MODEL ANSWERS TO THE FOURTH HOMEWORK

1. Chapter 2, Section 4: 13. First we write down the elements of U_{18}. These will be the left cosets, generated by integers coprime to 18. Of the integers between 1 and 17, those that are coprime to 18 are 1, 5, 7, 11, 13 and 17.
Thus the elements of U_{18} are [1], [5], [7], [11], [13] and [17]. We calculate the order of these elements.
[1] is the identity, it has order one.
Consider [5].

$$[5]^2 = [5^2] = [25] = [7],$$

as $25 = 7 \mod 18$. In this case

$$[5^3] = [5][5^2] = [5][7] = [35] = [17],$$

as $35 = 17 \mod 18$.
We could keep computing. But at this point, we can be a little more sly. By Lagrange the order of $g = [5]$ divides the order of G. As G has order 6, the order of [5] is one of 1, 2, 3, or 6. As we have already seen that the order is not 1, 2 or 3, by a process of elimination, we know that [5] has order 6.
As $[17] = [5]^3$, $[17]^2 = [5]^6 = [1]$. So [17] has order 2. Similarly, as $[7] = [5]^2$, $[7]^3 = [5]^6 = [1]$. So the order of [7] divides 3. But then the order of [7] is three.
It remains to compute the order of [11] and [13]. Now one of these is the inverse of [5]. It must then have order six. The other would then be $[5]^4$ and so this element would have order dividing 3, and so its order would be 3. Let us see which is which.

$$[5][11] = [55] = [1]$$

Thus [11] is the inverse of [5] and so it has order 6. Thus $[11] = [5]^5$. It follows that $[13] = [5]^4$ and so [13] has order 3.
Note that U_{18} is cyclic. In fact either [5] or [11] is a generator.
2. Chapter 2, Section 4: 13. First we write down the elements of U_{20}. Arguing as before, we get [1], [3], [7], [9], [11], [13], [17] and [19].
We compute the order of [3].

$$[3]^2 = [9].$$

$$[3]^3 = [27] = [7].$$

$$[3^4] = [3][3^3] = [3][7] = [21] = [1].$$

So [3] and [7] are elements of order 4 and [9] is an element of order 2. Now note that the other elements are the additive inverses of the elements we just wrote down. Thus for example

$$[17]^2 = [-3]^2 = [3]^2 = [9].$$

So [17] and [13] have order 4 and [11] and $[19] = [-1]$ have order 2. Thus U_{20} is not cyclic.

1. Chapter 2, Section 4: 24. Suppose not, that is suppose that there is a number a such that $a^2 = -1 \mod p$. Let $g = [a] \in U_p$. What is the order of g?

Well

$$g^2 = [a]^2 = [a^2] = [-1] \neq [1],$$

and so

$$g^4 = (g^2)^2 = [-1]^2 = [1].$$

Thus g has order 4. But the order of any element, divides the order of the group, in this case $p-1 = 4n+2$. But 4 does not divide $4n+2$, a contradiction.

2. Chapter 3, Section 1: 1 (a)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}.$$

(b)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}.$$

(c)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}.$$

5. It suffices to find the cycle type and take the lowest common multiples of the individual lengths of a cycle decomposition.

(a)

$$(1, 4)(2, 5, 3)$$

Order 6.

(b)

$$(1, 3, 2)$$

Order 3.

(c)

$$(2, 4)$$

Order 2.

2. Chapter 3, Section 2: 1 As σ and τ are cycles, we may find integers $a_1, a_2, \dots, a_k$ and $b_1, b_2, \dots, b_l$ such that $\sigma = (a_1, a_2, \dots, a_k)$ and $\tau = (b_1, b_2, \dots, b_l)$. To say that σ and τ are disjoint cycles is equivalent to saying that the two sets $S = \{a_1, a_2, \dots, a_k\}$ and $T = \{b_1, b_2, \dots, b_l\}$ are disjoint.

We want to prove that

$$\sigma\tau = \tau\sigma.$$

As both sides of this equation are permutations of the first n natural numbers, it suffices to show that they have the same effect on any integer $1 \leq j \leq n$.

If j is not in $S \cup T$, then there is nothing to prove; both sides clearly fix j. Otherwise $j \in S \cup T$. By symmetry we may asume $j \in S$. As S and T are disjoint, it follows that $j \notin T$.

As $j \in S$, $j = a_i$, some i. Then $\sigma(a_i) = a_{i+1}$, where we take $i + 1$ modulo k (that is we adopt the convention that $k + 1 = 1$). In this case $a_{i+1} \in S$ so $a_{i+1} \notin T$ as well. Thus both sides send $j = a_i$ to a_{i+1}. Thus both sides have the same effect on j, regardless of j and so

$$\sigma\tau = \tau\sigma.$$

2. Chapter 3, Section 2: 2

(a)

$$(1, 3, 4, 2)(5, 7, 9)$$

Order 12.

(b)

$$(1, 7)(2, 6)(3, 5).$$

Order 2.

(c)

$$(1, 6)(2, 5)(3, 7)$$

Order 2.

2. Chapter 3, Section 2:

3 (a)

$$(2, 4, 1)(3, 5, 7, 6).$$

Order 12.

(f)

$$(1, 4, 2, 5, 3)$$

Order 5.

