infty$, we have $C_A > 0$ and $C_i = 0$ for $i > A$.

Let $g(x) = \sum_{i=0}^{A} C_i \binom{x+i}{i}$, we have $f(x) = g(x)$ for all $x \in \mathbb{N}$. By the Lagrange Theorem, we conclude that $f(x) \equiv g(x)$.

In particular, $f(-t-1) = g(-t-1)$, in which $t \in \mathbb{N}$. Notice that

$$\binom{-t-1+i}{i} = \begin{cases} 0 & i > t \\ (-1)^i \binom{t}{i} & 0 \le i \le t \end{cases}$$

Therefore we have

$$f(-t-1) = \sum_{i=0}^{t} (-1)^i \binom{t}{i} C_i. \tag{5}$$

We use induction to prove that for every $l \in \mathbb{N}$,

$$C_l = \sum_{i=0}^{l} (-1)^i \binom{l}{i} f(-i-1).$$

When $l = 0$, taking $t = 0$ in (5) gives $f(-1) = C_0$ which is the desired result. If the equality holds for all $l' < l$, $l \ge 1$, then taking $t = l$ in (5) gives

$$\begin{aligned} C_l &= (-1)^l f(-l-1) + \sum_{i=0}^{l-1} (-1)^{l-i} \binom{l}{i} C_i \\ &= (-1)^l f(-l-1) + \sum_{i=0}^{l-1} (-1)^{l-i} \binom{l}{i} \sum_{j=0}^{i} (-1)^j \binom{i}{j} f(-j-1) \\ &= (-1)^l f(-l-1) + \sum_{j=0}^{l-1} (-1)^j f(-j-1) \sum_{i=j}^{l-1} (-1)^{l-i} \binom{l}{i} \binom{i}{j}. \end{aligned}$$

Since

$$\binom{l}{i}\binom{i}{j} = \binom{l}{l-i, i-j, j} = \binom{l}{j}\binom{l-j}{l-i},$$

we have

$$\begin{aligned} \sum_{i=j}^{l} (-1)^{l-i} \binom{l}{i}\binom{i}{j} &= \sum_{i=j}^{l} (-1)^{l-i} \binom{l}{j}\binom{l-j}{l-i} \\ &= \binom{l}{j} \sum_{i=j}^{l} (-1)^{l-i} \binom{l-j}{l-i} \\ &= 0. \end{aligned}$$

Therefore

$$\begin{aligned} C_l &= (-1)^l f(-l-1) + \sum_{j=0}^{l-1} (-1)^j f(-j-1) \sum_{i=j}^{l-1} (-1)^{l-i} \binom{l}{i}\binom{i}{j} \\ &= (-1)^l f(-l-1) + \sum_{j=0}^{l-1} (-1)^j f(-j-1) \binom{l}{j} \\ &= \sum_{j=0}^{l} (-1)^j \binom{l}{j} f(-j-1). \end{aligned}$$

thus we have completed our induction.

Finally we obtain our beautiful formula

$$
\begin{aligned}
F(m,n) &= \sum_{i=0}^{A} C_i d_i(n) \\
&= \sum_{i=0}^{A} \sum_{j=0}^{i} (-1)^j \binom{i}{j} f(-j-1) d_i(n).
\end{aligned}
$$

$\square$

Remark. In this study, we classify all the decomposition of sets of consecutive integers, find a method to construct them and derive formulas for the number of such decompositions. Furthermore, we find that the subject is closely related to cyclotomic polynomials and the study actually inspires us to classify cyclotomic polynomials with {0,1} coefficients, which is a future research project the author will be working on.

4 Computational Complexity

In this section, we will give an efficient algorithm to calculate $F(m,n)$ relying on the results in this paper and analyze its computational complexity.

Algorithm. Without loss of generosity, we may assume that $m < n$ and let $A = \Omega(m)$, then $A \leq \log_2 m$.

Step 1: Use Pollard Rho algorithm to obtain the prime factorization of m and n. The computational complexity is $O(max\{m,n\}^{\frac{1}{4}})$. Assume that $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ and $n = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$.

Step 2: For each $0 \leq i \leq s$, calculate $\binom{\alpha_i}{0}$, $\binom{\alpha_i+1}{1}$, $\binom{\alpha_i+2}{2}, \dots, \binom{\alpha_i+A}{A}$, using $\binom{\alpha_i+k}{k} = \frac{\alpha_i+k}{k}\binom{\alpha_i+k-1}{k-1}$. Then do the same thing for $\binom{\beta_j+l}{l}$, $0 \leq j \leq t$, $0 \leq l \leq A$. The computational complexity is $O(\log m \log n)$.

Step 3: Calculate $d_k(m)$ and $d_k(n)$ for all $0 \leq k \leq A$ using Proposition 3.12. The computational complexity is $O(\log m \log n)$.

Step 4: Calculate $\binom{k+1}{i}$ for all $0 \leq i \leq k \leq A$, using $\binom{k+1}{i} = \binom{k}{i-1} + \binom{k}{i}$. The computational complexity is $O(\log^2 m)$.

Step 5: Calculate $D_k(m)$ and $D_k(n)$ for all $0 \leq k \leq A$ using Proposition 3.13. The computational complexity is $O(\log^2 m)$.

Step 6: Calculate $F(m,n)$ using Proposition 3.20. The computational complexity is $O(\log m)$.

Thus we have an algorithm to calculate $F(m,n)$ with its computational complexity being $O(max\{\log m \log n, m^{\frac{1}{4}}, n^{\frac{1}{4}}\})$.

5 Acknowledgement

The author would like to thank Prof. Zhenhua Qu from East China Normal University for his support on this project. He would also like to acknowledge his friend Yifan Zhu from Shanghai Foreign Language School for suggesting Proposition 3.18 and 3.19 and Weihao Zhu from Shanghai High School for his generous help in Section 4.

References

[1] Brett Porter. *Cyclotomic Polynomials*. https://www.whitman.edu/Documents/Academics/Mathematics/2015/Final%20Project%20-%20Porter,%20Brett.pdf

[2] Ira M. Gessel, P. Stanley. *Algebraic Enumeration*. http://www-math.mit.edu/~rstan/pubs/pubfiles/79.pdf

[3] Ronald L. Graham, Donald E. Knuth, Oren Patashnik. *Concrete Mathematics*. Addison-Wesley, 1990. Print.

[4] Peter Borwein, Kwok-Kwong Stephen Choi. *On cyclotomic polynomials with* ± 1 *coefficients*.

[5] Coaches of Chinese Team Selection Test for IMO 2012. *Collection of Problems in Math Olympiads 2012*. ECNU Press, 2012. Print.

J. Fan, Class of 2017, Shanghai High School, Shanghai 200231, China
E-mail address, J. Fan: junhaofan@126.com