Math 4990 Fall 2017 (Darij Grinberg): homework set 8 with hints to solutions

Contents

I am giving just hints or brief outlines of the solutions below; unfortunately, this is all I have the time for. I hope they are reasonably clear. Please let me know (`mailto:dgrinber@umn.edu`) if you are stuck in some of the details.

0.1. Strange integers

Exercise 1. For any $m \in \mathbb{N}$ and $n \in \mathbb{N}$, define a rational number $T(m,n)$ by

$$T(m,n) = \frac{(2m)!\,(2n)!}{m!n!\,(m+n)!}.$$

(a) Prove that $4T(m,n) = T(m+1,n) + T(m,n+1)$ for every $m \in \mathbb{N}$ and $n \in \mathbb{N}$.

(b) Prove that $T(m,n) \in \mathbb{N}$ for every $m \in \mathbb{N}$ and $n \in \mathbb{N}$.

(c) Prove that $T(m,n)$ is an **even** integer for every $m \in \mathbb{N}$ and $n \in \mathbb{N}$ unless $(m,n) = (0,0)$.

(d) If $m \in \mathbb{N}$ and $n \in \mathbb{N}$ are such that $m+n$ is odd and $m+n > 1$, then prove that $4 \mid T(m,n)$.

The numbers $T(m,n)$ introduced in Exercise 1 are the so-called *super-Catalan numbers*; they are a subject of active research (see, e.g., [Gessel92] and [AleGhe14]). Exercise 1 **(b)** suggests that these numbers count something, but no one has so far discovered what; combinatorial proofs aren't always the easiest to find. The thread `https://artofproblemsolving.com/community/c6h1553916s1_supercatalan_numbers` on Art of Problem Solving also discusses the super-Catalan numbers and Exercise 1.

A detailed solution of Exercise 1 can be found in [Grinbe16, solution to Exercise 3.25]. We will be rather brief here.

To solve Exercise 1, we need the following lemma (which is [Grinbe16, Exercise 3.24]):

Lemma 0.1. Let m be a positive integer.

(a) The binomial coefficient $\dbinom{2m}{m}$ is even.

(b) Assume that m is odd and satisfies $m > 1$. Then, the binomial coefficient $\dbinom{2m-1}{m-1}$ is even.

(c) Assume that m is odd and satisfies $m > 1$. Then, $\dbinom{2m}{m} \equiv 0 \mod 4$.

Proof of Lemma 0.1 (sketched). **(a)** This follows from $\dbinom{2m}{m} = 2\dbinom{2m-1}{m-1}$.

(b) Lemma 0.1 **(a)** (applied to $m-1$ instead of m) shows that $\dbinom{2(m-1)}{m-1}$ is even. In other words, $\dbinom{2(m-1)}{m-1} \equiv 0 \bmod 2$. But m is odd; thus, $m \equiv 1 \bmod 2$. Now,

$$m\binom{2m-1}{m-1} = (2m-1)\underbrace{\binom{2(m-1)}{m-1}}_{\equiv 0 \bmod 2} \equiv 0 \bmod 2,$$

so that $0 \equiv \underbrace{m}_{\equiv 1 \bmod 2}\dbinom{2m-1}{m-1} \equiv \dbinom{2m-1}{m-1} \bmod 2$. In other words, $\dbinom{2m-1}{m-1}$ is even. This proves Lemma 0.1 **(b)**.

(c) We have $\dbinom{2m}{m} = 2\dbinom{2m-1}{m-1} \equiv 0 \bmod 4$ (since Lemma 0.1 **(b)** shows that $\dbinom{2m-1}{m-1}$ is even). This proves Lemma 0.1 **(c)**. □

Solution to Exercise 1 (sketched). **(a)** This is a straightforward computation: For $m \in \mathbb{N}$ and $n \in \mathbb{N}$, we have

$$\begin{aligned}
T(m+1,n) &= \frac{(2(m+1))!\,(2n)!}{(m+1)!n!\,(m+1+n)!} = \frac{(2m+2)(2m+1)\cdot(2m)!\,(2n)!}{(m+1)\cdot m!n!\cdot(m+1+n)\cdot(m+n)!} \\
&\qquad \left(\begin{array}{c}\text{since } (2(m+1))! = (2m+2)(2m+1)\cdot(2m)! \text{ and} \\ (m+1)! = (m+1)\cdot m! \text{ and } (m+1+n)! = (m+1+n)\cdot(m+n)!\end{array}\right) \\
&= \underbrace{\frac{(2m+2)(2m+1)}{(m+1)(m+1+n)}}_{=\frac{4m+2}{m+1+n}} \cdot \underbrace{\frac{(2m)!\,(2n)!}{m!n!\,(m+n)!}}_{=T(m,n)} = \frac{4m+2}{m+1+n}\cdot T(m,n)
\end{aligned}$$

and similarly

$$T(m,n+1) = \frac{4n+2}{m+1+n}\cdot T(m,n).$$

Add these two equalities and simplify.

(b) Apply induction on n:

Induction base: For each $m \in \mathbb{N}$, we have

$$T(m,0) = \frac{(2m)!\,(2\cdot 0)!}{m!0!\,(m+0)!} = \frac{(2m)!}{m!m!} = \binom{2m}{m} \in \mathbb{N}.$$

In other words, Exercise 1 **(b)** holds for $n = 0$.

Induction step: Let $N \in \mathbb{N}$. Assume (as the induction hypothesis) that Exercise 1 **(b)** holds for $n = N$. We must prove that Exercise 1 **(b)** holds for $n = N+1$.

For each $m \in \mathbb{N}$, we have

$$T(m,N+1) = 4 \underbrace{T(m,N)}_{\substack{\in\mathbb{N} \\ \text{(by the induction} \\ \text{hypothesis)}}} - \underbrace{T(m+1,N)}_{\substack{\in\mathbb{N} \\ \text{(by the induction} \\ \text{hypothesis)}}}$$
$$\left(\text{since Exercise 1 **(a)** yields } 4T(m,N) = T(m+1,N) + T(m,N+1)\right)$$
$$\in \mathbb{Z}$$

and therefore $T(m,N+1) \in \mathbb{N}$ (since the definition of $T(m,N+1)$ shows that $T(m,N+1)$ is positive). In other words, Exercise 1 **(b)** holds for $n = N+1$. This completes the induction step. Hence, Exercise 1 **(b)** is proven.

(c) Apply induction on n:

Induction base: For each positive integer m, we have

$$T(m,0) = \frac{(2m)!\,(2\cdot 0)!}{m!0!\,(m+0)!} = \frac{(2m)!}{m!m!} = \binom{2m}{m},$$

and this is even (by Lemma 0.1 **(a)**). In other words, for each positive integer m, the number $T(m,0)$ is an even integer. In other words, Exercise 1 **(c)** holds for $n = 0$ (because if $m \in \mathbb{N}$ and $n \in \mathbb{N}$ satisfy $(m,n) \neq (0,0)$ but $n = 0$, then m must be a positive integer).

Induction step: Let $N \in \mathbb{N}$. Assume (as the induction hypothesis) that Exercise 1 **(c)** holds for $n = N$. We must prove that Exercise 1 **(c)** holds for $n = N+1$.

Let $m \in \mathbb{N}$. Exercise 1 **(b)** shows that $T(m,N)$ is an integer. Thus, $4T(m,N) \equiv 0 \bmod 2$. Also, $(m+1,N) \neq (0,0)$ (since $m+1$ is positive). Thus, the induction hypothesis yields that $T(m+1,N)$ is an even integer. Hence, $T(m+1,N) \equiv 0 \bmod 2$.

Now, Exercise 1 **(a)** yields $4T(m,N) = T(m+1,N) + T(m,N+1)$. Thus,

$$T(m,N+1) = \underbrace{4T(m,N)}_{\equiv 0 \bmod 2} - \underbrace{T(m+1,N)}_{\equiv 0 \bmod 2} \equiv 0 \bmod 2.$$

In other words, $T(m,N+1)$ is even. In other words, Exercise 1 **(c)** holds for $n = N+1$. This completes the induction step. Hence, Exercise 1 **(c)** is proven.

(d) Apply induction on n:

Induction base: We must prove Exercise 1 **(d)** for $n = 0$. In other words, we must show that if $m \in \mathbb{N}$ is such that $m+0$ is odd and $m+0 > 1$, then $4 \mid T(m,0)$.

Let $m \in \mathbb{N}$ be such that $m+0$ is odd and $m+0>1$. From $m=m+0>1$, we conclude that m is a positive integer. Also, $m=m+0$ is odd. Now,

$$T(m,0) = \frac{(2m)!\,(2\cdot 0)!}{m!0!\,(m+0)!} = \frac{(2m)!}{m!m!} = \binom{2m}{m} \equiv 0 \bmod 4$$

(by Lemma 0.1 **(b)**). In other words, $4 \mid T(m,0)$. This completes our proof that Exercise 1 **(d)** holds for $n=0$.

Induction step: Let $N \in \mathbb{N}$. Assume (as the induction hypothesis) that Exercise 1 **(d)** holds for $n=N$. We must prove that Exercise 1 **(d)** holds for $n=N+1$.

