6.5. Dyck paths

**Def:** An up-down path is (informally) a path in $\mathbb{Z}^2$ that uses only the following two types of steps:

- "positive steps" (i.e., steps $(a, b) \rightarrow (a+1, b+1)$);
- "negative steps" (i.e., steps $(a, b) \rightarrow (a+1, b-1)$).

**Ex:**

A Dyck path is an up-down path that never falls below the $x$-axis (i.e., each point $(x, y)$ on the path satisfies $y \geq 0$).
Ex: The Dyck paths from \((0,0)\) to \((6,0)\) are

\[\text{There are } 5 = \binom{3}{2} \text{ of them.}\]
Prop. 6.8. Let \( n \in \mathbb{N} \). Then,
\[
\left( \text{# of Dyck paths from } (0,0) \text{ to } (2n,0) \right) = C_n.
\]

Proof. The map
\[
\{ \text{Dyck paths from } (0,0) \text{ to } (2n,0) \} \rightarrow \{ \text{legal paths from } (0,0) \text{ to } \{n,n\}\}
\]
which replaces each point \((x,y)\) on the Dyck path by
\[
\left( \frac{x+y}{2}, \frac{x-y}{2} \right)
\]
is a bijection. Thus, it follows from
\[
\left( \text{# of legal paths} \right) = C_n.
\]

\[
\square
\]

6.6, Super-Catalan numbers

Def. Let \( n,m \in \mathbb{N} \). Set
\[
T(m,n) = \frac{(2m)! \cdot (2n)!}{m! \cdot n! \cdot (m+n)!}.
\]

Thm. 6.9. (a) \( T(m,n) \) is a positive integer \( \forall m,n \in \mathbb{N} \), and is even when \( m+n > 0 \).

(b) \( T(m,n) = \binom{2m}{m} \binom{2n}{n} / \binom{m+n}{m} \) \( \forall m,n \in \mathbb{N} \).
(c) \( T(m, 0) = \binom{2^m}{m} \quad \forall m \in \mathbb{N}, \)

(d) \( T(m, 1) = 2 \cdot C_m \quad \forall m \in \mathbb{N}, \)

(e) \( 4 \cdot T(m, n) = T(m+1, n) + T(m, n+1) \quad \forall m, n \in \mathbb{N}, \)

(f) \( T(m, n) = T(n, m) \quad \forall m, n \in \mathbb{N}. \)

(g) \( T(m, n) = \sum_{k=-p}^{p} (-1)^k \binom{2m}{m+k} \binom{2n}{n-k}, \) \( \text{where} \quad p = \min \{m, n\}. \)

Proofs. See [lecture notes, Exercise 3.24] and/or google for "super-Catalan numbers". No one knows what \( T(m, n) \) counts.

7. Necklaces

7.1. \( \phi \) & \( \mu \)

Def. Let \( \mathcal{P} \) be the set \( \{1, 2, 3, \ldots, \mathcal{P} \}. \)

(as opposed to \( \mathbb{N} =\{0, 1, 2, 3, \ldots, \mathcal{N} \}. \)
Recall: Euler's totient function is the function \( \phi: \mathbb{P} \to \mathbb{N} \) sending each \( n \) to 
the \( \# \) of all \( m \in \mathbb{N} \) coprime to \( n \).

Prop. 7.1. Let \( n \in \mathbb{P} \). Let \( P_1, P_2, \ldots, P_k \) be the distinct prime divisors of \( n \). Then, \( \phi(n) = n \prod_{i \in \mathbb{P}^k} (1 - \frac{1}{P_i}) \).

Proof. This is Thm 2.30 with new notations.

Thm. 7.2. Let \( n \in \mathbb{P} \). Then, \( \sum_{d|n} \phi(d) = n \).

Here and in the following, 
"\( \sum \)" means "\( \sum_{d \in \mathbb{P}; \ d|n} \)".

Proof of Thm. 7.2. We have

\[
(63) \quad n = \sum_{i \in [n]} 1 = \sum_{d|n} \sum_{i \in [n]; \ \gcd(i,n)=d} 1
\]
(recall: \( \gcd(a, b) \) is the greatest common divisor of \( a \) and \( b \); it is divisible by each other divisor of \( a \) and \( b \)).

But fix a positive divisor \( d \) of \( n \).

