ALGEBRA I. PROBLEM SET 4.

THE CYCLIC GROUP $\mathbb{Z}/N\mathbb{Z}$ AND THE SYMMETRIC GROUP S_N.

DUE TUE, OCT 9.

In this handout we look at some number theory and counting related to the cyclic and symmetric groups. Hand in 4 questions to be graded by Oct 9 with at most two questions from **#1, #2, #3, #4**.

1. **Cyclic groups**

Let Z_n be the cyclic group of order $n \in \mathbb{Z}_{\geqslant 1}$, defined as

$$Z_n := \langle x \mid x^n = 1 \rangle.$$

Review §0.3 in Dummit and Foote where $\mathbb{Z}/n\mathbb{Z}$ is defined, and §1.3 on cyclic groups. We have $\mathbb{Z}/n\mathbb{Z} \cong Z_n$. Define the Euler ϕ function as

$$\phi(n) := |\{a \in \mathbb{Z} \mid 1 \leqslant a \leqslant n,\ (a,n) = 1\}|,$$

the number of positive integers up to n that are prime to n. In Z_n, the number of elements of order d, for $d \mid n$, is $\phi(d)$. (This may be shown by first proving that $Z_n = \langle x \rangle$ implies $|x^a| = n/(a,n)$.) Summing over all possibilities gives

$$\sum_{d|n} \phi(d) = n.$$

The following subset of $\mathbb{Z}/n\mathbb{Z}$ forms a group under multiplication:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1\}.$$

Clearly $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$.

#1 [Q16, §3.2.] Use Lagrange's Theorem in $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove

Fermat's Little Theorem: $\quad a^p \equiv a \bmod p \qquad (a \in \mathbb{Z},\ p \text{ prime}).$

#2 [Q17, §3.2.] For p prime and $n \in \mathbb{Z}_{\geqslant 1}$, find the order of $\overline{p}$ in $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$. Deduce that

$$n \mid \phi(p^n - 1).$$

#3 [Q22, §3.2.] Use Lagrange's Theorem in $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove

Euler's Theorem: $\quad a^{\phi(n)} \equiv 1 \bmod n \qquad (a \in \mathbb{Z},\ (a,n) = 1).$

#4 [Q23, §3.2.] Find the last two digits of $3^{3^{100}}$.

#5 Show that $\mathbb{Z}/n\mathbb{Z}$ forms a field under the operations of addition and multiplication mod n if and only if n is prime.

For p prime the finite field $\mathbb{Z}/p\mathbb{Z}$ is usually denoted $\mathbb{F}_p$. For any field F, the non-zero elements must form a group under multiplication. This group is denoted $F^\times$. We will see later that $F^\times$ is always cyclic. Hence

$$(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \qquad (p \text{ prime}).$$

Date: Oct 2, 2012.

It is shown in §4.4 that there is an isomorphism

$$\psi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n)$$
$$\psi(\overline{a}) = (x \mapsto x^a).$$

2. Symmetric groups

Review §1.3 on the symmetric group S_n and §4.3 which includes a part on conjugacy in S_n. As seen there, if $\sigma, \tau \in S_n$ with $\sigma = (a_1\ a_2\ \ldots a_m)$ then

$$\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \ldots \tau(a_m))$$

and similarly if σ is a disjoint product of cycles. It follows that two permutations in S_n are conjugate if and only if they have the same number of cycles of each length in their disjoint cycle decomposition.

A non-increasing sequence of positive integers that sum to n is called a *partition* of n. The number of partitions of n is given by the partition function $p(n)$. For example $p(4) = 5$ since 4 has the five partitions

$$4,\ 3+1,\ 2+2,\ 2+1+1,\ 1+1+1+1.$$

It follows from the above reasoning that

$$p(n) = \text{ the number of conjugacy classes in } S_n.$$

In §5.2 we saw that partitions also arise in connection with the invariant factors of Sylow p-subgroups of abelian groups:

$$p(n) = \text{ the number of isomorphism classes of an abelian group of order } p^n.$$

Note that the number of partitions of a set of size n (i.e. ways to write the set as a disjoint union of non-empty subsets) is larger than $p(n)$. For example there are 15 possible partitions of $\{a,b,c,d\}$:

$$\{\{a,b,c,d\}\},\ \{\{a,b,c\}\{d\}\},\ \{\{a,b,d\}\{c\}\},\ \{\{a,c,d\}\{b\}\},\ \{\{b,c,d\}\{a\}\},$$
$$\cdots, \{\{a,b\},\{c,d\}\},\ \{\{a,c\},\{b,d\}\},\ \{\{a,d\},\{b,c\}\},\ \{\{a\},\{b\},\{c\},\{d\}\}.$$

We may think of $p(n)$ as the number of partitions of a set containing n indistinguishable elements (i.e. a multiset).