Let $m \in \mathbb{N}$ be such that $m+(N+1)$ is odd and $m+(N+1)>1$. Then, $(m+1)+N = m+(N+1)$ is odd and $(m+1)+N = m+(N+1) > 1$. Thus, the induction hypothesis yields that $4 \mid T(m+1,N)$. Hence, $T(m+1,N) \equiv 0 \bmod 4$. Also, Exercise 1 **(b)** shows that $T(m,N)$ is an integer. Thus, $4T(m,N) \equiv 0 \bmod 4$.

Now, Exercise 1 **(a)** yields $4T(m,N) = T(m+1,N) + T(m,N+1)$. Thus,

$$T(m,N+1) = \underbrace{4T(m,N)}_{\equiv 0 \bmod 4} - \underbrace{T(m+1,N)}_{\equiv 0 \bmod 4} \equiv 0 \bmod 4.$$

In other words, $4 \mid T(m,N+1)$. In other words, Exercise 1 **(d)** holds for $n=N+1$. This completes the induction step. Hence, Exercise 1 **(d)** is proven. □

Exercise 2. Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$. Let $p = \min\{m,n\}$.

(a) Prove that

$$\sum_{k=-p}^{p} (-1)^k \binom{m+n}{m+k}\binom{m+n}{n+k} = \binom{m+n}{m}.$$

(b) Prove that

$$T(m,n) = \sum_{k=-p}^{p} (-1)^k \binom{2m}{m+k}\binom{2n}{n-k},$$

where $T(m,n)$ is defined as in Exercise 1.

[**Hint:** Part **(a)** should follow from something done in class. Then, compare part **(b)** with part **(a)**.]

Exercise 2 **(b)** is a result of von Szily (1894); see [Gessel92, (29)]. Needless to say, Exercise 2 **(b)** provides an alternative solution to Exercise 1 **(b)**.

A full solution of Exercise 2 can be found in Angela Chen's homework and in [Grinbe16, solution to Exercise 3.25] (this is one and the same solution, written up in slightly different ways).

0.2. The length of a permutation

Definition 0.2. Let $n \in \mathbb{N}$.

(a) We let S_n denote the set of all permutations of $[n]$.

Let $\sigma \in S_n$ be a permutation of $[n]$.

(b) An *inversion* of σ means a pair (i, j) of elements of $[n]$ satisfying $i < j$ and $\sigma(i) > \sigma(j)$.

(c) The *length* of σ is defined to be the number of inversions of σ. This length is denoted by $\ell(\sigma)$.

(d) The *sign* of σ is defined to be the integer $(-1)^{\ell(\sigma)}$. It is denoted by $(-1)^{\sigma}$.

Exercise 3. Let $p \in \mathbb{N}$ and $q \in \mathbb{N}$. Let $n = pq$. Consider the permutation $\sigma \in S_n$ that maps $(i-1)q + j$ to $(j-1)p + i$ for every $i \in [p]$ and $j \in [q]$.

(This permutation σ can be visualized as follows: Fill in a $p \times q$-matrix A with the entries $1, 2, \ldots, n$ by going row by row from top to bottom:

$$A = \begin{pmatrix} 1 & 2 & 3 & \cdots & q \\ q+1 & q+2 & q+3 & \cdots & 2q \\ 2q+1 & 2q+2 & 2q+3 & \cdots & 3q \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (p-1)q+1 & (p-1)q+2 & (p-1)q+3 & \cdots & pq \end{pmatrix}.$$

Fill in a $p \times q$-matrix B with the entries $1, 2, \ldots, n$ by going column by column from left to right:

$$B = \begin{pmatrix} 1 & p+1 & 2p+1 & \cdots & (q-1)p+1 \\ 2 & p+2 & 2p+2 & \cdots & (q-1)p+2 \\ 3 & p+3 & 2p+3 & \cdots & (q-1)p+3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p & 2p & 3p & \cdots & qp \end{pmatrix}.$$

The permutation σ then sends each entry of A to the corresponding entry of B.)

Find the length $\ell(\sigma)$ of the permutation σ.

A full solution of Exercise 3 can be found in Angela Chen's homework. (This is also the solution I had in mind.) We shall later sketch the solution after Definition 0.4 (which somewhat simplifies it).

0.3. Two equal counts

Exercise 4. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Prove that

$$\begin{aligned} &(\text{the number of all } (i, j) \in [n] \times [n] \text{ such that } i \geq j > \sigma(i)) \\ &= (\text{the number of all } (i, j) \in [n] \times [n] \text{ such that } \sigma(i) \geq j > i). \end{aligned}$$

Exercise 4 is a consequence of the following fact:

Lemma 0.3. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$ and $j \in [n]$. Then,

$$\begin{aligned} & (\text{the number of all } i \in [n] \text{ such that } i \geq j > \sigma(i)) \\ & = (\text{the number of all } i \in [n] \text{ such that } \sigma(i) \geq j > i). \end{aligned} \tag{1}$$

Indeed, if we sum up the equality (1) over all $j \in [n]$, then we obtain precisely the claim of Exercise 4.

Lemma 0.3 is [Han92, Lemme 2.1]. Anyway, it is also easy to prove:

First proof of Lemma 0.3 (sketched). The map σ is a permutation of $[n]$ (since $\sigma \in S_n$), thus a bijection $[n] \to [n]$.

Use the Iverson bracket notation. Then, any three integers p, q and r satisfy

$$\begin{aligned} [p \geq q > r] &= [p \geq q \text{ and } q > r] = [p \geq q] \underbrace{[q > r]}_{\substack{=[\text{not } r \geq q] \\ =1-[r \geq q]}} = [p \geq q](1 - [r \geq q]) \\ &= [p \geq q] - [p \geq q][r \geq q]. \end{aligned} \tag{2}$$

But

$$\begin{aligned} & (\text{the number of all } i \in [n] \text{ such that } i \geq j > \sigma(i)) \\ & = \sum_{i \in [n]} \underbrace{[i \geq j > \sigma(i)]}_{\substack{=[i \geq j]-[i \geq j][\sigma(i) \geq j] \\ (\text{by } (2))}} = \sum_{i \in [n]} ([i \geq j] - [i \geq j][\sigma(i) \geq j]) \\ & = \sum_{i \in [n]} [i \geq j] - \sum_{i \in [n]} [i \geq j][\sigma(i) \geq j] \end{aligned} \tag{3}$$

and similarly

$$\begin{aligned} & (\text{the number of all } i \in [n] \text{ such that } \sigma(i) \geq j > i) \\ & = \sum_{i \in [n]} [\sigma(i) \geq j] - \sum_{i \in [n]} [\sigma(i) \geq j][i \geq j]. \end{aligned}$$

Hence,

$$\begin{aligned} & (\text{the number of all } i \in [n] \text{ such that } \sigma(i) \geq j > i) \\ & = \underbrace{\sum_{i \in [n]} [\sigma(i) \geq j]}_{\substack{= \sum_{i \in [n]} [i \geq j] \\ (\text{here, we have substituted } i \\ \text{for } \sigma(i) \text{ in the sum, since} \\ \text{the map } \sigma \text{ is a bijection } [n] \to [n])}} - \sum_{i \in [n]} \underbrace{[\sigma(i) \geq j][i \geq j]}_{=[i \geq j][\sigma(i) \geq j]} \\ & = \sum_{i \in [n]} [i \geq j] - \sum_{i \in [n]} [i \geq j][\sigma(i) \geq j] \\ & = (\text{the number of all } i \in [n] \text{ such that } i \geq j > \sigma(i)) \end{aligned}$$

(by (3)). This proves Lemma 0.3. □

Second proof of Lemma 0.3 (sketched). The map σ is a permutation of $[n]$ (since $\sigma \in S_n$), thus a bijection $[n] \to [n]$.

