These homework problems are meant to expand your understanding of what goes on during class. Any you turn in will be graded and returned to you. Answers may or may not be posted on the web, depending on demand.

1. What is the highest order shuffle of 52 cards. The formulation of this problem worked out in class, is: find a collection of positive integers \( \{m_1, \ldots, m_k\} \) so that 
\[
m_1 + m_2 + \cdots + m_k = 52 \quad \text{and} \quad \operatorname{lcm}(m_1, m_2, \ldots, m_k)
\]
is as large as possible. Feel free to use a computer.

2. One fact we did not prove in class is that the order of \( A_n \) (the even permutations in \( S_n \)) is \( n!/2 \), or precisely half the order of \( S_n \). Write down (a) the 3 elements of \( A_3 \) and (b) the 12 elements of \( A_4 \). Don’t forget the identity!

3. Consider the element \( (234) \) in \( S_4 \). We say that an element \( y \in S_4 \) is conjugate with \( (234) \) if 
\[
y = x^{-1}(234)x \quad \text{for some} \quad x \in S_4.
\]
For example, \( (134) \) is conjugate to \( (234) \) since \( (12)(234)(12) = (134) \).

4. Prove that if \( a \equiv b \mod n \) then \( ca \equiv cb \mod n \) and \( a + c \equiv b + c \mod n \) for any positive integer \( c \). That is, show that if \( n|(a - b) \), then \( n|(ca - cb) \) and \( n||((a + c) - (b + c)) \). (Here “\( m|n \)” means “\( m \) divides \( n \).”)

5. Prove that if \( a \equiv b \mod n \) and \( c \equiv d \mod n \), then \( ac \equiv bd \mod n \). Another way of seeing this is that this means \( a = b + nr \) and \( c = d + ns \) for some integers \( r \) and \( s \). You want to show that \( ac = bd + nt \) for some integer \( t \).

6. Compute (a) \( 7^{50} \mod 13 \) and (b) \( 2^{1000} \mod 11 \). Here is an extended hint, using as an example the computation of \( 5^{23} \mod 7 \). We’ll compute various powers of 5:
\[
5^1 \equiv 5 \mod 7 \\
5^2 = 25 \equiv 4 \mod 7 \\
5^4 \equiv 4^2 \equiv 2 \mod 7 \\
5^8 \equiv 2^2 \equiv 4 \mod 7 \\
5^{16} \equiv 4^2 \equiv 2 \mod 7.
\]
Next we write 23 as \( 16 + 4 + 2 + 1 \), so \( 5^{23} = 5^{16} \cdot 5^4 \cdot 5^2 \cdot 5^1 \). Working modulo 7, we have 
\[
5^{23} \equiv 2 \cdot 2 \cdot 4 \cdot 5 \equiv 3 \mod 7.
\]

7. Show that not all the \( G_n \) are cyclic by showing that \( G_8 \) is isomorphic to \( D_2 \).

(a) Find all elements in \( S_4 \) that are conjugate with \( (12) \). We call this set of elements the conjugacy class of \( (12) \).

(b) Find all other conjugacy classes in \( S_4 \).

(c) Do any of your conjugacy classes intersect?
(d) Does any element not belong to a conjugacy class?

8. In this problem, we derive a formula for the Euler $\phi$-function (also known as the *totient* function). Recall that this is defined as

$$\phi(n) = \text{the number of integers } k \text{ with } 0 < k < n \text{ and } \gcd(k, n) = 1.$$

(a) Prove that for a prime $p$, $\phi(p^n) = (p - 1)p^{n-1}$. (Hint: what are the integers $0 < k < p^n$ that have a common factor with $p^n$?)

(b) (Hard, and I recommend you skip this part and just assume this for part (c).) Prove that $\phi$ is multiplicative. That is, if $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

(c) Derive a formula for $\phi(n)$. Your answer should involve the prime factorization of $n = p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}$.

(d) What is $\phi(10^{10})$?

9. Part (b) of the previous problem actually follows from the following more general version of the Chinese Remainder Theorem than in the previous homework. (This is with only two equations, but the general form is with an arbitrary number.) We’ll prove that, given two relatively prime integers $m$ and $n$ and elements $x \in G_m$ and $y \in G_n$, there is a unique $z \in G_{mn}$ such that

$$z \equiv x \mod m$$
$$z \equiv y \mod n.$$

(This means that order of $G_{mn}$ is the product of the orders of $G_m$ and $G_n$, which implies part (b) of the previous problem.)

Let $z = xm^{-1}m + yn^{-1}n$, where $m^{-1}$ is the inverse of $m$ in $G_n$ and $n^{-1}$ is the inverse of $n$ in $G_m$.

(a) Show that $z$ satisfies the equations above.

(b) Show that $z$ is an element of $G_{mn}$. That is, show that $z$ is relatively prime to $mn$. (Hint: show that $m$, $m^{-1}$, and $x$ are all elements of $G_n$, hence $xm^{-1}m$ is as well. This means that $xm^{-1}m$ is relatively prime to $m$. Do something similar with the other term.)

(c) Show that $z$ is unique in $G_{mn}$. That is, if $z'$ is another solution, show that $z - z'$ must be an integer multiple of $mn$. (Hint: we know that $z \equiv z' \mod m$ and $z \equiv z' \mod n$. What does this mean about $m$, $n$, and $z - z'$?)