2. Chapter 3, Section 2: 8 (a)

$$(2, 1)(2, 4)(3, 6)(3, 7)(3, 5).$$

(f)

$$(1, 3)(1, 5)(1, 2)(1, 4).$$

3. Easy, the conjugate is $(2, 7, 5, 3)(1, 6, 4)$. The order of σ is 12 and the order of τ is three.
4. There are quite a few possibilities for τ. One obvious one is

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 5 & 4 & 7 & 6 \end{pmatrix}.$$

Challenge Problems (Just for fun).
6. Chapter 2, Section 4: 36. Let $m = a^n - 1$. Then $\phi(m)$ is the order of the group $G = U_m$. By Lagrange, it suffices to exhibit a subgroup H of G of order n. Set $g = [a]$ and let $H = \langle g \rangle$. Then the order of H is the order of g. Now

$$g^n = [a]^n = [a^n] = [m + 1] = [1].$$

So the order of g divides n. On the other hand $a^i < m$, for any $i < n$ so that

$$g^i = [a^i] \neq [1].$$

Thus the order of g is n and so n divides m by Lagrange.
6. Chapter 2, Section 4: 37. Let G be a cyclic group of order n, and let $g \in G$ be a generator of G. Suppose $h \in G$. Then $h = g^i$, for some i.
First note that as

$$e = h^m = (g^i)^m = g^{im}$$

it follows that $im = jn$ is a multiple of n. Let $k = n/m$, so that $n = km$. Cancelling m from both sides we get that $i = jk$ is a multiple of k.
Conversely if $i = jk$ is a multiple of k then $h^m = e$ and so the order of h divides m.
Suppose that the prime p divides both j and m. Then j is a multiple of pk and so the order of h divides m/p.
It follows that h has order m if and only $i = jk$, where j is coprime to m.
The number of integers of the form kj, where j is coprime to m, is equal to the number of integers j coprime to m (and less than m) which is $\phi(m)$.
6. Chapter 2, Section 4: 38. Let G be a cyclic group of order n. Partition the elements of G into subsets A_m, where A_m consists of all

elements of order m. Then

$$\begin{aligned} n &= |G| \\ &= |\bigcup_{m|n} A_m| \\ &= \sum_{m|n} |A_m| \\ &= \sum_{m|n} \phi(m). \end{aligned}$$

7. Let $H = \langle (1,2)(1,2,3,\dots,n) \rangle$. We want to show that H is the whole of S_n. As the transpositions generate S_n, it suffices to prove that every transposition is in H.
Now the idea is that it is very hard to compute products in S_n, but it is easy to compute conjugates. So instead of using the fact that H is closed under products and inverses, let us use the fact that it is closed under taking conjugates (clear, as a conjugate is a product of elements of H and their inverses).
Since conjugation preserves cycle type, we start with the transposition $\sigma = (1,2)$ (in fact this is the only place to start).
To warm up, consider conjugating σ with $\tau = (1,2,3,\dots,n)$. The conjugate is $(2,3)$. Thus H must contain $(2,3)$.
Given that H contains $(2,3)$ it must contain the conjugate of $(2,3)$ by τ, which is $(3,4)$ (or what comes to the same thing, H must contain the conjugate of $(1,2)$ by τ^2).
Continuing in this way, it is clear that H (by an easy induction in fact) must contain every transposition of the form $(i, i+1)$ and of course the last one, $(n,1) = (1,n)$.
From here, let us try to show that H contains every transposition of the form $(1,i)$. For example, to get $(1,3)$, start with $(1,2)$ and conjugate it by $(2,3)$. Suppose, by way of induction, that H contains $(1,i)$. Then H must contain the conjugate of $(1,i)$ by $(i,i+1)$ which is $(1,i+1)$. Thus by induction H contains every transposition of the form $(1,i)$.
Now we are almost home. Note that H must contain every transposition of the form $(2,j)$. Indeed $(2,j)$ is the conjugate of $(1,j)$ by the transposition $(1,2)$.
Now consider an aribtrary transposition (i,j). This is the conjugate of $(1,2)$ by the element $(1,i)(2,j)$. Thus H contains every transposition.
Aliter:
There is another way to show that the transpositions $(i,i+1)$, $1 \leq i \leq n$ generate S_n. Consider a deck of cards in the order given by a

permutation $\tau \in S_n$. It is enough to show that we can put the deck of cards into the correct order, just using $(i, i+1)$, $1 \leq i \leq n$.
Suppose that we have rearranged the cards so that the first k cards are in the correct order. By induction it is enough to show we can put the $(k+1)$th card into the $(k+1)$th position.
Consider the $(k+1)$th card. Suppose it occupies position l. If $l = k+1$ we are done. Now $l > k$ since the first k cards are in their correct position. Thus $l > k+1$. If we apply the transposition $(l-1, l)$ then we put the $(k+1)$th card into the $(l-1)$th position. Continuing in this way, we can continue swapping until it is in the $(k+1)$th position.
It follows that we can undo any permutation by applying a sequence of transpositions $\tau_1, \tau_2, \dots, \tau_k$ of the form $(i, i+1)$,

$$\tau^{-1} = \tau_1 \tau_2 \dots \tau_k.$$

Taking inverses we express τ as product in the opposite order.
8. Look at the group $A(\mathbb{N})$ of permutations of the natural numbers. Now this is not countable, but consider the subgroup G consisting of all permutations that fix all but finitely many natural numbers. Note that $A(\mathbb{N})$ contains a nested sequence of copies of S_n, for all n, in an obvious way and that G is in fact the union of these finite subgroups. In particular G is countable, as it is the countable union of countable sets. Now suppose that $g_1, g_2, \dots, g_k$ were a finite set of generators. Then in fact there is some n such that $g_i \in S_n$, for all i. As S_n is a subgroup of G, it follows that

$$\langle g_1, g_2, \dots, g_k \rangle \subset S_n \neq G,$$

a contradiction. Put differently, no finite subset generates G, since any finite subset will only permute finitely many natural numbers.