We have

$$\begin{aligned}
&\left(\text{the number of all } i \in [n] \text{ such that } \underbrace{i \geq j > \sigma(i)}_{\iff (i \geq j \text{ but } \textbf{not } \sigma(i) \geq j)}\right) \\
&= (\text{the number of all } i \in [n] \text{ such that } i \geq j \text{ but } \textbf{not } \sigma(i) \geq j) \\
&= (\text{the number of all } i \in [n] \text{ such that } i \geq j) \\
&\qquad - (\text{the number of all } i \in [n] \text{ such that } i \geq j \text{ and } \sigma(i) \geq j)
\end{aligned}$$

and

$$\begin{aligned}
&\left(\text{the number of all } i \in [n] \text{ such that } \underbrace{\sigma(i) \geq j > i}_{\iff (\sigma(i) \geq j \text{ but } \textbf{not } i \geq j)}\right) \\
&= (\text{the number of all } i \in [n] \text{ such that } \sigma(i) \geq j \text{ but } \textbf{not } i \geq j) \\
&= \underbrace{(\text{the number of all } i \in [n] \text{ such that } \sigma(i) \geq j)}_{\substack{=(\text{the number of all } i \in [n] \text{ such that } i \geq j) \\ (\text{here, we have substituted } i \text{ for } \sigma(i), \text{ since the map } \sigma \text{ is a bijection } [n] \to [n])}} \\
&\qquad - \left(\text{the number of all } i \in [n] \text{ such that } \underbrace{\sigma(i) \geq j \text{ and } i \geq j}_{\iff (i \geq j \text{ and } \sigma(i) \geq j)}\right) \\
&= (\text{the number of all } i \in [n] \text{ such that } i \geq j) \\
&\qquad - (\text{the number of all } i \in [n] \text{ such that } i \geq j \text{ and } \sigma(i) \geq j) .
\end{aligned}$$

Comparing these two equalities, we obtain

$$\begin{aligned}
&(\text{the number of all } i \in [n] \text{ such that } i \geq j > \sigma(i)) \\
&= (\text{the number of all } i \in [n] \text{ such that } \sigma(i) \geq j > i) .
\end{aligned}$$

This proves Lemma 0.3 again. □

Note that none of the above proofs of Lemma 0.3 is bijective. Maja Schryer found a bijective proof:

Third proof of Lemma 0.3 (sketched). The map

$$\begin{aligned}
&\{i \in [n] \mid i \geq j > \sigma(i)\} \to \{i \in [n] \mid \sigma(i) \geq j > i\} , \\
&\qquad i \mapsto \left(\sigma^{k-1}(i) , \text{ where } k \text{ is the smallest positive integer satisfying } \sigma^k(i) \geq j\right)
\end{aligned}$$

is well-defined (indeed, it is easy to see that a positive integer k satisfying $\sigma^k(i) \geq j$ exists for every $i \in [n]$ satisfying $i \geq j$). Similarly, the map

$$\{i \in [n] \mid \sigma(i) \geq j > i\} \to \{i \in [n] \mid i \geq j > \sigma(i)\},$$
$$i \mapsto \left(\left(\sigma^{-1}\right)^k(i), \text{ where } k \text{ is the smallest nonnegative integer satisfying } \left(\sigma^{-1}\right)^k(i) \geq j\right)$$

is well-defined (notice that we are using $\left(\sigma^{-1}\right)^k$ here, not $\left(\sigma^{-1}\right)^{k-1}$). It is easy to check that these two maps are mutually inverse, and thus bijective. This bijection yields Lemma 0.3. □

0.4. Lehmer codes

Recall the following definition from the preceding homework set:

Definition 0.4. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$ be a permutation. For any $i \in [n]$, we let $\ell_i(\sigma)$ denote the number of $j \in \{i+1, i+2, \ldots, n\}$ such that $\sigma(i) > \sigma(j)$.

Exercise 5. Let $n \in \mathbb{N}$. Let G be the set of all n-tuples $(j_1, j_2, \ldots, j_n)$ of integers satisfying $0 \leq j_k \leq n-k$ for each $k \in [n]$. (In other words, $G = \{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n-2\} \times \cdots \times \{0, 1, \ldots, n-n\}$.)

(a) For any $\sigma \in S_n$ and $i \in [n]$, prove that $\sigma(i)$ is the $(\ell_i(\sigma)+1)$-th smallest element of the set $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$.

(b) For any $\sigma \in S_n$, prove that

$$(\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma)) \in G.$$

(c) Prove that the map

$$S_n \to G,$$
$$\sigma \mapsto (\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma))$$

is bijective.

(d) Show that $\ell(\sigma) = \ell_1(\sigma) + \ell_2(\sigma) + \cdots + \ell_n(\sigma)$ for each $\sigma \in S_n$.

(e) Show that

$$\sum_{\sigma \in S_n} x^{\ell(\sigma)} = (1+x)\left(1+x+x^2\right)\cdots\left(1+x+x^2+\cdots+x^{n-1}\right)$$

(an equality between polynomials in x). (If $n \leq 1$, then the right hand side of this equality is an empty product, and thus equals 1.)

Note that the n-tuple $(\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma))$ is known as the *Lehmer code* of the permutation σ.

Parts **(b)**, **(c)**, **(d)** and **(e)** of Exercise 5 are proven in [Grinbe16, §5.8 and the solution to Exercise 5.18]. (Specifically, Exercise 5 **(b)** is [Grinbe16, Proposition 5.47]; Exercise 5 **(c)** is [Grinbe16, Theorem 5.52]; Exercise 5 **(d)** is [Grinbe16, Proposition 5.46]; Exercise 5 **(e)** is [Grinbe16, Corollary 5.53]). But let us sketch the simple proofs here as well (they are simple because we have laid all the groundwork on the previous homework set):

Solution to Exercise 5 (sketched). **(a)** Let $\sigma \in S_n$ and $i \in [n]$. Then, σ is a permutation. Thus, the numbers $\sigma(1), \sigma(2), \ldots, \sigma(n)$ are distinct. Now,

$$\underbrace{[n]}_{\substack{=\{1,2,\ldots,n\} \\ =\{\sigma(1),\sigma(2),\ldots,\sigma(n)\} \\ \text{(since } \sigma \text{ is a permutation)}}} \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$$
$$= \{\sigma(1), \sigma(2), \ldots, \sigma(n)\} \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$$
$$= \{\sigma(i), \sigma(i+1), \ldots, \sigma(n)\} \qquad (4)$$

(since $\sigma(1), \sigma(2), \ldots, \sigma(n)$ are distinct).

Recall that $\ell_i(\sigma)$ denotes the number of $j \in \{i+1, i+2, \ldots, n\}$ such that $\sigma(i) > \sigma(j)$. In other words, $\ell_i(\sigma)$ is the number of $j \in \{i+1, i+2, \ldots, n\}$ such that $\sigma(j) < \sigma(i)$. In other words, $\ell_i(\sigma)$ is the number of entries of the sequence $(\sigma(i+1), \sigma(i+2), \ldots, \sigma(n))$ that are smaller than $\sigma(i)$. Thus, there are precisely $\ell_i(\sigma)$ entries in the sequence $(\sigma(i+1), \sigma(i+2), \ldots, \sigma(n))$ that are smaller than $\sigma(i)$. If we add an entry $\sigma(i)$ to this sequence, then this fact does not change (because this new entry $\sigma(i)$ is not smaller than $\sigma(i)$). Thus, there are precisely $\ell_i(\sigma)$ entries in the sequence $(\sigma(i), \sigma(i+1), \ldots, \sigma(n))$ that are smaller than $\sigma(i)$. Since the entries of this sequence are distinct (because $\sigma(1), \sigma(2), \ldots, \sigma(n)$ are distinct), we can rewrite this as follows: There are precisely $\ell_i(\sigma)$ elements of the set $\{\sigma(i), \sigma(i+1), \ldots, \sigma(n)\}$ that are smaller than $\sigma(i)$. In other words, $\sigma(i)$ is the $(\ell_i(\sigma)+1)$-th smallest element of the set $\{\sigma(i), \sigma(i+1), \ldots, \sigma(n)\}$. In view of (4), this rewrites as follows: $\sigma(i)$ is the $(\ell_i(\sigma)+1)$-th smallest element of the set $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$. This solves Exercise 5 **(a)**.

(b) Let $\sigma \in S_n$. For each $i \in \{1, 2, \ldots, n\}$, we have $\ell_i(\sigma) \leq n-i$ (since $\ell_i(\sigma)$ is the number of $j \in \{i+1, i+2, \ldots, n\}$ such that $\sigma(i) > \sigma(j)$, and clearly this number cannot be larger than $|\{i+1, i+2, \ldots, n\}| = n-i$) and thus $\ell_i(\sigma) \in \{0, 1, \ldots, n-i\}$. Hence,

$$(\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma)) \in \{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n-2\} \times \cdots \times \{0, 1, \ldots, n-n\}$$
$$= G.$$

This solves Exercise 5 **(b)**.

(c) The sets S_n and G are finite and have the same size (namely, $n!$). But the map

$$S_n \to G,$$
$$\sigma \mapsto (\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma))$$

is injective (by Exercise 5 **(b)** on homework set #7), and therefore bijective (because any injective map between two finite sets having the same size must be bijective). This solves Exercise 5 **(c)**.

(d) Let $\sigma \in S_n$. The definition of $\ell(\sigma)$ yields that

$$\begin{aligned}
\ell(\sigma) &= (\text{the number of inversions of } \sigma) \\
&= (\text{the number of pairs } (i,j) \text{ of elements of } [n] \text{ satisfying } i < j \text{ and } \sigma(i) > \sigma(j)) \\
&\qquad (\text{by the definition of an inversion}) \\
&= \sum_{i \in [n]} \underbrace{(\text{the number of } j \in [n] \text{ satisfying } i < j \text{ and } \sigma(i) > \sigma(j))}_{\substack{=(\text{the number of } j \in \{i+1, i+2, \ldots, n\} \text{ such that } \sigma(i) > \sigma(j)) \\ (\text{since the } j \in [n] \text{ satisfying } i<j \text{ are precisely the } j \in \{i+1,i+2,\ldots,n\})}} \\
&= \sum_{i \in [n]} \underbrace{(\text{the number of } j \in \{i+1, i+2, \ldots, n\} \text{ such that } \sigma(i) > \sigma(j))}_{\substack{=\ell_i(\sigma) \\ (\text{by the definition of } \ell_i(\sigma))}} \\
&= \sum_{i \in [n]} \ell_i(\sigma) = \ell_1(\sigma) + \ell_2(\sigma) + \cdots + \ell_n(\sigma).
\end{aligned}$$

This solves Exercise 5 **(d)**.

