(1) (3.10) How many subgroups of order 4 does the group D_4 have?

Proof. This one is tricky. As I pointed out in an email message, in Example 15 there are a list of subgroups of D_4, three of which have order 3. These subgroups are all the centralizers of the different elements of the group. The question is, are there any others? The answer to that is no. The hard part is to see why are there no others.

Note that there are two elements of order 4, namely R_{90} and R_{270}. They each generate the same subgroup of order 4, which is on the list. All other elements of D_4 have order 2. Also notice that all three subgroups of order 4 on the list contain R_{180}, which commutes with all elements of the group. Now let $H = \{e, a, b, c\}$ be a subgroup of order 4 not on the list. Thus the elements a, b, c all have order 2 (for if H contained an element of order 4, it would equal a subgroup on the list). Furthermore, these elements must all commute with each other, otherwise we would get a fifth element. To see why, suppose that $ab = c$, while $ba \neq c$, Then ba is a new element not already in H. Hence all pairs of elements in H commute. Now one of a, b or c is not a rotation, otherwise $H = \{R_{90}, R_{180}, R_{270}, R_{0}\}$ which is on the list. Say a is not a rotation. Then $H = C(a)$, which again means H is on the list, and we are done.

(2) (3.22) Show $\mathcal{U}(14) = \langle 3\rangle = \langle 5\rangle$. Hence $\mathcal{U}(14)$ is cyclic. Is $\mathcal{U}(14) = \langle 11\rangle$?

Proof. This is strictly brute force. We have $\mathcal{U}(14) = \{1, 3, 5, 9, 11, 13\}$. We take powers of 3 to get:

$$3^1 = 3, 3^2 = 9, 3^3 = 27 = 13, 3^4 = 13 \cdot 3 = 39 = 11, 3^5 = 33 = 5, 3^6 = 1.$$

This is all of $\mathcal{U}(14)$, whence 3 generates the group. In a similar fashion we have that

$$\{5^1 = 55^2 = 11, 5^3 = 13, 5^4 = 9, 5^5 = 3, 5^6 = 1\} = \mathcal{U}(14).$$

Thus both 3 and 5 generate the group. On the other hand

$$\{11^1 = 11, 11^2 = 121 = 9, 11^3 = 99\} = 1 \neq \mathcal{U}(14).$$

So 11 does not generate.

(3) (3.24) Suppose that n is an even positive integer and H is a subgroup of $\mathbb{Z}_n$. Prove that either every member of H is even or exactly half are even.

Proof. The key is that if n is even, then the sum of two even integers modulo n and the sum of two odd mod n is even. To see why let a and b be even or both odd integers, then $a + b$ is even. Then using the division algorithm we can write $a + b = nq + r$ with $0 \leq r < n$. Since $a + b$ is even and nq is even, r must be even as claimed. Similarly the sum of an even and an odd mod n is again odd.

Now let H be a subgroup. If all the elements of H are even, we're done. Otherwise let $\mathcal{E}$ and $\mathcal{O}$ denote the even and the odd elements of H, so $\mathcal{E} \bigcup \mathcal{O} = H$. Let $a \in \mathcal{O}$ and define a map $\mathcal{E} \to \mathcal{O}$ via $x \mapsto x + a$. Then adding a to an element also defines a map in the reverse direction. Clearly these maps are inverses of each other, since $x + 2a$ has the same parity as x. Thus the two sets $\mathcal{E}$ and $\mathcal{O}$ have the same order, and we are done.

(4) (4.22) Show that a group of order 3 is cyclic.

Proof. We will use brute force. Let $G = \{e, a, b\}$ (e the identity element). It will suffice to show that $a^2 = b$, for then $a^3 = e$ (the only element left) and so a generates G. Clearly $a^2 \neq a$, for that would imply $a = e$, which it is not. Now suppose that $a^2 = e$. But we also know that ab is in G, and it cannot equal either a or b (by the cancelation property). Thus $ab = e$ and so $a^2 = ab$. Therefore again by cancelation we have $e = b$, a contradiction. Thus $a^2 = b$ and so a is a generator.

(5) (3.34) Find the six cyclic subgroups of $U(15)$.

Proof: $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$. We will examine the cyclic subgroup generated by each element of G.

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{2, 4, 8, 1\}$

$\langle 4 \rangle = \{4, 1\}$

$\langle 7 \rangle = \{7, 4, 13, 1\}$

$\langle 8 \rangle = \{8, 4, 2, 1\} = \langle 2 \rangle$

$\langle 11 \rangle = \{11, 1\}$

$\langle 13 \rangle = \{13, 13^2 = 169 = 4, 7, 1\} = \langle 7 \rangle$

$\langle 14 \rangle = \{14, 1\}$

Some of the subgroups listed above are duplicates. However, there are six distinct cyclic subgroups; namely the subgroups generated by each of $1, 2, 4, 7, 11, 14$.