Math 4990 Fall 2017 (Darij Grinberg): homework set 8 page 1

Contents

0.1. Strange integers .................. 1
0.2. The length of a permutation .................. 4
0.3. Two equal counts .................. 5
0.4. Lehmer codes .................. 8
0.5. Permutations as composed transpositions .................. 14
0.6. Another partition identity .................. 23

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 3.24]. We will be rather brief here.

To solve Exercise 1, we need the following lemma (which is [Grinbe16, Exercise 3.23]):
Lemma 0.1. Let $m$ be a positive integer.

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

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

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

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

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

\[
m\binom{2m-1}{m-1} = (2m-1) \binom{2m-1}{m-1} \equiv 0 \mod 2,
\]

so that \( 0 \equiv \binom{2m-1}{m-1} \equiv \binom{2m-1}{m-1} \mod 2 \). In other words, \( \binom{2m-1}{m-1} \) is even. This proves Lemma 0.1 (b).

(c) We have \( \binom{2m}{m} = 2 \binom{2m-1}{m-1} \equiv 0 \mod 4 \) (since Lemma 0.1 (b) shows that \( \binom{2m-1}{m-1} \) 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

\[
T(m+1,n) = \frac{(2(m+1))!(2n)!}{(m+1)!n!(m+1+n)!} = \frac{(2m+2)(2m+1)(2m)!}{(m+1)\cdot m!\cdot (m+1+n)\cdot (m+n)!},
\]

since \( (2(m+1))! = (2m+2)(2m+1)(2m)! \) and \\
\[
= \frac{(2m+2)(2m+1)}{(m+1)(m+1+n)} \cdot \frac{(2m)!}{m!n!(m+n)!} = \frac{4m+2}{m+1+n} \cdot T(m,n).
\]

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

$$T(m, N + 1) = 4 \left( T(m, N) \right)_{\in \mathbb{N}} - T(m + 1, N)_{\in \mathbb{N}}$$

(by the induction hypothesis) 

(since Exercise 1 (a) yields $4T(m, N) = T(m + 1, N) + T(m, N + 1)$)

$$\in \mathbb{Z}$$

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 Exercise 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, $4T(m, N) \equiv 0 \pmod{2}$. 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, $T(m + 1, N) \equiv 0 \pmod{2}$.

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

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

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,
\[
T(m, 0) = \frac{(2m)! (2 \cdot 0)!}{m!0! (m + 0)!} = \frac{(2m)!}{m!m!} = \left( \frac{2m}{m} \right) \equiv 0 \mod 4
\]
(by Lemma 0.1 (b)). In other words, \( 4 \mid T(m, 0) \). This completes our proof that Exercise 0.1 \((d)\) holds for \( n = 0 \).

**Induction step:** Let \( N \in \mathbb{N} \). Assume (as the induction hypothesis) that Exercise 0.1 \((d)\) holds for \( n = N \). We must prove that Exercise 0.1 \((d)\) 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, \( T(m + 1, N) \equiv 0 \mod 4 \).

Also, Exercise 0.1 \((b)\) shows that \( T(m, N) \) is an integer. Thus, \( 4T(m, N) \equiv 0 \mod 4 \).

Now, Exercise 0.1 \((a)\) yields \( 4T(m, N) = T(m + 1, N) + T(m, N + 1) \). Thus,
\[
T(m, N + 1) = \underbrace{4T(m, N)}_{\equiv 0 \mod 4} \underbrace{- T(m + 1, N)}_{\equiv 0 \mod 4} \equiv 0 \mod 4.
\]

In other words, \( 4 \mid T(m, N + 1) \). In other words, Exercise 0.1 \((d)\) holds for \( n = N + 1 \). This completes the induction step. Hence, Exercise 0.1 \((d)\) is proven.

---

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

(a) Prove that
\[
\sum_{k=-p}^{p} (-1)^k \binom{m+n}{m+k} \binom{m+n}{n+k} = \binom{m+n}{m+n}.
\]

(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 0.1.

**[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 0.1 \((b)\).

A full solution of Exercise 2 can be found in Angela Chen’s homework and in [Grinbe16, solution to Exercise 3.24] (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 \( \sigma \) means a pair \((i, j)\) of elements of \([n]\) satisfying \( i < j \) and \( \sigma(i) > \sigma(j) \).