(e) We have

$$\begin{aligned}
&\sum_{\sigma\in S_n} \underbrace{x^{\ell(\sigma)}}_{\substack{=\ell_1(\sigma)+\ell_2(\sigma)+\cdots+\ell_n(\sigma)\\ \text{(by Exercise 5 (d))}}} \\
&= \sum_{\sigma\in S_n} x^{\ell_1(\sigma)+\ell_2(\sigma)+\cdots+\ell_n(\sigma)} = \underbrace{\sum_{(i_1,i_2,\ldots,i_n)\in G}}_{\substack{=\sum_{(i_1,i_2,\ldots,i_n)\in\{0,1,\ldots,n-1\}\times\{0,1,\ldots,n-2\}\times\cdots\times\{0,1,\ldots,n-n\}} \\ \text{(since } G=\{0,1,\ldots,n-1\}\times\{0,1,\ldots,n-2\}\times\cdots\times\{0,1,\ldots,n-n\})}} \underbrace{x^{i_1+i_2+\cdots+i_n}}_{=x^{i_1}x^{i_2}\cdots x^{i_n}} \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } (i_1,i_2,\ldots,i_n) \text{ for } (\ell_1(\sigma),\ell_2(\sigma),\ldots,\ell_n(\sigma)) \\ \text{in the sum, since the map } S_n\to G,\ \sigma\mapsto(\ell_1(\sigma),\ell_2(\sigma),\ldots,\ell_n(\sigma)) \\ \text{is a bijection (by Exercise 5 (c))}\end{array}\right) \\
&= \underbrace{\sum_{(i_1,i_2,\ldots,i_n)\in\{0,1,\ldots,n-1\}\times\{0,1,\ldots,n-2\}\times\cdots\times\{0,1,\ldots,n-n\}}}_{=\sum_{i_1\in\{0,1,\ldots,n-1\}}\sum_{i_2\in\{0,1,\ldots,n-2\}}\cdots\sum_{i_n\in\{0,1,\ldots,n-n\}}} x^{i_1}x^{i_2}\cdots x^{i_n} \\
&= \sum_{i_1\in\{0,1,\ldots,n-1\}}\sum_{i_2\in\{0,1,\ldots,n-2\}}\cdots\sum_{i_n\in\{0,1,\ldots,n-n\}} x^{i_1}x^{i_2}\cdots x^{i_n} \\
&= \underbrace{\left(\sum_{i_1\in\{0,1,\ldots,n-1\}} x^{i_1}\right)}_{=1+x+x^2+\cdots+x^{n-1}} \underbrace{\left(\sum_{i_2\in\{0,1,\ldots,n-2\}} x^{i_2}\right)}_{=1+x+x^2+\cdots+x^{n-2}} \cdots \underbrace{\left(\sum_{i_n\in\{0,1,\ldots,n-n\}} x^{i_n}\right)}_{=1+x+x^2+\cdots+x^{n-n}} \\
&= \left(1+x+x^2+\cdots+x^{n-1}\right)\left(1+x+x^2+\cdots+x^{n-2}\right)\cdots\left(1+x+x^2+\cdots+x^{n-n}\right) \\
&= \left(1+x+x^2+\cdots+x^{n-1}\right)\left(1+x+x^2+\cdots+x^{n-2}\right)\cdots(1+x)\,1 \\
&= \left(1+x+x^2+\cdots+x^{n-1}\right)\left(1+x+x^2+\cdots+x^{n-2}\right)\cdots(1+x) \\
&= (1+x)\left(1+x+x^2\right)\cdots\left(1+x+x^2+\cdots+x^{n-1}\right).
\end{aligned}$$

This solves Exercise 5 **(e)**. □

Exercise 5 **(d)** also lets us solve Exercise 3 with less trouble than otherwise:

Hints to Exercise 3. The map $[p]\times[q]\to[n]$, $(i,j)\mapsto(i-1)q+j$ is a bijection (since $n=pq$). In other words, the map $[p]\times[q]\to[n]$, $(u,v)\mapsto(u-1)q+v$ is a bijection.

If (i,j) and (u,v) are two elements of $[p]\times[q]$, then we have the following equivalences:

$$((i-1)q+j<(u-1)q+v) \iff (i<u \text{ or } (i=u \text{ and } j<v)) \qquad (5)$$

and

$$((j-1)p+i>(v-1)p+u) \iff (j>v \text{ or } (j=v \text{ and } i>u)). \qquad (6)$$

(Indeed, both of these equivalences can easily be checked, by recalling that j and v belong to $[q]$ and that i and u belong to $[p]$.)

Let $k \in [n]$. Then, the definition of $\ell_k(\sigma)$ yields

$$\begin{aligned}
&\ell_k(\sigma) \\
&= \left(\text{the number of all } j \in \{k+1, k+2, \ldots, n\} \text{ such that } \sigma(k) > \sigma(j)\right) \\
&= \left(\text{the number of all } j \in [n] \text{ such that } k < j \text{ and } \sigma(k) > \sigma(j)\right) \\
&\qquad \left(\begin{array}{c}\text{since the } j \in \{k+1, k+2, \ldots, n\} \text{ are precisely} \\ \text{the } j \in [n] \text{ such that } k < j\end{array}\right) \\
&= \left(\text{the number of all } h \in [n] \text{ such that } k < h \text{ and } \sigma(k) > \sigma(h)\right) \\
&\qquad (\text{here, we have renamed the index } j \text{ as } h). \qquad (7)
\end{aligned}$$

Now, forget that we fixed k. We thus have proven (7) for each $k \in [n]$.

Fix $(i,j) \in [p] \times [q]$. Set $k = (i-1)q + j$. Then, $k \in [n]$, and thus (7) yields

$$\begin{aligned}
&\ell_k(\sigma) \\
&= \left(\text{the number of all } h \in [n] \text{ such that } k < h \text{ and } \sigma(k) > \sigma(h)\right) \\
&= \left(\text{the number of all } (u,v) \in [p] \times [q] \text{ such that } \underbrace{k}_{=(i-1)q+j} < (u-1)q + v \right. \\
&\qquad \left. \text{and } \sigma\left(\underbrace{k}_{=(i-1)q+j}\right) > \sigma((u-1)q+v)\right) \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } (u-1)q+v \text{ for } h\text{, since the} \\ \text{map } [p] \times [q] \to [n],\ (u,v) \mapsto (u-1)q+v \text{ is a bijection}\end{array}\right) \\
&= \left(\text{the number of all } (u,v) \in [p] \times [q] \text{ such that } (i-1)q + j < (u-1)q + v \right. \\
&\qquad \left. \text{and } \underbrace{\sigma((i-1)q+j)}_{\substack{=(j-1)p+i \\ (\text{by the definition of } \sigma)}} > \underbrace{\sigma((u-1)q+v)}_{\substack{=(v-1)p+u \\ (\text{by the definition of } \sigma)}}\right) \\
&= \left(\text{the number of all } (u,v) \in [p] \times [q] \text{ such that } \underbrace{(i-1)q + j < (u-1)q + v}_{\substack{\iff (i<u \text{ or } (i=u \text{ and } j<v)) \\ (\text{by (5)})}} \right. \\
&\qquad \left. \text{and } \underbrace{(j-1)p + i > (v-1)p + u}_{\substack{\iff (j>v \text{ or } (j=v \text{ and } i>u)) \\ (\text{by (6)})}}\right)
\end{aligned}$$

$$\begin{aligned}
&= (\text{the number of all } (u,v) \in [p] \times [q] \text{ such that } (i < u \text{ or } (i = u \text{ and } j < v)) \\
&\qquad \text{and } (j > v \text{ or } (j = v \text{ and } i > u))) \\
&= (\text{the number of all } (u,v) \in [p] \times [q] \text{ such that } (i < u \text{ or } (i = u \text{ and } j < v)) \\
&\qquad \text{and } j > v) \\
&\qquad \left(\begin{array}{c} \text{here, we have dismissed the possibility that } (j = v \text{ and } i > u), \\ \text{because this possibility is incompatible with} \\ \text{the condition } (i < u \text{ or } (i = u \text{ and } j < v)) \end{array} \right) \\
&= (\text{the number of all } (u,v) \in [p] \times [q] \text{ such that } i < u \text{ and } j > v) \\
&\qquad \left(\begin{array}{c} \text{here, we have dismissed the possibility that } (i = u \text{ and } j < v), \\ \text{because this possibility is incompatible with the condition } j > v \end{array} \right) \\
&= \underbrace{(\text{the number of all } u \in [p] \text{ such that } i < u)}_{= p - i} \\
&\qquad \cdot \underbrace{(\text{the number of all } v \in [q] \text{ such that } j > v)}_{= j - 1} \\
&= (p - i)(j - 1).
\end{aligned}$$

In view of $k = (i-1) q + j$, this rewrites as

$$\ell_{(i-1)q+j}(\sigma) = (p - i)(j - 1). \tag{8}$$

Now, forget that we fixed (i, j). We thus have proven (8) for each $(i, j) \in [p] \times [q]$.