Then, the map

\[
\{ i \in [n] \mid \gcd(i, n) = d \} \rightarrow \{ m \in \left[ \frac{n}{d} \right] \mid m \text{ is coprime to } \frac{n}{d} \},
\]

\[ i \mapsto i/d \]

is well-defined & bijective. Thus,

\[
\text{(\# of } i \in [n] \text{ such that } \gcd(i, n) = d) = \left( \text{(\# of } m \in \left[ \frac{n}{d} \right] \text{ such that } m \text{ is coprime to } \frac{n}{d} \right) = \phi \left( \frac{n}{d} \right) \quad \text{(by the definition of } \phi) .
\]

In other words,

\[
\sum_{\substack{i \in [n] \\ \gcd(i, n) = d}} 1 = \phi \left( \frac{n}{d} \right) .
\]
Summing up this equality over all positive divisors $d$ of $n$, we get
\[
\sum_{d \mid n} \sum_{i \in \mathbb{Z}_+ ; \gcd(i,n) = d} 1 = \sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)
\]
(here, we substituted $d$ for $n/d$, since the map \{positive divisors of $n$\} $\rightarrow$ \{positive divisors of $n^2$\},
\[d \rightarrow \frac{n}{d}\]
is bijective).

Thus, (63) becomes \( n = \sum_{d \mid n} \phi(d) \).

Remark. Alternative way to explain this proof:

Double-count the $n$ fractions $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}$.

After cancelling, their denominators will be divisors of $n$,
with each positive divisor $d$ occurring exactly $\phi(d)$ times.
Def. An \( n \in \mathbb{P} \) is said to be **squarefree** if

\[
\text{no } p \text{ square } > 1 \text{ divides } n. \\
\text{perfect square}
\]

In other words, \( n \) is squarefree if each prime appears at most once in its factorization.

For example, \( 15 \) is a squarefree (since \( 15 = 3 \times 5 \)) but \( 12 \) is not (since \( 2^2 | 12 \) or since \( 12 = 2^2 \times 3 \)).

Def. The (number-theoretical) **Möbius function** is the function \( \mu: \mathbb{P} \rightarrow \mathbb{Z} \) sending each \( n \) to

\[
\begin{cases} 
(-1)^{\text{(# of prime factors of } n)} & \text{if } n \text{ is squarefree} \\
0 & \text{otherwise}
\end{cases}
\]

**Ex:**

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mu(n) )</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>
Thm. 7.3. Let \( n \in \mathbb{P} \). Then, \( \sum_{d \mid n} \mu(d) = [n=1] \).

Proof. Let \( p_1, p_2, \ldots, p_k \) be the distinct prime factors of \( n \).

Then, \( n = 1 \) is equivalent to \( k = 0 \).

Thus, \( [n=1] = [k=0] \).

Now, the divisors of \( n \) all have the form \( p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \) with \( a_1, a_2, \ldots, a_k \geq 0 \). Among these, the squarefree divisors are the ones where \( a_1, a_2, \ldots, a_k \leq 1 \).

Thus, the squarefree divisors of \( n \) are precisely the numbers \( \prod_{i \in I} p_i \) for \( I \subseteq \{k\} \). More precisely, the map

\[
I \mapsto \prod_{i \in I} p_i
\]

is a bijection (by the Fundamental Theorem of Arithmetic).

Hence, \( \sum_{d \mid n, d \text{ squarefree}} \mu(d) = \sum_{I \subseteq \{k\}} \mu\left( \prod_{i \in I} p_i \right) \).
\[
\sum_{I \in \mathcal{K}} (-1)^{|I|} = \left[ \mathcal{K} = \emptyset \right] \quad (\text{by Thm. 2.24})
\]

\[
\left[ k = 0 \right] = \left[ n = 1 \right].
\]

Now,
\[
\sum_{d \mid n} \mu(d) = \sum_{d \mid n; \ d \text{ is squarefree}} \mu(d) + \sum_{d \mid n; \ d \not\text{ is squarefree}} \mu(d)
\]

\[
= \left[ n = 1 \right]
\]

\[
= \left[ n = 1 \right].
\]

---

**Thm. 7.4 (number-theoretical Möbius inversion I).**

Let \( (a_1, a_2, a_3, \ldots) \) and \( (b_1, b_2, b_3, \ldots) \) be two sequences of numbers. Assume that

\[
a_n = \sum_{d \mid n} b_d \quad \text{for all } n \in \mathbb{P}.
\]
Then, 

\[ b_n = \sum_{d \mid n} \mu \left( \frac{n}{d} \right) a_d \quad \text{for all } n \in \mathbb{P}. \]

(65)