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

(d) The sign of \( \sigma \) 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 \( \sigma \) 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 \( \sigma \) then sends each entry of \( A \) to the corresponding entry of \( B \).

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

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

\[(\text{the number of all } (i, j) \in [n] \times [n] \text{ such that } i \geq j > \sigma(i))\]

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

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

(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 $\sigma$ 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

\[
[p \geq q > r] = [p \geq q \text{ and } q > r] = [p \geq q, q > r] = [p \geq q](1 - [r \geq q])
\]

\[
= [p \geq q] - [p \geq q][r \geq q].
\]

(2)

But

\[
\begin{align*}
\sum_{i \in [n]} [i \geq j > \sigma(i)] &= \sum_{i \in [n]} ([i \geq j] - [i \geq j][\sigma(i) \geq j]) \\
&= \sum_{i \in [n]} [i \geq j] - \sum_{i \in [n]} [i \geq j][\sigma(i) \geq j]
\end{align*}
\]

(3)

and similarly

\[
\text{(the number of all } i \in [n] \text{ such that } \sigma(i) \geq j > i)
\]

\[
= \sum_{i \in [n]} [\sigma(i) \geq j] - \sum_{i \in [n]} [\sigma(i) \geq j][i \geq j].
\]

Hence,

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

(4)

Here, we have substituted $i$ for $\sigma(i)$ in the sum, since the map $\sigma$ is a bijection $[n] \to [n]$.

\[
\begin{align*}
= \sum_{i \in [n]} [i \geq j] - \sum_{i \in [n]} [i \geq j][\sigma(i) \geq j]
\end{align*}
\]

= (the number of all $i \in [n]$ such that $i \geq j > \sigma(i))$
(by (3)). This proves Lemma 0.3.

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

We have

\[
\left( \text{the number of all } i \in [n] \text{ such that } i \geq j \land \sigma(i) \geq j \right) \\
\quad \iff (i \geq j \text{ but not } \sigma(i) \geq j)
\]

\[
= (\text{the number of all } i \in [n] \text{ such that } i \geq j \text{ but not } \sigma(i) \geq j)
\]

\[
= (\text{the number of all } i \in [n] \text{ such that } i \geq j)
\]

and

\[
\left( \text{the number of all } i \in [n] \text{ such that } \sigma(i) \geq j > \sigma(i) \right)
\]

\[
\iff (\sigma(i) \geq j \text{ but not } i \geq j)
\]

\[
= (\text{the number of all } i \in [n] \text{ such that } \sigma(i) \geq j \text{ but not } i \geq j)
\]

\[
= (\text{the number of all } i \in [n] \text{ such that } \sigma(i) \geq j)
\]

Comparing these two equalities, we obtain

\[
(\text{the number of all } i \in [n] \text{ such that } i \geq j > \sigma(i))
\]

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

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

\[
\{ i \in [n] \mid i \geq j > \sigma(i) \} \to \{ i \in [n] \mid \sigma(i) \geq j > i \},
\]

\[
i \mapsto \left( \sigma^{k-1}(i), \text{ where } k \text{ is the smallest positive integer satisfying } \sigma^k(i) \geq j \right)
\]
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

\[
\{ i \in [n] \mid \sigma (i) \geq j > i \} \rightarrow \{ i \in [n] \mid i \geq j \}
\]

\[
i \mapsto \left( (\sigma^{-1})^k (i) \right), \quad \text{where } k \text{ is the smallest nonnegative integer satisfying } (\sigma^{-1})^k (i) \geq j
\]

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

\[\square\]

### 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

\[
S_n \rightarrow G,
\]

\[
\sigma \mapsto (\ell_1 (\sigma), \ell_2 (\sigma), \ldots, \ell_n (\sigma))
\]

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 \( \sigma \).
Parts (b), (c), (d) and (e) of Exercise 5 are proven in [Grinbe16, §5.8 and the solution to Exercise 5.17]. (Specifically, Exercise 5(b) is [Grinbe16, Proposition 5.44]; Exercise 5(c) is [Grinbe16, Theorem 5.49]; Exercise 5(d) is [Grinbe16, Proposition 5.43]; Exercise 5(e) is [Grinbe16, Corollary 5.50]). 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, \( \sigma \) is a permutation. Thus, the numbers \( \sigma(1), \sigma(2), \ldots, \sigma(n) \) are distinct. Now,

\[
\left\{ \begin{array}{c}
\{1, 2, \ldots, n\} \\
\setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}
\end{array} \right. \\
= \{\sigma(1), \sigma(2), \ldots, \sigma(n)\} \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}
\]

(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 \( \{\sigma(i), \sigma(i + 1), \ldots, \sigma(n)\} \).

