MATH 301 · FALL 2026

Problem Set 99: p-Fixed Point Congruence and Sylow's Theorems

DUE never, optional Problem Set!

I want to be with those who know secret things or else alone.

Rainer Maria Rilke

This is an **optional problem set** exploring more topics related to group actions. We cover the elegant p-fixed point congruence and several of its important applications, including the Sylow theorems. If you are planning to pursue graduate studies in mathematics, you should do all these problems.

Suppose that G is a group acting on a set X. If $g \in G$, then we say $x \in X$ is a **fixed point** of g if $g(x) = x$. We let X^g denote the set of all fixed points of g,

$$X^g := \{x \in X : g(x) = x\} \subseteq X.$$

More generally, if $H \subseteq G$ is a subgroup, then we say $x \in X$ is a **fixed point** of H if $h(x) = x$ for all $h \in H$. That is, x is a fixed point of every element of H. We write X^H for the set of all H-fixed points,

$$X^H := \{x \in X : h(x) = x \text{ for all } h \in H\} \subseteq X.$$

Note that $X^g = X^{\langle g \rangle}$.

99.1 · Fixed Point Congruence

In the previous problem set you (implicitly) proved the following important theorem in Problem 3.5.

THEOREM 99.1 (Orbit-Stabilizer Theorem)
Let G be a finite group acting on a set X. Then for every $x \in X$ we have

$$|G| = |Gx||G_x|.$$

One important consequence of the Orbit-Stabilizer Theorem is that the size of any G-orbit must divide the order of the group G. When the order of G is a power of a prime p, this has a simple but powerful corollary: the **p-fixed point congruence**.

Before stating this result, some notation and terminology: If p is a prime, then we say a finite group G is a **p-group** if the order of G is a power of p. Recall that if $a, b, n \in \mathbb{Z}$ are integers, then we say a is **congruent** to b **modulo** n if $a - b$ is a multiple of n; in that case, we write

$$a \equiv b \bmod n.$$

PROBLEM 99.1

Prove the p-Fixed Point Congruence Theorem.

THEOREM 99.2 (p-Fixed Point Congruence)
Let G be a p-group for some prime p. If X is a finite set on which G acts, then

$$|X| \equiv |X^G| \bmod p.$$

As a first consequence of this theorem we deduce a partial converse to Lagrange's Theorem. Recall that Lagrange's Theorem says that the order of any subgroup, and in particular the order of any element, must divide the order of G. It is not generally true that for every divisor d of the order of G that there exists a subgroup of order d. However, this is the case for each *prime* divisor of the order of G.

PROBLEM 99.2

Let G be a finite group and let p be a prime dividing $|G|$. Let $\sigma = (123\cdots p) \in S_p$ be a p-cycle in the pth symmetric group. Note that $C_p = \langle\sigma\rangle$ acts naturally on p-tuples G^p by cyclically permuting coordinates.

$$\sigma(g_1, g_2, \ldots, g_p) := (g_2, g_3, \ldots, g_p, g_1).$$

1. Let $X \subseteq G^p$ be the set of all p-tuples whose coordinates multiply to 1 in G,

   $$X = \{(g_1, g_2, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = 1\}.$$

   Prove that $\sigma(X) = X$, hence X is a C_p-set.

2. Prove that the number of elements in X is $|X| = |G|^{p-1}$.

3. Prove that σ must have at least 2 fixed points in X.

4. Prove that G contains an element with order p.

   The theorem we just proved is due to Cauchy.

   THEOREM 99.3 (Cauchy's Theorem)
   If G is a finite group and p is a prime dividing the order of G, then G has an element of order p.

5. Let's prove a corollary. Let p be a prime and suppose that G is a non-trivial finite group such that every nontrivial element has p-power order. Prove that G is a p-group.

PROBLEM 99.3

If G is a group, then the **center** of G, denoted $Z(G)$ is defined by

$$Z(G) = \{h \in G : ghg^{-1} = h \text{ for all } g \in G\}.$$

The center is the subgroup of G comprised of all elements which commute with every element of G. The following result may be proved using the p-fixed point congruence.

1. If G is a p-group, prove that $Z(G)$ is a nontrivial subgroup. **Hint:** It all comes down to choosing the right action.

2. (Challenge) Let p be a prime. Prove that any group of order p^2 is isomorphic to C_{p^2} or $C_p \times C_p$.

99.2 · Lucas's Theorem

We can use the p-fixed point congruence to prove interesting congruences about binomial coefficients. Recall that given natural numbers m, n we let $\binom{m}{n}$ denote the number of ways to choose n distinct elements from a set of m elements. Or equivalently, if X is a set of m elements, then $\binom{m}{n}$ is the number of n-element subsets of X. The formula for $\binom{m}{n}$ is

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

PROBLEM 99.4

Let p be a prime. Let $\sigma = (12\cdots p) \in S_p$ be a p-cycle.

1. Let $0 < k < p$. Let $X_p := \{1, 2, \ldots, p\}$ and let $\binom{X_p}{k}$ denote the set of all k element subsets of X_p. Note that $C_p := \langle\sigma\rangle$ acts naturally on $\binom{X_p}{k}$. Use the p-fixed point congruence to prove that $\binom{p}{k}$ is a multiple of p. This can be done directly from the formula for $\binom{p}{k}$, but there is a richer proof using the p-fixed point congruence and I'd like you to find it.