Exercise 5 **(d)** yields

$$\begin{aligned}
\ell(\sigma) &= \ell_1(\sigma) + \ell_2(\sigma) + \cdots + \ell_n(\sigma) \\
&= \sum_{k\in[n]} \ell_k(\sigma) = \underbrace{\sum_{(i,j)\in[p]\times[q]}}_{=\sum_{i=1}^{p}\sum_{j=1}^{q}} \underbrace{\ell_{(i-1)q+j}(\sigma)}_{\substack{=(p-i)(j-1) \\ \text{(by (8))}}} \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } (i-1)q+j \text{ for } k \text{ in the sum,} \\ \text{since the map } [p]\times[q]\to[n],\ (i,j)\mapsto(i-1)q+j \\ \text{is a bijection}\end{array}\right) \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q}(p-i)(j-1) = \underbrace{\left(\sum_{i=1}^{p}(p-i)\right)}_{\substack{=\sum_{k=0}^{p-1} k \\ \text{(here, we have substituted } k \\ \text{for } p-i \text{ in the sum)}}} \underbrace{\left(\sum_{j=1}^{q}(j-1)\right)}_{\substack{=\sum_{k=0}^{q-1} k \\ \text{(here, we have substituted } k \\ \text{for } j-1 \text{ in the sum)}}} \\
&= \underbrace{\left(\sum_{k=0}^{p-1}k\right)}_{=\frac{(p-1)p}{2}} \underbrace{\left(\sum_{k=0}^{q-1}k\right)}_{=\frac{(q-1)q}{2}} = \frac{(p-1)p}{2}\cdot\frac{(q-1)q}{2} = \frac{pq(p-1)(q-1)}{4}.
\end{aligned}$$

This solves Exercise 3. □

0.5. Permutations as composed transpositions

Recall a basic notation regarding permutations, which we shall now extend:

Definition 0.5. Let $n \in \mathbb{N}$. Let i and j be two distinct elements of $[n]$. We let $t_{i,j}$ be the permutation in S_n which switches i with j while leaving all other elements of $[n]$ unchanged. Such a permutation is called a *transposition*.

Let us furthermore set $t_{i,i} = \mathrm{id}$ for each $i \in [n]$. Thus, $t_{i,j}$ is defined even when i and j are not distinct.

Thus, we have defined a permutation $t_{i,j} \in S_n$ whenever $n \in \mathbb{N}$ and whenever i and j are two elements of $[n]$. This permutation has the following properties:

- It satisfies $t_{i,j}(i) = j$ and $t_{i,j}(j) = i$.
- It leaves any element of $[n]$ other than i and j unchanged. (In other words, it satisfies $t_{i,j}(k) = k$ for each $k \in [n] \setminus \{i, j\}$.)
- It is an involution, i.e., it satisfies $t_{i,j} \circ t_{i,j} = \mathrm{id}$.

Exercise 6. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$.

(a) Prove that there is a unique n-tuple $(i_1, i_2, \ldots, i_n) \in [1] \times [2] \times \cdots \times [n]$ such that

$$\sigma = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{n,i_n}.$$

(b) Consider this n-tuple $(i_1, i_2, \ldots, i_n)$. Define the relation $\sim$ and the $\sim$-equivalence classes $E_1, E_2, \ldots, E_m$ as in Exercise 7 on homework set #7 (for $X = [n]$). (Thus, m is the number of cycles in the cycle decomposition of σ.)

Prove that m is the number of all $k \in [n]$ satisfying $i_k = k$.

A detailed solution to Exercise 6 **(a)** can be found in [Grinbe16, solution to Exercise 5.9]. Let us here give a brief sketch:

Solution to Exercise 6 (sketched). **(a)** The trick is to prove the following:

> *Observation 1:* Let $n \in \mathbb{N}$. Let $k \in \{0, 1, \ldots, n\}$. Let $\sigma \in S_n$ be such that
>
> $$(\sigma(i) = i \text{ for each } i \in \{k+1, k+2, \ldots, n\}). \qquad (9)$$
>
> Then, there is a unique k-tuple $(i_1, i_2, \ldots, i_k) \in [1] \times [2] \times \cdots \times [k]$ such that $\sigma = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{k,i_k}$.

[*Proof of Observation 1:* This is proven by induction on k.

The *induction base* (the case $k = 0$) is a trivial exercise in understanding empty lists[1]. (In fact, for $k = 0$, the equality (9) shows that $\sigma(i) = i$ for each $i \in [n]$, and thus $\sigma = \mathrm{id} = (\text{empty composition of permutations}) = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{0,i_0}$ for the 0-tuple $(i_1, i_2, \ldots, i_0) = ()$.)

Induction step: Let $k \in \{0, 1, \ldots, n\}$ be positive. Assume (as the induction hypothesis) that Observation 1 holds for $k-1$ instead of k. We then must prove Observation 1 for k. So let $\sigma \in S_n$ be such that (9) holds. We must prove that there is a unique k-tuple $(i_1, i_2, \ldots, i_k) \in [1] \times [2] \times \cdots \times [k]$ such that $\sigma = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{k,i_k}$.

Set $g = \sigma^{-1}(k)$. Thus, $\sigma(g) = k$ and $g \in [k]$ [2]. Thus, k and g belong to the set $[k]$.

The permutation $t_{k,g}$ is either a transposition (if $k \neq g$) or the identity map (if $k = g$). In either case, it satisfies $t_{k,g} \circ t_{k,g} = \mathrm{id}$ and leaves all elements of $[n]$ other than k and g unchanged. Hence, the permutation $t_{k,g}$ leaves each $i \in \{k+1, k+2, \ldots, n\}$ unchanged (since i does **not** belong to the set $[k]$, and thus i equals neither k nor g).

Define $\tau \in S_n$ by $\tau = \sigma \circ t_{k,g}$. (Notice that $\left(t_{k,g}\right)^{-1} = t_{k,g}$.) Then, from (9), we can easily derive that $\tau(i) = i$ for each $i \in \{k+1, k+2, \ldots, n\}$ (because the permutation $t_{k,g}$ leaves i unchanged). Combining this with the fact that $\tau(k) = k$

[1] Specifically, you need to know that there is only one 0-tuple $(i_1, i_2, \ldots, i_0)$, namely the empty 0-tuple $()$.

[2] *Proof.* Assume the contrary. Thus, $g \notin [k]$, so that $g \in \{k+1, k+2, \ldots, n\}$. Therefore, (9) (applied to $i = g$) yields $\sigma(g) = g$. But $\sigma(g) = k \in [k]$. This contradicts $\sigma(g) = g \notin [k]$. This contradiction shows that our assumption was false, qed.

(because $\underbrace{\tau}_{=\sigma\circ t_{k,g}}(k)=\sigma\left(\underbrace{t_{k,g}(k)}_{=g}\right)=\sigma(g)=k$), we conclude that $\tau(i)=i$ for each $i\in\{k,k+1,\ldots,n\}$. Hence, by the induction hypothesis, we can apply Observation 1 to $k-1$ and τ instead of k and σ. We conclude that there is a unique $(k-1)$-tuple $(i_1,i_2,\ldots,i_{k-1})\in[1]\times[2]\times\cdots\times[k-1]$ such that $\tau=t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k-1,i_{k-1}}$. We can easily extend this $(k-1)$-tuple to a k-tuple $(i_1,i_2,\ldots,i_k)\in[1]\times[2]\times\cdots\times[k]$ such that $\sigma=t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k,i_k}$ [3]. Thus, there exists **at least one** k-tuple $(i_1,i_2,\ldots,i_k)\in[1]\times[2]\times\cdots\times[k]$ such that $\sigma=t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k,i_k}$.

Recall that we must prove that there is a **unique** k-tuple $(i_1,i_2,\ldots,i_k)\in[1]\times[2]\times\cdots\times[k]$ such that $\sigma=t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k,i_k}$. We have just proven that there exists **at least one** such k-tuple. Hence, it only remains to show that there exists **at most one** such k-tuple.

Let $(u_1,u_2,\ldots,u_k)$ and $(v_1,v_2,\ldots,v_k)$ be two k-tuples $(i_1,i_2,\ldots,i_k)\in[1]\times[2]\times\cdots\times[k]$ such that $\sigma=t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k,i_k}$. We shall prove that $(u_1,u_2,\ldots,u_k)=(v_1,v_2,\ldots,v_k)$. This will, of course, entail that there exists **at most one** such k-tuple; thus, the induction step will be complete.