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

$$\ell(\sigma) = (\text{the number of inversions of } \sigma)$$

$$= (\text{the number of pairs } (i,j) \text{ of elements of } [n] \text{ satisfying } i < j \text{ and } \sigma(i) > \sigma(j))$$

(by the definition of an inversion)

$$= \sum_{i \in [n]} (\text{the number of } j \in [n] \text{ satisfying } i < j \text{ and } \sigma(i) > \sigma(j))$$

(by the definition of an inversion)

$$= \sum_{i \in [n]} (\text{the number of } j \in \{i+1, i+2, \ldots, n\} \text{ such that } \sigma(i) > \sigma(j))$$

(since the $j \in [n]$ satisfying $i < j$ are precisely the $j \in \{i+1, i+2, \ldots, n\}$)

$$= \sum_{i \in [n]} \ell_i(\sigma)$$

(by the definition of $\ell_i(\sigma)$)

$$= \sum_{i \in [n]} \ell_i(\sigma) = \ell_1(\sigma) + \ell_2(\sigma) + \cdots + \ell_n(\sigma).$$

This solves Exercise 5(d).
(e) We have
\[
\sum_{\sigma \in S_n} x^{\ell_1(\sigma)} + \ell_2(\sigma) + \cdots + \ell_n(\sigma)
\]
(by Exercise 5(d))
\[
= \sum_{\sigma \in S_n} x^{\ell_1(\sigma)} + \ell_2(\sigma) + \cdots + \ell_n(\sigma)
= \sum_{(i_1, i_2, \ldots, i_n) \in G} x^{i_1 + i_2 + \cdots + i_n}
\]
where we have substituted \((i_1, i_2, \ldots, i_n)\) for \((\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma))\)
in the sum, since the map \(S_n \to G, \sigma \mapsto (\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma))\)
is a bijection (by Exercise 5(c)).
\[
= \sum_{i_1 \in \{0, 1, \ldots, n-1\}} \sum_{i_2 \in \{0, 1, \ldots, n-2\}} \cdots \sum_{i_n \in \{0, 1, \ldots, n-n\}} x^{i_1} x^{i_2} \cdots x^{i_n}
\]
\[
= \left( \sum_{i_1 \in \{0, 1, \ldots, n-1\}} x^{i_1} \right) \left( \sum_{i_2 \in \{0, 1, \ldots, n-2\}} x^{i_2} \right) \cdots \left( \sum_{i_n \in \{0, 1, \ldots, n-n\}} x^{i_n} \right)
\]
\[
= (1 + x + x^2 + \cdots + x^{n-1}) (1 + x + x^2 + \cdots + x^{n-2}) \cdots (1 + x + x^2 + \cdots + x^{n-n})
\]
\[
= (1 + x + x^2 + \cdots + x^{n-1}) (1 + x + x^2 + \cdots + x^{n-2}) (1 + x)
\]
\[
= (1 + x) \left( 1 + x + x^2 \right) \cdots \left( 1 + x + x^2 + \cdots + x^{n-1} \right).
\]
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:
\[
((i - 1)q + j < (u - 1)q + v) \iff (i < u \text{ or } (i = u \text{ and } j < v)) \quad (5)
\]
and
\[
((j - 1)p + i > (v - 1)p + u) \iff (j > v \text{ or } (j = v \text{ and } i > u)). \quad (6)
\]
(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

$$\ell_k (\sigma) = (\text{the number of all } j \in \{k + 1, k + 2, \ldots, n\} \text{ such that } \sigma (k) > \sigma (j))$$

$$= (\text{the number of all } j \in [n] \text{ such that } k < j \text{ and } \sigma (k) > \sigma (j))$$

(since the $j \in \{k + 1, k + 2, \ldots, n\}$ are precisely the $j \in [n]$ such that $k < j$)

$$= (\text{the number of all } h \in [n] \text{ such that } k < h \text{ and } \sigma (k) > \sigma (h))$$

(here, we have renamed the index $j$ as $h$).

