MATH 188: Homework #7

Due on Jun 14, 2024 at 23:59pm

Professor Kunnawalkam Elayavalli

Ray Tsai

A16848188

Problem 1

Do the case of general n of Example 7.11, i.e., give a formula for the number of necklaces (considered equivalent up to reflection) of length n using an alphabet of size k.

Proof. Note that D_n consists of n rotations and n reflections. By Example 7.10, each rotations of order i has $\gcd(n, i)$ cycles. Note that each reflection is of order 2. When n is odd, each reflection fixes only 1 point, and thus each reflection consists of one 1-cycle and $\frac{n-1}{2}$ 2-cycles. On the other hand, for even n, half of the reflections fixes 2 points and the other half fixes no point. That is, when n is even, there are $\frac{n}{2}$ reflections with $\frac{n-2}{2} + 2 = \frac{n}{2} + 1$ cycles and $\frac{n}{2}$ reflections with $\frac{n}{2}$ cycles. In total, there are

It now follows from Theorem 7.9 that there are

$$\begin{cases} \frac{1}{2n}\sum_{i=1}^{n} k^{\gcd(n,i)} + \frac{1}{2}\left(k^{\frac{n+1}{2}}\right) & n \text{ is odd} \\ \frac{1}{2n}\sum_{i=1}^{n} k^{\gcd(n,i)} + \frac{1}{4}\left(k^{\frac{n}{2}+1} + k^{\frac{n}{2}}\right) & n \text{ is even} \end{cases}$$

necklaces. □

Problem 2

Consider assigning one of k colors to each of the entries of a 3×3 matrix.

(a) How many ways are there to do this if we consider two colorings the same if they differ by rotation? To be explicit, one rotation clockwise means:

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \mapsto \begin{bmatrix} g & d & a \\ h & e & b \\ i & f & c \end{bmatrix}$$

Proof. Note that we may interpret the outer 8 elements of a 3×3 matrix in clockwise order as a word of length 8, up to "even" cyclic shift. In particular, let $G = 2\mathbb{Z}/8$ be the group of even integers mod 8, let $X = \mathbb{Z}/8$ be the set of 8 outer positions, and let Y be the set of colors. Then a function $X \to Y$ is a word of length 8, and a G-orbit represents a word up to "even" cyclic shift. So the words up to "even" cyclic shift are in bijection with G-orbits of Y^X. Each element of G gives a permutation of some even power of $(01 \cdots 7)^g$. Specifically, the permutations are

$$(0246)(1357), (04)(15)(26)(37), (0642)(1753), (0)(1)(2)(3)(4)(5)(6)(7). \tag{1}$$

It now follows from Theorem 7.9 that the number of orderings of the outer 8 elements of a 3×3, up to rotation, is $\frac{1}{4}(k^8 + k^4 + 2k^2)$. In addition to the 8 outer elements, we also have to determine the center element of the 3×3 matrix. Note that the choice of the center element is independent of the choice of the outer 8 elements. Hence, there are

$$\frac{1}{4}(k^9 + k^5 + 2k^3)$$

ways to color the 9 entries, up to rotations. $\square$

(b) How many colorings (up to rotation) are there that use exactly 3 different colors from the k, each used to color 3 entries?

Proof. We again interpret the outer 8 elements of a 3×3 matrix in clockwise order as a word of length 8, up to "even" cyclic shift, and continue using G, X, Y defined in (a). We need to use exactly 3 different colors, each used to color 3 entries. Let $W \subset Y^X$ be the set of a word of length 8 with exactly 3 colors, 3 entries being the first color, 3 being the second color, and the rest 2 entries be the last color. Since there are $\binom{k}{3}$ ways to pick 3 colors from Y, 3 way to pick the color which only appears twice in the word, and $\frac{8!}{3!3!2!}$ ways to arrange the colors, we have $|W| = 3\binom{k}{3}\frac{8!}{3!3!2!} = 1680\binom{k}{3}$. Notice in (1) that the trivial permutation $I = (0)(1)(2)(3)(4)(5)(6)(7)$ is the only permutations given by G whose cycles all have lengths that divide 3. That is, I is the only permutation which fixes any word $w \in W$. It now follows by the Burnside Lemma that the number of ways to color the outer 8 elements given our rule is

$$|W/G| = \frac{1}{|G|}\sum_{g \in G} |W^g| = \frac{1}{|G|}|W^I| = \frac{1}{|G|}|W| = \frac{1680\binom{k}{3}}{4} = 420\binom{k}{3}.$$

But then according to our rule, the center entry of the matrix is determined by the outer 8 entries, so this is also the total number of ways to color the whole matrix with our rule, up to rotation. $\square$

Problem 3

In Theorem 7.9, take $X = [n]$, $Y = [d]$, and $G = \mathfrak{S}_n$ with the natural action on X.

(a) Find a bijection between G-orbits on Y^X and weak compositions; give a closed formula for their number using this interpretation.

Proof. Note that the each G-orbit on Y^X represents a word up to the ordering of the characters. Let O be a G-orbit. Suppose that a word in O consists of a_i number of i's, for each $i \in [d]$. Note that $a_1 + \cdots + a_d = n$ and $0 \leq a_i \leq n$ for all i, which makes $(a_1, \ldots, a_d)$ a weak compositions of n with d parts. Since each word in O contains the same number of each i, it is well-defined to map O to the weak composition $(a_1, \ldots, a_d)$.