#6 Let σ be an m-cycle in S_n. Show that the size of the conjugacy class of σ in S_n is

$$(m-1)!\binom{n}{m}.$$

#7 [Q35, §4.3.] Let p be a prime. Find a formula for the number of conjugacy classes of elements of order p in S_n using the greatest integer function.

#8 Show that S_p has $(p-2)!$ Sylow p-subgroups for p prime. Use this to prove

Wilson's Theorem: $(p-1)! \equiv -1 \bmod p$ (p prime).

#9 Show that the number of partitions of n, if we care about the order of the summands, is 2^{n-1} (so for example $n = 4$ has 8 of these:

$$4,\ 3+1,\ 1+3,\ 2+2,\ 2+1+1,\ 1+2+1,\ 1+1+2,\ 1+1+1+1).$$

Deduce that $p(n) \leqslant 2^{n-1}$.

Hardy and Ramanujan found close approximations to $p(n)$ in 1918. Their results imply the asymptotic relation

$$p(n) \sim \frac{1}{4\sqrt{3}} e^{\frac{2\pi}{\sqrt{6}}\sqrt{n}} \qquad (n \to \infty).$$

Rademacher, building on their work, found a remarkable exact formula for $p(n)$ in 1937.

3. More counting: Stirling numbers

For $n,k\in\mathbb{Z}_{\geqslant 0}$ define the *Stirling subset number*[1] $\left\{ n \atop k \right\}$ as follows

$$\left\{ n \atop k \right\} = \text{ the number of ways to partition a set of size } n \text{ into } k \text{ non-empty subsets.}$$

The total number of ways to partition a set of size n is given by the Bell number:

$$\sum_{k=0}^{n} \left\{ n \atop k \right\} = \mathrm{Bell}(n)$$

and, as we already saw, $\mathrm{Bell}(4) = 15$. The Stirling subset numbers satisfy a relation similar to Pascal's rule for binomial coefficients:

$$\left\{ n \atop k-1 \right\} + k\left\{ n \atop k \right\} = \left\{ n+1 \atop k \right\}, \qquad (n,k\in\mathbb{Z}) \tag{3.1}$$

$$\left\{ n \atop 0 \right\} = \left\{ 0 \atop n \right\} = 0, \qquad \left\{ 0 \atop 0 \right\} = 1, \qquad (n\in\mathbb{Z}_{\neq 0}). \tag{3.2}$$

The *Stirling cycle number*[2] $\left[n \atop k \right]$ is defined as

$$\left[n \atop k \right] = \text{ the number of permutations in } S_n \text{ that have } k \text{ disjoint cycles.}$$

Clearly

$$\sum_{k=0}^{n} \left[n \atop k \right] = n!$$

and similarly to (3.1), (3.2) we have

$$\left[n \atop k-1 \right] + n\left[n \atop k \right] = \left[n+1 \atop k \right], \qquad (n,k\in\mathbb{Z}) \tag{3.3}$$

$$\left[n \atop 0 \right] = \left[0 \atop n \right] = 0, \qquad \left[0 \atop 0 \right] = 1, \qquad (n\in\mathbb{Z}_{\neq 0}). \tag{3.4}$$

Using (3.1)-(3.4) forwards and backwards determines $\left\{ n \atop k \right\}$, $\left[n \atop k \right]$ uniquely for all $n,k\in\mathbb{Z}$.

#10 Use the recursions (3.1)-(3.4) to show that both types of Stirling numbers are really two sides of the same coin:

$$\left[n \atop k \right] = \left\{ -k \atop -n \right\}, \qquad (n,k\in\mathbb{Z}).$$

The Stirling numbers satisfy many relations. For example, with $n\in\mathbb{Z}_{\geqslant 0}$, we have the polynomial identities

$$\sum_{k=0}^{n} \left\{ n \atop k \right\} x(x-1)\cdots(x-k+1) = x^n,$$

$$x(x+1)\cdots(x+n-1) = \sum_{k=0}^{n} \left[n \atop k \right] x^k.$$

[1] We are using Knuth's names and notation. In the literature they are often called Stirling numbers of the second kind, even though they were discovered first.

[2] Or Stirling number of the first kind