(7)

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

$$\ell_k (\sigma) = (\text{the number of all } h \in [n] \text{ such that } k < h \text{ and } \sigma (k) > \sigma (h))$$

$$= \left( \text{the number of all } (u, v) \in [p] \times [q] \text{ such that } \frac{k}{= (i - 1)q + j} < (u - 1)q + v$$

and $\sigma \left( \frac{k}{= (i - 1)q + j} \right) > \sigma ((u - 1)q + v)$

here, we have substituted $(u - 1)q + v$ for $h$, since the map $[p] \times [q] \to [n], (u, v) \mapsto (u - 1)q + v$ is a bijection

$$= (\text{the number of all } (u, v) \in [p] \times [q] \text{ such that } (i - 1)q + j < (u - 1)q + v$$

and $\sigma \left( \frac{(i - 1)q + j}{= (j - 1)p + i} \right) > \sigma \left( \frac{(u - 1)q + v}{= (v - 1)p + u} \right)$

(by the definition of $\sigma$)

$$\iff (i < u \text{ or } (i = u \text{ and } j < v))$$

(by 5)

(by 6)

$$\iff (j > v \text{ or } (j = v \text{ and } i > u))$$

(by 6)
= (the number of all \((u,v) \in [p] \times [q]\) such that \((i < u \text{ or } (i = u \text{ and } j < v))\)
and \((j > v \text{ or } (j = v \text{ and } i > u)))\)

= (the number of all \((u,v) \in [p] \times [q]\) such that \((i < u \text{ or } (i = u \text{ and } j < v))\)
and \(j > v)\)

here, we have dismissed the possibility that \((j = v \text{ and } i > u)\),
because this possibility is incompatible with
the condition \((i < u \text{ or } (i = u \text{ and } j < v))\)\)

= (the number of all \((u,v) \in [p] \times [q]\) such that \(i < u \text{ and } j > v)\)

here, we have dismissed the possibility that \((i = u \text{ and } j < v)\),
because this possibility is incompatible with the condition \(j > v)\)

= (the number of all \(u \in [p]\) such that \(i < u)\)

\[= p - i \cdot \text{(the number of all } v \in [q]\text{ such that } j > v)\]

\[= j - 1\]

= \((p - i) (j - 1)\).

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

\[\ell_{(i-1)q+j}(\sigma) = (p - i) (j - 1).\]  \hspace{1cm} (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
\[ \ell_n(\sigma) = \ell_1(\sigma) + \ell_2(\sigma) + \cdots + \ell_n(\sigma) \]
\[ = \sum_{k \in [n]} \ell_k(\sigma) = \sum_{(i,j) \in [p] \times [q]} \ell_{(i-1)q+j}(\sigma) \]
\[ = \sum_{i=1}^{p} \sum_{j=1}^{q} \ell_{i} \cdot \ell_{j} \]
\[ = \sum_{k=0}^{p-1} \frac{p-1}{2} \cdot \frac{(q-1)q}{2} = \frac{pq(p-1)(q-1)}{4}. \]

This solves Exercise 5.

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 \( t_{ij} \) 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 \( t_{ii} = \text{id} \) for each \( i \in [n] \). Thus, \( t_{ij} \) is defined even when \( i \) and \( j \) are not distinct.

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

- It satisfies \( t_{ij}(i) = j \) and \( t_{ij}(j) = i \).
- It leaves any element of \([n]\) other than \( i \) and \( j \) unchanged. (In other words, it satisfies \( t_{ij}(k) = k \) for each \( k \in [n] \setminus \{i,j\} \)).
- It is an involution, i.e., it satisfies \( t_{ij} \circ t_{ij} = \text{id} \).
**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 \( \sigma \).)
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
\[
(\sigma (i) = i \text{ for each } i \in \{k+1, k+2, \ldots, n\}). \tag{9}
\]
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. In fact, for \( k = 0 \), the equality (9) shows that \( \sigma (i) = i \) for each \( i \in [n] \), and thus \( \sigma = \text{id} = (\text{empty composition of permutations}) = t_{1, i_1} \circ t_{2, i_2} \circ \cdots \circ t_{0, i_0} \) 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 \( g \in [k] \). 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 \( t_{k, g} \circ t_{k, g} = \text{id} \) 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 \( g \)).

