MODEL ANSWERS TO THE THIRD HOMEWORK

Chapter 2, Section 4: 1. (b) Concentric circles with centre the origin.
(c) The real line union ∞, where the number $m \in \mathbb{R} \cup \{\infty\}$ represents the slope.
2. Chapter 2, Section 4: 9.

$$\begin{aligned}
[0] &= 0 + H = \{[0], [4], [8], [12]\} \\
[1] &= 1 + H = \{[1], [5], [9], [13]\} \\
[2] &= 2 + H = \{[2], [6], [10], [14]\} \\
[3] &= 3 + H = \{[3], [7], [11], [15]\}
\end{aligned}$$

2. Chapter 2, Section 4: 10. Four.
2. 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 are 1, 3, 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.
2. Chapter 2, Section 4: 16. For every i, there is a unique b_i which is the inverse of a_i. Thus the elements of G are both $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$. Now

$$\begin{aligned} x^2 &= (a_1 a_2 \dots a_n)(a_1 a_2 \dots a_n) \\ &= (a_1 a_2 \dots a_n)(b_1 b_2 \dots b_n) \\ &= (a_1 b_1)(a_2 b_2)(a_3 b_3) \dots (a_n b_n) = e^n = e, \end{aligned}$$

where we used the fact that G is abelian to rearrange these products.
3. 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.

3. Chapter 2, Section 4: 26. Define

$$f\colon S \longrightarrow T$$

by the rule

$$f(Ha) = a^{-1}H.$$

The key point is to check that f is well-defined. The problem is that if $b \in Ha$, then $Ha = Hb$ and we have to check that $Ha^{-1} = Hb^{-1}$.
As $b \in Ha$, we have $b = ha$. But then $b^{-1} = a^{-1}h^{-1}$. As H is a subgroup $h^{-1} \in H$. But then $b^{-1} \in a^{-1}H$ so that $a^{-1}H = b^{-1}H$ and f is well-defined.
To show that f is a bijection, we will show that it has an inverse. Define

$$g\colon T \longrightarrow S$$

by the rule

$$g(aH) = Ha^{-1}.$$

We have to show that g is well-defined. This follows, exactly as in the proof that f is well-defined. Then $g(f(aH)) = g(Ha^{-1}) = aH$ and similarly fg is the identity. It follows that f is a bijection.
3. Chapter 2, Section 4: 27.
Let $[a]_L$ denote the left-coset generated by a and let $[a]_R$ denote the right-coset generated by a. Suppose that $b \in [a]_L$. Then $[a]_L = [b]_L$ and so $aH = bH$. By assumption $Ha = Hb$. But then $[a]_R = [b]_R$ and so $b \in [a]_R$.
As b is an arbitrary element of $[a]_L$, it follows that $[a]_L \subset [a]_R$. In other words $aH \subset Ha$. Multiplying both sets on the right by a^{-1} we get the inclusion

$$aHa^{-1} \subset H.$$

Now this is valid for any $a \in G$, so that

$$bHb^{-1} \subset H.$$

for all $b \in G$. Take $b = a^{-1}$. Then

$$a^{-1}Ha \subset H,$$

so that multipying on the left by a, we get

$$Ha \subset aH.$$

Thus $Ha = aH$ and $aHa^{-1} = H$.
4. **Challenge Problems** 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.

4. **Challenge Problems** 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.

I claim that h has order m if and only if $i = kj$, where $k = n/m$ and j is coprime to m.

Suppose that $i = kj$. Then

$$h^m = (g^i)^m = g^{kjm} = g^{jn} = (g^n)^j = e.$$

Now suppose that $a < m$ and consider $h^a = g^{akj}$. This is equal to the identity if and only if akj is divisible by n. Dividing by k, this is the same as saying that aj is divisible by m. As j is coprime to m, this would mean that m divides a, impossible.

This establishes the claim. 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 $\phi(m)$.

4. **Challenge Problems** 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

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