**Ex:** In the situation of Thm. 7.4, we have

\[ b_8 = a_8 - a_4 \quad (\text{by (65) for } n = 8) \]

and

\[ b_{12} = a_{12} - a_6 - a_4 + a_2 \quad (\text{by (65) to } n = 12). \]

Check:

\[ a_8 - a_4 = (b_8 + b_4 + b_2 + b_1) - (b_4 + b_2 + b_1) = b_8; \]

\[ a_{12} - a_6 - a_4 + a_2 = b_{12} (b_{12} + b_6 + b_4 + b_3 + b_2 + b_1) \]

\[ - (b_6 + b_3 + b_2 + b_1) \]

\[ - (b_4 + b_2 + b_1) \]

\[ + (b_2 + b_1) \]

\[ = b_{12}. \]

**Proof of Thm. 7.4.** Fix \( n \in \mathbb{P}. \) Then,
\[
\sum_{d \mid n} \mu \left( \frac{n}{d} \right) a_d = \sum_{e \mid n} \mu \left( \frac{n}{e} \right) a_e = \sum_{e \mid n} \mu \left( \frac{n}{e} \right) \sum_{d \mid e} b_d \\
= \sum_{e \mid n} \sum_{d \mid e} \mu \left( \frac{n}{e} \right) b_d = \sum_{d \mid n} \sum_{e \mid \frac{n}{d}} \mu \left( \frac{n}{e} \right) b_d \\
= \sum_{f \mid \frac{n}{d}} \sum_{e \mid f} \mu \left( \frac{f}{e} \right)
\]

(here, we substituted \( f \) for \( \frac{n}{e} \), since the map \( \{ \text{divisors } e \text{ of } n \text{ that satisfy } d \mid f \} \) \( \rightarrow \) \( \{ \text{divisors of } \frac{n}{e} \} \), \( e \rightarrow \frac{n}{e} \) is a bijection)
\[ \sum \frac{\mu(f)}{\Delta} b_d \]

(by Thm. 7.3, applied to \( \frac{n}{d} \) instead of \( n \))

\[ \sum \left[ \frac{n}{d} = 1 \right] b_d = \sum [d = n] b_d = b_n, \quad \Box \]

Rmk. The converse also holds: \( (65) \Rightarrow (64) \).

Prop. 7.5. Let \( n \in \mathbb{P} \). Then, \( \sum \frac{n}{d} \mu(d) = \phi(\Omega(n)) \).

1st proof. Thm. 7.2 says \( n = \sum \phi(d) \), for all \( n \in \mathbb{P} \).

Thus, Thm. 7.4 (applied) to \( \alpha_i = i \) and \( b_i = \phi(i) \) yields
\[ \phi(n) = \sum_{d \ln} \mu\left(\frac{n}{d}\right) \frac{n}{d} = \sum_{d \ln} \mu(d) \frac{n}{d} \]

(here, we have substituted \( \frac{n}{d} \) for \( d \) in the sum, as before).

2nd proof (idea). Let \( p_1, p_2, \ldots, p_k \) be the distinct prime divisors of \( n \). Then, Prop. 7.4 yields

\[ \phi(n) = n \prod_{i \in \{p\}} \left(1 - \frac{1}{p_i}\right) \]

Prop. 2.25(b)

\[ = n \sum_{I \subseteq \{p\}} (-1)^{|I|} \prod_{i \in I} \frac{1}{p_i} \]

(by the same reasoning) (as in the proof of Thm. 7.3)

\[ = n \sum_{d \text{ is squarefree}} \mu(d) \frac{1}{d} \]

(since \( \mu(d) = 0 \)) (since \( \mu(d) = 0 \))

\[ = n \sum_{d \ln} \mu(d) \frac{1}{d} \]

(when \( d \) is not squarefree)
\[ = \sum_{d \mid n} \mu(d) \frac{n}{d}. \]

See number theory texts for more about \( \phi, \mu \) and similar functions (e.g. [Niven/Zuckerman/Montgomery]).

7.2. A simple lemma

Prop. 7.6. Let \( X \) be a set, let \( \sigma \) be a permutation of \( X \).

Let \( n \) be a positive integer such that \( \sigma^n = \text{id} \).

Then, \( \sigma \) has a disjoint union the size of any cycle of \( \sigma \) divides \( n \).

Proof. Let \( C \) be a cycle of \( \sigma \). We must show \( |C| \mid n \).

Let \( \sigma \in C \). Let \( k \) be the smallest positive integer such that \( \sigma^k(x) = x \).