Defining \( \tau \in S_n \) by \( \tau = \sigma \circ t_{k, g} \). (Notice that \( (t_{k, g})^{-1} = t_{k, g} \).) 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 \( \tau (k) = k \)

---

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

2Proof: 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 $\tau (k) = \sigma (t_{k,g} (k)) = \sigma (g) = k$), 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 $k$ and $\tau$ instead of $k$ and $\sigma$. 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 $\sigma = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{k,i_k}$. 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 $\sigma = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{k,i_k}$. 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. 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 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, $u_j \leq j$ 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 $u_j \leq j \leq k - 1 < k$)). In other words, the permutations $t_{1,u_1}, t_{2,u_2}, \ldots, t_{k-1,u_{k-1}}$ leave $k$ unchanged. Now,

\[
\overbrace{\sigma}^{=t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k,u_k}} (u_k) = (t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k,u_k}) (u_k)
\]

\[
= (t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k-1,u_{k-1}}) (t_{k,u_k} (u_k))
\]

\[
= (t_{1,u_1} \circ t_{2,u_2} \circ \cdots \circ t_{k-1,u_{k-1}}) (k) = k
\]

\[3^\text{Proof.}\] 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 $\tau \circ t_{k,g} = \sigma \circ t_{k,g} \circ t_{k,g} = \sigma$, so that

\[
\sigma = (t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{k,i_{k-1}}) \circ t_{k,g} = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{k,g}.
\]

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,

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

so that

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

$$
= t_{1, u_1} \circ t_{2, u_2} \circ \cdots \circ t_{k-1, u_{k-1}}.
$$

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 5(a).

(b) If $\tau \in S_n$ is any permutation, then $z(\tau)$ shall denote the number of cycles in the cycle decomposition of $\tau$. Thus, $m = z(\sigma)$ (since $m$ is the number of cycles in the cycle decomposition of $\sigma$). 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 $\tau$ looks as follows:

![Diagram]

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 $z(\tau \circ t_{p,q}) = z(\tau) - 1 = 5 - 1 = 4$. And we can indeed confirm this: The cycle decomposition of $\tau \circ t_{p,q} = \tau \circ t_{5,3}$ looks as follows:

![Diagram]

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 $\tau$; more precisely, all cycles of $\tau$ 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 $\tau$ 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 $\tau$, 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 $\tau$ has a cycle containing the element $p$ alone (since $\tau(p) = p$). Let $z_1$ be this cycle. Thus, $z_1 = \{p\}$. Hence, $z_1$ does not contain $q$ (since $q \neq p$).

Furthermore, let $z_2$ be the cycle in the cycle decomposition of $\tau$ that contains the element $q$. This cycle $z_2$ is distinct from $z_1$ (because $z_1$ does not contain $q$). Thus, $z_2$
does not contain \( p \) (since \( p \) is contained in the cycle \( z_1 \), which is distinct from \( z_2 \)). In other words, \( p \notin z_2 \).

Let us analyze what happens to the cycle decomposition of \( \tau \) when we compose \( \tau \) with \( t_{p,q} \) (thus obtaining \( \tau \circ t_{p,q} \)). The only values of \( \tau \) that change when we compose \( \tau \) 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 \( z_1 \) and \( z_2 \) in the cycle decomposition of \( \tau \) 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 \( z_1 \) and \( z_2 \). We claim that these two cycles are **merged into a single cycle** in \( \tau \circ t_{p,q} \).

Indeed, let us write the cycle \( z_2 \) in the form \( z_2 = \{ \tau^0 (q), \tau^1 (q), \ldots, \tau^{k-1} (q) \} \), where \( k \) is the smallest positive integer satisfying \( \tau^k (q) = q \). (Indeed, \( z_2 \) can be written in this form, since \( z_2 \) is the cycle of \( \tau \) that contains \( q \).) Thus,

\[
\begin{align*}
z_2 &= \{ \tau^0 (q), \tau^1 (q), \ldots, \tau^{k-1} (q) \} \\
&= \{ \tau^1 (q), \tau^2 (q), \ldots, \tau^k (q) \}
\end{align*}
\]

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

Let \( \gamma \) be the permutation \( \tau \circ t_{p,q} \in S_n \). Thus, each \( i \in [k-1] \) satisfies \( \gamma (\tau^i (q)) = \tau^{i+1} (q) \). In other words, the permutation \( \gamma \) 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 \( \gamma \). Let us denote this cycle by \( z' \). Thus, \( \tau^i (q) \in z' \) for each \( i \in [k] \).

