1. [Artin 2011 2.8.3-4] (a) Show that every group of order $p^k$ (where $p$ prime) contains an element of order $p$.

(b) Show that every group of order 35 contains an element of order 5 and an element of order 7.

Remark: The more general case for (b) of a group of order $pq$ remains elusive for the moment, but, as we will see later, if $p \mid |G|$ then $G$ has an element of order $p$.

(a) Let $G$ be of order $p^k$, with $p$ prime and let 1 denote the identity. Choose some element $x \neq 1$ of $G$. Then the order of $x$ divides the order of $G$. Hence the order of $x$, i.e. the smallest positive power that is the identity, is $p^m$ for some $m \leq k$. Then I claim $y = x^{(p^m - 1)}$ has order $p$. Indeed, if $0 < a < p$ then $y^a = x^{(ap^m - 1)}$ and $ap^m - 1 < p^m$ so this is not equal to 1. Further $y^p = x^{(p^m)} = 1$.

(b) Let $G$ be a group of order 35. Any non-identity element has order greater than 1 and dividing $|G| = 35$, hence is 5, 7, or 35. If there’s an element $x$ of order 35 then, as in (a), we get an element $x^7$ of order 5 and $x^5$ of order 7 and we’re done in this case.

Thus the only way for there not to be both an element of order 5 and an element of order 7 is for there to be, other than the identity, only elements of order 5 or of order 7.

Suppose all elements are of order 5. Then I claim that the sets of the form $S_x = \{x, x^2, x^3, x^4 \mid x \in G - \{1\}\}$ partition $G - \{1\}$. Indeed, if $S_x$ and $S_y$ overlap, then $x^a = y^b$ for some $a$ and $b$ not equivalent to zero mod 5. Because 5 is prime, there is some $s$ such that $sa \equiv 1 \pmod{5}$ by problem set 2 problem 6. Hence $x = y^s$. So $S_x \subset S_y$ (because the latter contains all non-identity powers of $y$). Likewise we see $S_y \subset S_x$.

Thus if all elements except 1 are of order 5, then $5 - 1 = 4$ divides $|G| - 1$. But 4 does not divide $35 - 1 = 34$.

Similarly, if all elements are of order 7, then $7 - 1 = 6$ divides $|G| - 1$. But 6 does not divide 34 either.

Thus there are elements of both orders, 5 and 7.
4. Show there are precisely two isomorphism classes of groups of order $2p$ where $p$ is an odd prime. Describe them. (Hint: Use your work and/or results from problems 1, 2, and 3.)

Let $G$ be a group of order $2p$. By the reasoning in 1(b), we see that there can’t be only elements (other than the identity) of order $p$ because $p - 1$ doesn’t divide $|G| - 1 = 2p$. Also, by the result in 3(b) that the order of a group in which every element (other than the identity) has order 2 is $2^n$ shows that we don’t have every element (other than the identity) of order 2.

Thus there is at least one element of order 2 and at least one element of order $p$. The element of order $p$ generates a (cyclic) subgroup we’ll call $H$ of order $p$. We have $[G : H] = 2p/p = 2$. Hence by problem 2(a) we see $H$ is normal. Let $K$ be the subgroup generated by the element of order 2. We have $H \cap K = \{1\}$. I claim $HK$ is all of $G$. Indeed, I claim it has $2p$ distinct elements: suppose $h_1k_1 = h_2k_2$. Then $h_2^{-1}h_1 = k_2k_1^{-1}$. Thus both are 1 and so $h_1 = h_2$ and $k_1 = k_2$. Thus elements of the form $hk$ are distinct for all pairs $(h, k)$. Thus there are $2p$ distinct elements of this form, hence all of $G$.

Thus we’re in the situation in which we have a semidirect product ($H$ normal subgroup, $K$ a subgroup, $H \cap K = \{1\}$, $HK = G$). Thus $G = H \rtimes_{\phi} K$ for some $\phi : K \to Aut(H)$. We choose isomorphisms of $H$ with $\mathbb{Z}/p\mathbb{Z}$ and of $K$ with $\mathbb{Z}/2\mathbb{Z}$. Such a $\phi$ is determined by where $1 \in \mathbb{Z}/2\mathbb{Z}$ is sent. Our choices are any element of $Aut(\mathbb{Z}/p\mathbb{Z})$ of order 2. By problem set 2 problem 6, $Aut(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$. An element of order 2 is an element $a \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a^2 \equiv 1 \pmod{p}$.

I claim only 1 and $-1 \equiv p - 1$ satisfy this. Indeed, suppose $p$ divides $a^2 - 1$ (i.e. $a^2 - 1$ is zero mod $p$). Then, using that $a^2 - 1 = (a - 1)(a + 1)$, we see that either $p$ divides $a - 1$ or $p$ divides $a + 1$. These are the two cases of $a$ equivalent to 1 and $-1$ modulo $p$.

Hence there are two groups. If we choose $\phi$ sending $1 \in \mathbb{Z}/2\mathbb{Z}$ to the identity automorphism, we get $C_2 \times C_p \cong C_{2p}$. If we choose $\phi$ sending $1 \in \mathbb{Z}/2\mathbb{Z}$ to the automorphism “multiplication by $-1$” then we get the dihedral group $D_p$ (which was described in class as precisely this semidirect product).