Now, if \( p \in N \) is arbitrary, then

\[ g^p(x) = g^{p \cdot k}(x), \] (66)
where \( p \% k \) means "remainder of \( p \) modulo \( k \)."

(Proof of (66): Induction on \( p \), using \( g^k(x) = \text{id} \).)

Also, \( g^0(x), g^1(x), \ldots, g^{k-1}(x) \) are distinct, since otherwise there would be \( 0 \leq a < b < k \) such that \( g^a(x) = g^b(x) \) \( \Rightarrow x = g^{b-a}(x) \), which would contradict the minimality of \( k \).

Thus, \( C = \{ g^0(x), g^1(x), \ldots, g^{k-1}(x) \} \) \( \text{for distinct elements} \) \( k \) elements \( \text{distinct elements} \), so that \( |C| = k \).

Now, (66) yields \( g^n(x) = g \% k \), \( g^n(x) = g^n(x) = x = g^0(x) \)

\( \Rightarrow \) \( n \% k = 0 \) (since \( g^0(x), g^1(x), \ldots, g^{k-1}(x) \) are distinct)

\( \Rightarrow \) \( k \mid n \Rightarrow \# |C| = k \mid n. \) \( \Box \)
(We have used Prop. 7.6 already when we were discussing shift-equivalence.)

7.3. Necklaces

Idea:

Consider rotated versions to be identical.

but reflected versions are not (unless you can also set them by rotation).
Def: Let $Q$ be a set, let $n$ be a positive integer.

(2) The map
$$g : Q^n \to Q^n,$$
$$(q_1, q_2, \cdots, q_n) \mapsto (q_2, q_3, \cdots, q_n, q_1)$$

is called rotation.

This $g$ is a permutation of $Q^n$, and satisfies $g^n = id$.

(b) The cycles of $g$ are called necklaces with $n$ beads and colors from $Q$.

(idea: the necklace containing $(q_1, q_2, \cdots, q_n)$ is
if \((g_1, g_2, \ldots, g_n) \in \mathbb{Q}^n\), then \([(g_1, g_2, \ldots, g_n)]\) shall mean the necklace (= cycle of \(p\)) that contains it.

(c) The set of all necklaces with \(n\) beads and colors from \(\mathbb{Q}\), denoted by \(\mathbb{Q}^n_{\text{neck}}\).

(d) The cardinality of a necklace (i.e., the number of \(n\)-tuples \(\vec{g} \in \mathbb{Q}^n\) that belong to the necklace) is called its \underline{period}.

[Ex: The necklace \([(2, 1, 1, 2, 1, 1)]\) is equal to \(\{(2,1,1,2,1,1), (1,1,2,1,1,2), (1,2,1,1,2,1)\}\) and has period 3.]
(e) The set of all necklaces with \( n \) beads and colors from \( Q \) having period \( k \) is denoted by \( Q^n_{\text{neck},k} \).

**Question:** How many necklaces are there in \( Q^n_{\text{neck}} \), when \( n \) and \( |Q| \) are given?

**Cor. 7.7:** The period of any necklace in \( Q^n_{\text{neck}} \) is a positive divisor of \( n \).

**Proof.** It is the size of a cycle of \( p \), thus divides \( n \) (by Prop. 7.6).

**Lem. 7.8.** Let \( Q^n \) and \( n \) be as before, let \( k \) be a positive divisor of \( n \). Then,

\[
|Q^n_{\text{neck},k}| = |Q^k_{\text{neck},k}|.
\]
Thm. 7.9. Let $Q$ and $n$ be as before. Let $q = |Q|$. 

(a) we have $|Q_{\text{neck}}, n| = \frac{1}{n} \sum \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum \mu(d) q^{n/d}$.

(b) we have $|Q_{\text{neck}}| = \frac{1}{n} \sum \phi\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum \phi(d) q^{n/d}$.

(c) Let $Q = [q]$, and let $a_1, a_2, \ldots, q \in \mathbb{N}$. Then,

(\# of \# of necklaces with $n$ beads and colors \# from $Q$, where color $i$ appears $a_i$ many times \forall $i$)

\[
= \frac{1}{n} \sum \phi\left(\frac{n}{d}\right) \left( \frac{d}{a_1 \frac{d}{n}, a_2 \frac{d}{n}, \ldots, a_q \frac{d}{n}} \right).
\]

This is understood to be $0$ unless all the $a_i \frac{d}{n} \in \mathbb{N}$ and $\sum a_i = \frac{n}{d}$.