Applying this to \( i = k \), we conclude that \( \tau^k (q) \in z' \). Thus, \( q = \tau^k (q) \in z' \).

The cycle \( z' \) contains all elements of \( z_2 \) (since \( z_2 = \{ \tau^1 (q), \tau^2 (q), \ldots, \tau^k (q) \} \)). In other words, the cycle \( z' \) contains all elements of \( z_2 \) (since \( z_2 = \{ \tau^1 (q), \tau^2 (q), \ldots, \tau^k (q) \} \)).

Also, \( \gamma (q) = (\tau \circ t_{p,q}) (q) = \tau \left( t_{p,q} (q) \right) = \tau (p) = p \). Hence, \( p \) lies on the same cycle in the cycle decomposition of \( \gamma \) as \( q \). In other words, \( p \) lies on the cycle in the cycle decomposition of \( \gamma \) that contains \( q \). Since the latter cycle is \( z' \) (because \( q \in z' \)), we thus conclude that \( p \) lies on \( z' \). In other words, \( p \in z' \). In other words, the cycle \( z' \) contains all elements of \( z_1 \) (since \( z_1 = \{ p \} \)).

The cycle \( z' \) in the cycle decomposition of \( \gamma \) thus contains all elements of \( z_1 \) and all elements of \( z_2 \). In view of \( \gamma = \tau \circ t_{p,q} \), this rewrites as follows: The cycle \( z' \) in the cycle decomposition of \( \tau \circ t_{p,q} \) contains all elements of \( z_1 \) and all elements of \( z_2 \). Furthermore, this cycle \( z' \) cannot contain any other elements (because if it did, then

\[\text{Proof.} \text{ Let } i \in [k-1]. \text{ Hence, } \tau^i (q) \neq q \text{ (since } k \text{ is the smallest positive integer satisfying } \tau^k (q) = q \). \text{ Also, } \tau^i (q) \neq p \text{ (since } \tau^i (q) \in \{ \tau^0 (q), \tau^1 (q), \ldots, \tau^{k-1} (q) \} = z_2 \text{ but } p \notin z_2 \). \text{ Thus, } \tau^i (q) \text{ equals neither } p \text{ nor } q. \text{ Hence, the transposition } t_{p,q} \text{ leaves } \tau^i (q) \text{ unchanged. In other words, } t_{p,q} (\tau^i (q)) = \tau^i (q). \]

Now,

\[
\gamma \left( \tau^i (q) \right) = (\tau \circ t_{p,q}) (\tau^i (q)) = \tau \left( t_{p,q} \left( \tau^i (q) \right) \right) = \tau (\tau^i (q)) = \tau^{i+1} (q), \text{ qed.}
\]
it would contain elements from cycles in the cycle decomposition of $\tau$ other than $z_1$ and $z_2$; but this would contradict the fact that all cycles other than $z_1$ and $z_2$ in the cycle decomposition of $\tau$ remain unchanged in the cycle decomposition of $\tau \circ t_{p,q}$.

Hence, this cycle $\mathcal{z}'$ contains all elements of $z_1$ and all elements of $z_2$ and no more elements. Thus, the cycles $z_1$ and $z_2$ are merged into a single cycle in $\tau \circ t_{p,q}$.

So we have seen that when we compose $\tau$ with $t_{p,q}$, the cycle decomposition does not change except for the fact that the two cycles $z_1$ and $z_2$ get merged into a single cycle. Thus, 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 $\tau$. In other words, $z(\tau \circ t_{p,q}) = z(\tau) - 1$. This proves Observation 2.