We know that $(u_1,u_2,\ldots,u_k)$ is a k-tuple $(i_1,i_2,\ldots,i_k)\in[1]\times[2]\times\cdots\times[k]$ such that $\sigma=t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k,i_k}$. In other words, $(u_1,u_2,\ldots,u_k)\in[1]\times[2]\times\cdots\times[k]$ and $\sigma=t_{1,u_1}\circ t_{2,u_2}\circ\cdots\circ t_{k,u_k}$. Notice that $(u_1,u_2,\ldots,u_k)\in[1]\times[2]\times\cdots\times[k]$ shows that $u_j\in[j]$ for each $j\in[k]$. In other words, $u_j\le j$ for each $j\in[k]$. Thus, each $j\in[k-1]$ satisfies $t_{j,u_j}(k)=k$ (because k equals neither j nor u_j (since $u_j\le j\le k-1<k$)). In other words, the permutations $t_{1,u_1},t_{2,u_2},\ldots,t_{k-1,u_{k-1}}$ leave k unchanged. Now,

$$\begin{aligned}\underbrace{\sigma}_{=t_{1,u_1}\circ t_{2,u_2}\circ\cdots\circ t_{k,u_k}}(u_k)&=\left(t_{1,u_1}\circ t_{2,u_2}\circ\cdots\circ t_{k,u_k}\right)(u_k)\\&=\left(t_{1,u_1}\circ t_{2,u_2}\circ\cdots\circ t_{k-1,u_{k-1}}\right)\left(\underbrace{t_{k,u_k}(u_k)}_{=k}\right)\\&=\left(t_{1,u_1}\circ t_{2,u_2}\circ\cdots\circ t_{k-1,u_{k-1}}\right)(k)=k\end{aligned}$$

[3] *Proof.* To extend the $(k-1)$-tuple $(i_1,i_2,\ldots,i_{k-1})\in[1]\times[2]\times\cdots\times[k-1]$ to a k-tuple $(i_1,i_2,\ldots,i_k)\in[1]\times[2]\times\cdots\times[k]$, we need only to define i_k. Let us define i_k by $i_k=g$. This yields a well-defined k-tuple $(i_1,i_2,\ldots,i_k)\in[1]\times[2]\times\cdots\times[k]$, because $i_k=g\in[k]$. It remains to prove that this k-tuple satisfies $\sigma=t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k,i_k}$.

We have $\tau=\sigma\circ t_{k,g}$, so that $\tau\circ t_{k,g}=\sigma\circ\underbrace{t_{k,g}\circ t_{k,g}}_{=\mathrm{id}}=\sigma$, so that

$$\sigma=\underbrace{\tau}_{=t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k-1,i_{k-1}}}\circ\underbrace{t_{k,g}}_{\substack{=t_{k,i_k}\\(\text{since } g=i_k)}}=\left(t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k-1,i_{k-1}}\right)\circ t_{k,i_k}=t_{1,i_1}\circ t_{2,i_2}\circ\cdots\circ t_{k,i_k}.$$

This completes our proof.

(since the permutations $t_{1,u_1}, t_{2,u_2}, \ldots, t_{k-1,u_{k-1}}$ leave k unchanged). Thus, $u_k = \sigma^{-1}(k) = g$. Similarly, $v_k = g$.

Now,

$$\sigma = t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k,u_k} = \left(t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k-1,u_{k-1}}\right) \circ t_{k,u_k}$$
$$= \left(t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k-1,u_{k-1}}\right) \circ t_{k,g} \qquad (\text{since } u_k = g),$$

so that

$$\tau = \underbrace{\sigma}_{=\left(t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k-1,u_{k-1}}\right) \circ t_{k,g}} \circ t_{k,g} = \left(t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k-1,u_{k-1}}\right) \circ \underbrace{t_{k,g} \circ t_{k,g}}_{=\operatorname{id}}$$
$$= t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k-1,u_{k-1}}.$$

In other words, $(u_1, u_2, \ldots, u_{k-1})$ is a $(k-1)$-tuple $(i_1, i_2, \ldots, i_{k-1}) \in [1] \times [2] \times \cdots \times [k-1]$ such that $\tau = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{k-1,i_{k-1}}$. Similarly, $(v_1, v_2, \ldots, v_{k-1})$ is such a $(k-1)$-tuple as well.

But recall that there is a unique $(k-1)$-tuple $(i_1, i_2, \ldots, i_{k-1}) \in [1] \times [2] \times \cdots \times [k-1]$ such that $\tau = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{k-1,i_{k-1}}$. Thus, any two such $(k-1)$-tuples are identical. Hence, $(u_1, u_2, \ldots, u_{k-1})$ and $(v_1, v_2, \ldots, v_{k-1})$ are identical (since $(u_1, u_2, \ldots, u_{k-1})$ and $(v_1, v_2, \ldots, v_{k-1})$ are two such $(k-1)$-tuples). Combining this with $u_k = v_k$ (which follows from $u_k = g$ and $v_k = g$), we obtain $(u_1, u_2, \ldots, u_k) = (v_1, v_2, \ldots, v_k)$. As we have said, this completes the induction step. Thus, Observation 1 is proven.]

Now, let $n \in \mathbb{N}$ and $\sigma \in S_n$. Then, $\{n+1, n+2, \ldots, n\}$ is the empty set. In other words, there exists no $i \in \{n+1, n+2, \ldots, n\}$. Hence, the statement $(\sigma(i) = i$ for each $i \in \{n+1, n+2, \ldots, n\})$ is vacuously true. Thus, Observation 1 (applied to $k = n$) shows that there is a unique n-tuple $(i_1, i_2, \ldots, i_n) \in [1] \times [2] \times \cdots \times [n]$ such that $\sigma = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{n,i_n}$. This solves Exercise 6 **(a)**.

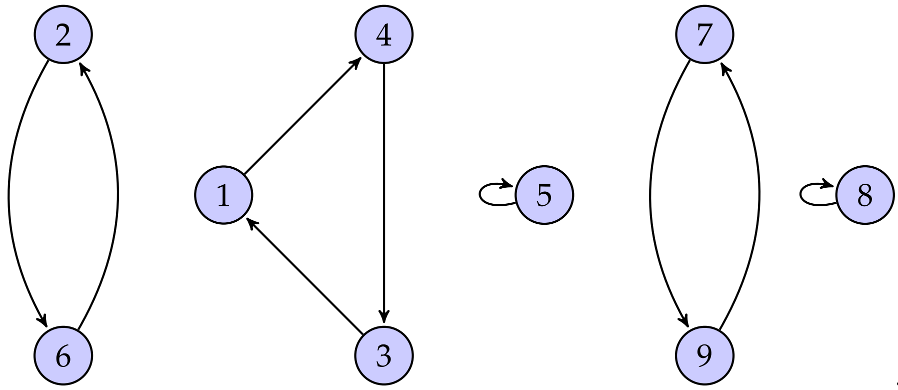
(b) If $\tau \in S_n$ is any permutation, then $z(\tau)$ shall denote the number of cycles in the cycle decomposition of τ. Thus, $m = z(\sigma)$ (since m is the number of cycles in the cycle decomposition of σ). Hence, it remains to prove that $z(\sigma)$ is the number of all $k \in [n]$ satisfying $i_k = k$.

Let us first prove a basic fact:

> *Observation 2:* Let $\tau \in S_n$ and $p \in [n]$ be such that $\tau(p) = p$. Let q be an element of $[n]$ distinct from p. Then, $z(\tau \circ t_{p,q}) = z(\tau) - 1$.

[*Example:* For this example, let $n = 9$, and let $\tau \in S_9$ be the permutation whose one-line notation is $(4, 6, 1, 3, 5, 2, 9, 8, 7)$ (that is, which satisfies $(\tau(1), \tau(2), \ldots, \tau(9)) =$

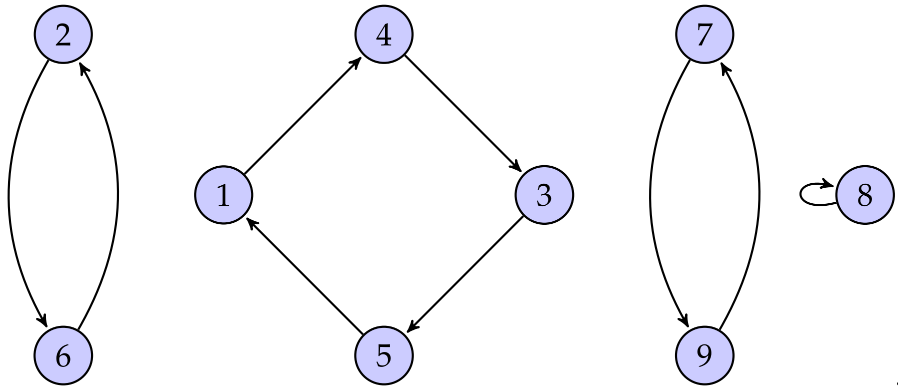
$(4,6,1,3,5,2,9,8,7))$. Then, the cycle decomposition of τ looks as follows:



.

This contains 5 cycles. Thus, $z(\tau) = 5$.

Now, let $p = 5$ and $q = 3$. (This clearly satisfies $\tau(p) = p$.) Then, Observation 2 yields $z(\tau \circ t_{p,q}) = \underbrace{z(\tau)}_{=5} - 1 = 5 - 1 = 4$. And we can indeed confirm this: The cycle decomposition of $\tau \circ t_{p,q} = \tau \circ t_{5,3}$ looks as follows:



.