2. Let m be a natural number coprime to p. Prove that $\binom{mp^n}{p^n}$ is not a multiple of p for any $n \geq 0$. **Hint:** Consider the group $G \subseteq S_{mp^n}$ generated by the disjoint p^n cycles

$$\begin{aligned}
\sigma_1 &= (12\cdots p^n),\\
\sigma_2 &= ((p^n+1)(p^n+2)\cdots(2p^n)),\\
&\vdots\\
\sigma_m &= (((m-1)p^n+1)((m-1)p^n+2)\cdots(mp^n)).
\end{aligned}$$

   Since each of the σ_i commute, each element $g \in G$ may be expressed as

$$g = \sigma_1^{a_1}\sigma_2^{a_2}\cdots\sigma_m^{a_m}$$

   for some integers a_i.

3. (Challenge) Suppose that m, n are natural numbers with base-p expansions

$$\begin{aligned}
m &= a_d p^d + a_{d-1}p^{d-1} + \ldots + a_1 p + a_0\\
n &= b_d p^d + b_{d-1}p^{d-1} + \ldots + b_1 p + b_0.
\end{aligned}$$

Note that this means each of the digits satisfy $0 \le a_i, b_i < p$ for all i. Prove that

$$\binom{m}{n} \equiv \binom{a_d}{b_d}\binom{a_{d-1}}{b_{d-1}} \cdots \binom{a_1}{b_1}\binom{a_0}{b_0} \bmod p.$$

This result is known as **Lucas's Theorem**; it is one of my favorites.

99.3 · Sylow's Theorems

The Sylow Theorems are a collection of three related results on the p-subgroups of a finite group G. These results are all consequences of the p-fixed point congruence. The first result may be viewed as a strengthening of Cauchy's theorem.

PROBLEM 99.5

We will prove the following theorem.

THEOREM 99.4 (First Sylow Theorem)
Let G be a finite group. Suppose p is a prime such that $|G| = mp^n$ where $n \ge 1$ and m is coprime to p. Then G contains a subgroup H of order p^n.

1. Let $k \ge 0$ and define $\binom{G}{k}$ to be the set of all k-element subsets of G. Note that G acts naturally on $\binom{G}{k}$ by left-multiplication. Prove that $\binom{G}{p^n}$ contains an element Y such that p does not divide the size of the orbit GY.

2. Let Y be the subset from the previous part. Prove that the stabilizer G_Y has order p^n.

If p^n is the largest power of p dividing $|G|$, then a subgroup $H \subseteq G$ with order p^n is called a **p-Sylow subgroup**. Hence Theorem 99.4 says that G contains a p-Sylow subgroup for every prime p dividing $|G|$. These subgroups are named after the Norwegian mathematician Peter Ludvig Sylow who first proved their existence in 1872.

PROBLEM 99.6

Let G be a finite group. Suppose p is a prime such that $|G| = mp^n$ where $n \ge 1$ and m is coprime to p.

1. Prove Sylow's second theorem.

THEOREM 99.5 (Second Sylow Theorem)
If H is a Sylow subgroup of G and K is any p-subgroup of G, then there exists a $g \in G$ such that $gKg^{-1} \subseteq H$. In particular, any two p-Sylow subgroups in G are conjugate.

Hint: Consider the natural action of K on G/H.

2. If $H \subseteq G$ is a subgroup, the **normalizer** $N_G(H) \subseteq G$ of H is the subgroup of all elements $g \in G$ such that $gHg^{-1} = H$. Note that $N_G(H)$ is the largest subgroup of G for which H is a normal subgroup of $N_G(H)$. Prove Sylow's third theorem.

THEOREM 99.6
If $H \subseteq G$ is a p-Sylow subgroup and m_p is the number of p-Sylow subgroups in G, then

(a) $m_p = [G : N_G(H)]$,

(b) $m_p \equiv 1 \bmod p$,

(c) m_p divides m.

99.4 · Applications of Sylow

Together these three theorems form a powerful tool for analyzing and classifying finite groups. Here is one example of how to use the Sylow theorems.

PROBLEM 99.7

Let $p < q$ be primes and suppose that $q \not\equiv 1 \bmod p$. We will prove that any group G of order pq must be cyclic.

1. Prove that G contains elements $g, h \in G$ with $\operatorname{ord}(g) = p$ and $\operatorname{ord}(h) = q$ such that $hgh^{-1} = g^k$ for some integer k.
2. Prove that $k^q \equiv 1 \bmod p$ and use this to argue that $gh = hg$.
3. Prove that $G = \langle gh \rangle$.
4. Classify all groups of order 15.

PROBLEM 99.8

In this problem we practice using Sylow's Theorems.

1. Prove that any group of order 126 must contain a normal subgroup of order 7.
2. Suppose G is a group with order 1000. Prove that G contains a normal subgroup $N \trianglelefteq G$ such that $1 < |N| < 1000$.