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

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

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

\textit{Induction base:} We have $$z(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{0,i_0}) = z(id) = n$$ (since the permutation id has $n$ cycles in its cycle decomposition). Comparing this with $$n - 0 + \left| \left\{ k \in [0] \mid i_k = k \right\} \right| = n - 0 + |\emptyset| = n,$$

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

\textit{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

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

We must prove that (10) holds for $p$.}
We have \( p \in [n] \) (since \( p \in \{0, 1, \ldots, n\} \) is positive). Also,

\[
\begin{align*}
\left\{ k \in [p] \mid i_k = k \right\} & = \{p\} \cup [p - 1] \quad \text{since } p \in \{0, 1, \ldots, n\} \text{ is positive.} \\
& = \{p\} \cup [p - 1] \quad \text{if } i_p = p; \\
& = \varnothing \quad \text{if } i_p \neq p
\end{align*}
\]

\[
\left\{ \begin{array}{ll}
\{p\}, & \text{if } i_p = p; \\
\varnothing, & \text{if } i_p \neq p
\end{array} \right. = \left\{ \begin{array}{ll}
\{p\}, & \text{if } i_p = p; \\
\varnothing, & \text{if } i_p \neq p
\end{array} \right.
\]

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, \( t_{p,i_p} = \text{id} \). Also, (12) becomes

\[
\left\{ \begin{array}{ll}
\{p\}, & \text{if } i_p = p; \\
\varnothing, & \text{if } i_p \neq p
\end{array} \right. = \left\{ \begin{array}{ll}
\{p\}, & \text{if } i_p = p; \\
\varnothing, & \text{if } i_p \neq p
\end{array} \right. \quad \text{(since } i_p = p) \]

so that

\[
|\{k \in [p] \mid i_k = k\}| = |\{p\} \cup [p - 1] \mid i_k = k\}| = |\{k \in [p - 1] \mid i_k = k\}| + 1
\]

(13)

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

Now,

\[
t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p,i_p} = (t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}) \circ t_{p,i_p} = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}.
\]

Hence,

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

\[
= n - p + |\{k \in [p - 1] \mid i_k = k\}| + 1
\]

\[
= |\{k \in [p] \mid i_k = k\}| \quad \text{(by (13))}
\]

\[
= n - p + |\{k \in [p] \mid i_k = k\}|.
\]
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

\[
\{k \in [p] \mid i_k = k\} = \begin{cases} 
\{p\}, & \text{if } i_p = p; \\
\emptyset, & \text{if } i_p \neq p
\end{cases} = \emptyset \quad \text{(since } i_p \neq p) \]

\[
= \{k \in [p - 1] \mid i_k = k\}. \quad (14)
\]

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

\[
z(\tau) = z\left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}\right) = n - (p - 1) + \left[\begin{array}{c} k \in [p - 1] \mid i_k = k \end{array}\right] = n - p + 1 + |\{k \in [p] \mid i_k = k\}|. \quad (15)
\]

But

\[
t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p,i_p} = \left(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}}\right) \circ t_{p,i_p} = \tau \circ t_{p,i_p}. \quad (16)
\]

We have $\tau(p) = p$ \footnote{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, $(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{p-1,i_{p-1}})(p) = p$. 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 $\tau(p) = p$.}

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

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

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.]
Now, apply (10) to $p = n$. The result is
\[
z(t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{n,i_n}) = n - n + \sum_{k=0}^{n} \left| \{k \in [n] \mid i_k = k\} \right| = \left| \{k \in [n] \mid i_k = k\} \right|.
\]
In view of $\sigma = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{n,i_n}$, this rewrites as $z(\sigma) = \left| \{k \in [n] \mid i_k = k\} \right|$. 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
\[
i_1 \geq i_2 \geq \cdots \geq i_k \quad \text{and} \quad i_1 + i_2 + \cdots + i_k = n.
\]

**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 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
\[
(3,3,3), \quad (2,2,2,1), \quad (2,2,2,1,1), \quad (1,1,1,1,1,1,1,1,1).
\]
Meanwhile, the partitions counted by $b$ in Exercise 7 are
\[
(9), \quad (6,3), \quad (5,4), \quad (3,3,3).
\]
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:

  [https://www.math.upenn.edu/~wilf/PIMS/PIMSlectures.pdf](https://www.math.upenn.edu/~wilf/PIMS/PIMSlectures.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


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/2018-10-03.