This contains 4 cycles. Thus, $z(\tau \circ t_{p,q}) = 4$, exactly as Observation 2 foretold.

As this example shows, the cycle decomposition of $\tau \circ t_{p,q}$ is actually "almost the same as" that of τ; more precisely, all cycles of τ appear in the cycle decomposition of $\tau \circ t_{p,q}$, with the exception of two cycles (the cycles $\{5\}$ and $\{3,1,4\}$), which get merged into a single cycle in the cycle decomposition of $\tau \circ t_{p,q}$. Visually speaking, when we compose τ with $t_{p,q}$, we "re-route" the arc from $\sigma^{-1}(q) = 4$ to $q = 3$ through the vertex $p = 5$; therefore, the vertex p (which formed a 1-vertex cycle in τ, since $\tau(p) = p$) gets "caught up" in the cycle $\{3,1,4\}$, which causes the two cycles to get merged. This behavior clearly generalizes; the proof below just makes this more formal.]

[*Proof of Observation 2:* The cycle decomposition of τ has a cycle containing the element p alone (since $\tau(p) = p$). Let $\mathfrak{z}_1$ be this cycle. Thus, $\mathfrak{z}_1 = \{p\}$. Hence, $\mathfrak{z}_1$ does not contain q (since $q \neq p$).

Furthermore, let $\mathfrak{z}_2$ be the cycle in the cycle decomposition of τ that contains the element q. This cycle $\mathfrak{z}_2$ is distinct from $\mathfrak{z}_1$ (because $\mathfrak{z}_1$ does not contain q). Thus, $\mathfrak{z}_2$

does not contain p (since p is contained in the cycle $\mathfrak{z}_1$, which is distinct from $\mathfrak{z}_2$). In other words, $p \notin \mathfrak{z}_2$.

Let us analyze what happens to the cycle decomposition of τ when we compose τ with $t_{p,q}$ (thus obtaining $\tau \circ t_{p,q}$). The only values of τ that change when we compose τ with $t_{p,q}$ are the values at the numbers p and q (because $t_{p,q}$ leaves all other numbers unchanged). Hence, all cycles other than $\mathfrak{z}_1$ and $\mathfrak{z}_2$ in the cycle decomposition of τ remain unchanged in the cycle decomposition of $\tau \circ t_{p,q}$ (because these cycles contain neither p nor q). The only two cycles that can possibly change are $\mathfrak{z}_1$ and $\mathfrak{z}_2$. We claim that these two cycles are **merged into a single cycle** in $\tau \circ t_{p,q}$.

Indeed, let us write the cycle $\mathfrak{z}_2$ in the form $\mathfrak{z}_2 = \left\{\tau^0 (q), \tau^1 (q), \ldots, \tau^{k-1} (q)\right\}$, where k is the smallest positive integer satisfying $\tau^k (q) = q$. (Indeed, $\mathfrak{z}_2$ can be written in this form, since $\mathfrak{z}_2$ is the cycle of τ that contains q.) Thus,

$$\mathfrak{z}_2 = \left\{\tau^0 (q), \tau^1 (q), \ldots, \tau^{k-1} (q)\right\} = \left\{\tau^1 (q), \tau^2 (q), \ldots, \tau^{k} (q)\right\}$$

(since $\tau^0 (q) = q = \tau^k (q)$).

Let γ be the permutation $\tau \circ t_{p,q} \in S_n$. Thus, each $i \in [k-1]$ satisfies $\gamma\left(\tau^i (q)\right) = \tau^{i+1} (q)$ [4]. In other words, the permutation γ sends each of the elements $\tau^1 (q), \tau^2 (q), \ldots, \tau^k (q)$ (apart from the last one) to the next one. Hence, the elements $\tau^1 (q), \tau^2 (q), \ldots, \tau^k (q)$ lie on one and the same cycle in the cycle decomposition of γ. Let us denote this cycle by $\mathfrak{z}'$. Thus, $\tau^i (q) \in \mathfrak{z}'$ for each $i \in [k]$. Applying this to $i = k$, we conclude that $\tau^k (q) \in \mathfrak{z}'$. Thus, $q = \tau^k (q) \in \mathfrak{z}'$.

The cycle $\mathfrak{z}'$ contains $\tau^1 (q), \tau^2 (q), \ldots, \tau^k (q)$. In other words, the cycle $\mathfrak{z}'$ contains all elements of $\mathfrak{z}_2$ (since $\mathfrak{z}_2 = \left\{\tau^1 (q), \tau^2 (q), \ldots, \tau^k (q)\right\}$).

Also, $\underbrace{\gamma}_{=\tau \circ t_{p,q}} (q) = \left(\tau \circ t_{p,q}\right)(q) = \tau\left(\underbrace{t_{p,q}(q)}_{=p}\right) = \tau(p) = p$. Hence, p lies on the same cycle in the cycle decomposition of γ as q. In other words, p lies on the cycle in the cycle decomposition of γ that contains q. Since the latter cycle is $\mathfrak{z}'$ (because $q \in \mathfrak{z}'$), we thus conclude that p lies on $\mathfrak{z}'$. In other words, $p \in \mathfrak{z}'$. In other words, the cycle $\mathfrak{z}'$ contains all elements of $\mathfrak{z}_1$ (since $\mathfrak{z}_1 = \{p\}$).

The cycle $\mathfrak{z}'$ in the cycle decomposition of γ thus contains all elements of $\mathfrak{z}_1$ and all elements of $\mathfrak{z}_2$. In view of $\gamma = \tau \circ t_{p,q}$, this rewrites as follows: The cycle $\mathfrak{z}'$ in the cycle decomposition of $\tau \circ t_{p,q}$ contains all elements of $\mathfrak{z}_1$ and all elements of $\mathfrak{z}_2$. Furthermore, this cycle $\mathfrak{z}'$ cannot contain any other elements (because if it did, then

[4] *Proof.* Let $i \in [k-1]$. Hence, $\tau^i (q) \neq q$ (since k is the **smallest** positive integer satisfying $\tau^k (q) = q$). Also, $\tau^i (q) \neq p$ (since $\tau^i (q) \in \left\{\tau^0 (q), \tau^1 (q), \ldots, \tau^{k-1} (q)\right\} = \mathfrak{z}_2$ but $p \notin \mathfrak{z}_2$). Thus, $\tau^i (q)$ equals neither p nor q. Hence, the transposition $t_{p,q}$ leaves $\tau^i (q)$ unchanged. In other words, $t_{p,q}\left(\tau^i (q)\right) = \tau^i (q)$.

Now, $\underbrace{\gamma}_{=\tau \circ t_{p,q}} \left(\tau^i (q)\right) = \left(\tau \circ t_{p,q}\right)\left(\tau^i (q)\right) = \tau\left(\underbrace{t_{p,q}\left(\tau^i (q)\right)}_{=\tau^i (q)}\right) = \tau\left(\tau^i (q)\right) = \tau^{i+1} (q)$, qed.

it would contain elements from cycles in the cycle decomposition of τ other than $\mathfrak{z}_1$ and $\mathfrak{z}_2$; but this would contradict the fact that all cycles other than $\mathfrak{z}_1$ and $\mathfrak{z}_2$ in the cycle decomposition of τ remain unchanged in the cycle decomposition of $\tau \circ t_{p,q}$). Hence, this cycle $\mathfrak{z}'$ contains all elements of $\mathfrak{z}_1$ and all elements of $\mathfrak{z}_2$ and no more elements. Thus, the cycles $\mathfrak{z}_1$ and $\mathfrak{z}_2$ are merged into a single cycle in $\tau \circ t_{p,q}$.

So we have seen that when we compose τ with $t_{p,q}$, the cycle decomposition does not change except for the fact that the two cycles $\mathfrak{z}_1$ and $\mathfrak{z}_2$ get merged into a single cycle. Thus, the total number of cycles in the cycle decomposition decreases by 1. In other words, the total number of cycles in the cycle decomposition of $\tau \circ t_{p,q}$ is 1 less than the total number of cycles in the cycle decomposition of τ. In other words, $z\left(\tau \circ t_{p,q}\right) = z\left(\tau\right) - 1$. This proves Observation 2.]

Next, we make the following claim: For each $p \in \{0, 1, \ldots, n\}$, we have

$$z\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p,i_p}\right) = n - p + \left|\{k \in [p] \mid i_k = k\}\right|. \tag{10}$$

[*Proof of (10):* We shall prove (10) by induction on p:

Induction base: We have

$$z\left(\underbrace{t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{0,i_0}}_{=\mathrm{id}}\right) = z\left(\mathrm{id}\right) = n$$

(since the permutation id has n cycles in its cycle decomposition). Comparing this with

$$n - 0 + \left|\underbrace{\{k \in [0] \mid i_k = k\}}_{\substack{=\varnothing \\ (\text{since } [0]=\varnothing)}}\right| = n - 0 + \underbrace{|\varnothing|}_{=0} = n,$$

we obtain $z\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{0,i_0}\right) = n - 0 + \left|\{k \in [0] \mid i_k = k\}\right|$. In other words, (10) holds for $p = 0$. This completes the induction base.