On the other hand, given $(a_1, \ldots, a_d)$ a weak compositions of n with d parts, we may map it to a G-orbit O such that each word $w \in O$ contains a_i number of $i's$, for all $i \in [d]$. This mapping is well-defined because words which contain the same number of each characters are in the same orbit, and hence the bijection.

It now follows that
$$|[d]^{[n]}/\mathfrak{S}_n| = \binom{n+d-1}{n}.$$
□

(b) By varying d, explain how the equality between the expression in Theorem 7.9 and your answer to (a) gives a new proof for Corollary 3.30.

Proof. Given a perumtation σ, let $c(\sigma)$ denote the number of cycles in σ. By Theorem 7.9 and (a),
$$\binom{n+d-1}{n} = |[d]^{[n]}/\mathfrak{S}_n| = \frac{1}{n!}\sum_{\sigma \in \mathfrak{S}_n} d^{c(\sigma)} = \frac{1}{n!}\sum_{k=1}^{n} c(n,k) d^k.$$

It now follows that
$$\frac{(n+d-1)!}{(d-1)!} = \sum_{k=0}^{n} c(n,k) d^k.$$
□

Problem 4

Let p be a prime and $n \geq p$. Use the method of §7.4 for the following:

(a) Show that
$$S(n,k) \equiv S(n-p, k-p) + S(n-p+1, k) \pmod{p}.$$

Proof. Let X be the set of partitions of $[n]$ into k blocks. Let σ be the permutation which is the p-cycle $(12\cdots p)$. Given a set $S = \{s_1, \ldots, s_m\} \subseteq [n]$, define $g \in \mathfrak{S}_n$ such that $g(S) = \{\sigma(s_1), \ldots, \sigma(s_m)\}$. Hence, given partition $P = \{B_1, \ldots, B_k\} \in X$, we may also define $g(P)$ to be $\{\sigma(B_1), \ldots, \sigma(B_k)\}$. Note that g generates a cyclic group of order p.

Now consider X^g. Suppose $P \in X^g$. Then, $P = g(P)$. That is, $\sigma : P \to P$ is also a permutation of P. But then note that $\sigma^p(B_j) = B_j$ for all j, so the lengths of cycles of σ as a permutation of P divide p, which can either be 1 or p.

Suppose that σ acts as a trivial permutation on P. Consider some $B_j \in P$ which contains 1. Since $\sigma(B_j) = B_j$, we know $2 = \sigma(1) \in B_j$. It now follows from induction that $\{1, \ldots, p\} \subseteq B_j$, and there are $S(n-p+1, k)$ such partitions in X.

On the other hand, suppose σ contains a p cycle when acting on P. Since $\sigma(B_j) = B_j$ if $B_j \cap \{1, \ldots, p\} = \emptyset$, we know every block B_l in the p cycle contains some $i \in \{1, \ldots, p\}$, and thus each B_l in the p cycle contains exactly one element in $\{1, \ldots, p\}$. Observe that if B_l contains an element not in $\{1, \ldots, p\}$, then $\sigma(B_l)$ is different from any block in the p cycle. Hence, each $B_l = \{i\}$, for some $1 \leq i \leq p$, and there are $S(n-p, k-p)$ such partitions in X.

It now follows that $|X^g| = S(n-p, k-p) + S(n-p+1, k)$ and Lemma 7.15 that
$$S(n,k) \equiv S(n-p, k-p) + S(n-p+1, k) \pmod{p}.$$

□

(b) Show that
$$c(n,k) \equiv c(n-p, k-p) - c(n-p, k-1) \pmod{p}.$$

Proof. Let X be the set of permutations in $\mathfrak{S}_n$ with exactly k different cycles, and we let $\mathfrak{S}_n$ act on X by conjugation. Let $\sigma \in X$. Let $g = (12\cdots p) \in \mathfrak{S}_n$. Note that g generates a cyclic group of order p.

Now consider X^g. Suppose $\sigma \in X$. Since $g \cdot \sigma = g\sigma g^{-1} = \sigma$, we have $g = \sigma g \sigma^{-1}$, and thus $(12\cdots p) = (\sigma(1)\sigma(2)\cdots\sigma(p))$. Hence, σ cyclic shifts each element in $\mathbb{Z}/p$ by some constant $r \in \mathbb{Z}/p$.

If $r = 0$, then σ consists of trivial cycles $(1)(2)\cdots(p)$ and $k-p$ cycles using the remaining $n-p$ elements. Hence, there are $c(n-p, k-p)$ such σ in this case.

On the other hand, if $1 \leq r \leq p-1$, then σ consists of a cycle $(1+r,\ 2+r,\ \cdots\ p+r)$ and $k-1$ cycles using the remaining $n-p$ elements. Since there are $p-1$ choices for r, there are $(p-1)c(n-p, k-1)$ such σ in this case.

Hence, we have $|X^g| = c(n-p, k-p) + (p-1)c(n-p, k-1)$. It now follows from Lemma 7.15 that
$$c(n,k) \equiv c(n-p, k-p) - c(n-p, k-1) \pmod{p}.$$

□