Induction step: Let $p \in \{0, 1, \ldots, n\}$ be positive. Assume that (10) holds for $p - 1$ instead of p. In other words, assume that

$$z\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}\right) = n - (p-1) + \left|\{k \in [p-1] \mid i_k = k\}\right|. \tag{11}$$

We must prove that (10) holds for p.

We have $p \in [n]$ (since $p \in \{0, 1, \ldots, n\}$ is positive). Also,

$$\left\{ k \in \underbrace{[p]}_{=\{p\} \cup [p-1]} \mid i_k = k \right\}$$
$$= \{k \in \{p\} \cup [p-1] \mid i_k = k\} = \underbrace{\{k \in \{p\} \mid i_k = k\}}_{= \begin{cases} \{p\}, & \text{if } i_p = p; \\ \varnothing, & \text{if } i_p \neq p \end{cases}} \cup \{k \in [p-1] \mid i_k = k\}$$
$$= \begin{cases} \{p\}, & \text{if } i_p = p; \\ \varnothing, & \text{if } i_p \neq p \end{cases} \cup \{k \in [p-1] \mid i_k = k\}. \qquad (12)$$

We are in one of the following two cases:

Case 1: We have $i_p = p$.

Case 2: We have $i_p \neq p$.

Let us first consider Case 1. In this case, we have $i_p = p$. Thus, $t_{p,i_p} = \mathrm{id}$. Also, (12) becomes

$$\{k \in [p] \mid i_k = k\}$$
$$= \underbrace{\begin{cases} \{p\}, & \text{if } i_p = p; \\ \varnothing, & \text{if } i_p \neq p \end{cases}}_{\substack{=\{p\} \\ (\text{since } i_p = p)}} \cup \{k \in [p-1] \mid i_k = k\} = \{p\} \cup \{k \in [p-1] \mid i_k = k\},$$

so that

$$|\{k \in [p] \mid i_k = k\}| = |\{p\} \cup \{k \in [p-1] \mid i_k = k\}|$$
$$= |\{k \in [p-1] \mid i_k = k\}| + 1 \qquad (13)$$

(since $p \notin \{k \in [p-1] \mid i_k = k\}$).

Now,

$$t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p,i_p} = \left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}} \right) \circ \underbrace{t_{p,i_p}}_{=\mathrm{id}} = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}.$$

Hence,

$$z\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p,i_p} \right) = z\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}} \right)$$
$$= n - (p-1) + |\{k \in [p-1] \mid i_k = k\}| \qquad (\text{by (11)})$$
$$= n - p + \underbrace{|\{k \in [p-1] \mid i_k = k\}| + 1}_{\substack{=|\{k \in [p] \mid i_k = k\}| \\ (\text{by (13)})}}$$
$$= n - p + |\{k \in [p] \mid i_k = k\}|.$$

Thus, we have proven that (10) holds for p in Case 1.

Let us now consider Case 2. In this case, we have $i_p \neq p$. But $i_p \in [p]$ (since $(i_1, i_2, \ldots, i_n) \in [1] \times [2] \times \cdots \times [n]$), so that $i_p \leq p$. Thus, $i_p < p$ (since $i_p \neq p$).

Also, (12) becomes

$$\begin{aligned} &\{k \in [p] \mid i_k = k\} \\ &= \underbrace{\begin{cases} \{p\}, & \text{if } i_p = p; \\ \varnothing, & \text{if } i_p \neq p \end{cases}}_{\substack{=\varnothing \\ (\text{since } i_p \neq p)}} \cup \{k \in [p-1] \mid i_k = k\} \\ &= \{k \in [p-1] \mid i_k = k\}. \end{aligned} \tag{14}$$

Let $\tau = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}$. Thus,

$$\begin{aligned} z(\tau) &= z\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}\right) = \underbrace{n-(p-1)}_{=n-p+1} + \left|\underbrace{\{k \in [p-1] \mid i_k = k\}}_{\substack{=\{k \in [p] \mid i_k = k\} \\ (\text{by (14)})}}\right| \\ &= n - p + 1 + |\{k \in [p] \mid i_k = k\}|. \end{aligned} \tag{15}$$

But

$$t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p,i_p} = \underbrace{\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}\right)}_{=\tau} \circ t_{p,i_p} = \tau \circ t_{p,i_p}. \tag{16}$$

We have $\tau(p) = p$ [5]. Hence, Observation 2 (applied to $q = i_p$) yields $z\left(\tau \circ t_{p,i_p}\right) = z(\tau) - 1$. But from (16), we obtain

$$\begin{aligned} z\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p,i_p}\right) &= z\left(\tau \circ t_{p,i_p}\right) = z(\tau) - 1 \\ &= n - p + |\{k \in [p] \mid i_k = k\}| \qquad (\text{by (15)}). \end{aligned}$$

Thus, we have proven that (10) holds for p in Case 2.

We thus know that (10) holds for p (because we have proven this in each of the two Cases 1 and 2). This completes the induction step. Thus, (10) is proven.]

[5] *Proof.* From $(i_1, i_2, \ldots, i_n) \in [1] \times [2] \times \cdots \times [n]$, we conclude that $i_j \in [j]$ for each $j \in [n]$. Thus, for each $j \in [p-1]$, we have $i_j \in [j]$, so that $i_j \leq j \leq p-1 < p$. Therefore, for each $j \in [p-1]$, the permutation t_{j,i_j} leaves the number p unchanged (since p equals neither j nor i_j (because $i_j \leq j < p$)). In other words, the permutations $t_{1,i_1}, t_{2,i_2}, \ldots, t_{p-1,i_{p-1}}$ leave the number p unchanged. Hence, $\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}\right)(p) = p$. In view of $\tau = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}$, this rewrites as $\tau(p) = p$.

Now, apply (10) to $p = n$. The result is

$$z\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{n,i_n}\right) = \underbrace{n - n}_{=0} + \left|\left\{k \in [n] \ \mid \ i_k = k\right\}\right| = \left|\left\{k \in [n] \ \mid \ i_k = k\right\}\right|.$$

In view of $\sigma = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{n,i_n}$, this rewrites as $z(\sigma) = \left|\left\{k \in [n] \ \mid \ i_k = k\right\}\right|$. In other words, $z(\sigma)$ is the number of all $k \in [n]$ satisfying $i_k = k$. This solves Exercise 6 **(b)**. □

0.6. Another partition identity

Recall the following:

Definition 0.6. Let $n \in \mathbb{Z}$. A *partition* of n means a finite list $(i_1, i_2, \ldots, i_k)$ of positive integers satisfying

$$i_1 \geq i_2 \geq \cdots \geq i_k \qquad \text{and} \qquad i_1 + i_2 + \cdots + i_k = n.$$

Exercise 7. Let $n \in \mathbb{N}$ and $p \in \mathbb{N}$. Let a be the number of all partitions $(i_1, i_2, \ldots, i_k)$ of n satisfying $k \geq p$ and $i_1 = i_2 = \cdots = i_p$. Let b be the number of all nonempty partitions $(i_1, i_2, \ldots, i_k)$ of n such that all of $i_1, i_2, \ldots, i_k$ are $\geq p$. Prove that $a = b$.

Example 0.7. Let $n = 9$ and $p = 3$. Then, the partitions counted by a in Exercise 7 are

$$(3,3,3), \qquad (2,2,2,2,1), \qquad (2,2,2,1,1,1), \qquad (1,1,1,1,1,1,1,1,1).$$

Meanwhile, the partitions counted by b in Exercise 7 are

$$(9), \qquad (6,3), \qquad (5,4), \qquad (3,3,3).$$

Thus, $a = 4$ and $b = 4$ in this case.

A full solution of Exercise 7 can be found in Angela Chen's homework. (This is also the solution I had in mind.)

Further reading on partitions includes:

- Herbert S. Wilf, *Lectures on Integer Partitions*, 2009.
  `https://www.math.upenn.edu/~wilf/PIMS/PIMSLectures.pdf`

- George E. Andrews, Kimmo Eriksson, *Integer Partitions*, Cambridge University Press 2004.

- Igor Pak, *Partition bijections, a survey*, Ramanujan Journal, vol. 12 (2006), pp. 5–75.
  `http://www.math.ucla.edu/~pak/papers/psurvey.pdf`

The Wikipedia articles on partitions, the pentagonal number theorem and Ramanujan's congruences are also useful. That said, none of these is necessary for the above exercise.

References

[AleGhe14] Emily Allen, Irina Gheorghiciuc, *A weighted interpretation for the super Catalan numbers*, arXiv:1403.5246v2.

[Gessel92] Ira M. Gessel, *Super Ballot Numbers*, Journal of Symbolic Computation, Volume 14, Issues 2–3, August-September 1992, pp. 179–194.
`https://doi.org/10.1016/0747-7171(92)90034-2`

[Grinbe16] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
`http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf`
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see `https://github.com/darijgr/detnotes/releases/tag/2019-01-10` .

[Han92] Guo-Niu Han, *Calcul Denertien*, PhD thesis 1991.
`http://emis.ams.org/journals/SLC/books/hanthese.html`