This is help for the redo of Exercises 4.7, 4.8, and 4.9 due Monday, May 5th. These hints are only hints; you will have to write the answers in your own words. Good luck!

4.7

What is going on here? $S_{(a,b)}$ is better described as all numbers that can be written as the sum of a multiple of $a$ and a multiple of $b$. So if $a = 3$ and $b = 5$, it’s all numbers that look like $3m + 5n$, for example $8 (m = n = 1)$ or $6 (m = 2, n = 0)$ or $-11 (m = -2, n = -1)$. So in general it’s everything that looks like $ma + nb$. This is what you should keep in mind throughout; it’s everything that looks like $ma + nb$.

So how do we approach these problems? Consider the first part. We have to show that a certain set ($S_{(a,b)}$) is closed under subtraction. To do this, first we have to know what it means to be closed under an operation. For instance, saying that a set $X$ is closed under addition means that for every $x$ and every $y$ in $X$, $x + y$ is also in $X$. Here, it means that for every $z$ and $z'$ in $X$, $z - z' \in X$. But what do $z$ and $z'$ look like? They look like $x + y$ and $x' + y'$, where $x$ and $x'$ are multiples of $a$, and $y$ and $y'$ are multiples of $b$. And it’s the same $a$ and $b$ for both $z$ and $z'$! So you should subtract them from one another; use various axioms (hint: distribution and/or commutativity) to show that $z - z'$ is also in $X$.

In the second part, the goal is to show that a and b are elements of $S_{(a,b)}$. Again, these are the same $a$ and $b$. So write $a = x + y$ such that $x$ is a multiple of $a$ and $y$ is a multiple of $b$. Remember, they can be any integer multiples. If you have trouble, let $a = 3$ and $b = 5$ again, and see how to write 3 as a combination of multiples of 3 and 5.

In the third part, we have a lot to parse. First, if either $a$ or $b$ is nonzero means that at least one of them, possibly both, is nonzero. So for instance suppose $a \neq 0$. Then they want you to show that $S_{(a,b)} \neq \{0\}$. What does that mean? It does not mean that $S_{(a,b)}$ is not the empty set; it means that $S_{(a,b)}$ is not the set with one element, which is zero. So you have to find a non-zero $x + y$ in $S_{(a,b)}$, using that $a$ or $b$ is not zero. Again, recall what $x$ and $y$ look like. If $a = 0$, plug that into what I said what important to remember at the beginning of this problem.

The fourth part is the whole point of this. Take the smallest element of $S_{(a,b)}$ and call it $d$. The book’s hint says to take the Division Algorithm and the fact it is the smallest element of $S_{(a,b)}$ to show that the remainder of $a$ divided by $d$ is zero. So use the division algorithm; $a = dq + r$, where $0 \leq r < d$. If $r \neq 0$, then $r = a - dq$; show that this gives a contradiction with $d$ being the smallest element of $S_{(a,b)}$. Thus $d|a$. You will also have to show that $d|b$. Thus $d$ is a common divisor; the book suggests that you then use the way to write $d = ma + nb$ to show that the greatest common divisor of $a$ and $b$ divides it; then you must use that to show it is the gcd.

If you’ve made it this far, you should be able to finish up on your own. Even if you can’t prove the fifth part, you can use it to do the sixth part.
4.8

This is just an application of 4.7d; it should not be scary. I think that explaining the example should allow you to do one of the possibilities a, b, or c by mimicking it.

The goal is to write the greatest common divisor of $a$ and $b$ (call it $d$) as a combination of $a$'s and $b$'s, so that $ma + nb = d$. So the book uses $a = 78$ and $b = 30$ as an example. Everyone should be able to follow the first bit; $78 = 2 \cdot 30 + 18$ is using the Division algorithm, with remainder 18. Then we do it again on 30 and the remainder 18, getting $30 = 1 \cdot 18 + 12$, remainder 12. And so on, until the last non-zero remainder gives us the greatest common divisor $d = 6$ (in this case). This is the Euclidean algorithm, and you should understand it.

But then we rearrange each of the equations so that the remainder is alone on the left! For instance, instead of $78 = 2 \cdot 30 + 18$ we get $18 = 78 - 2 \cdot 30$. The other two are gotten similarly from the next two equations.

Now, we actually take the last equation with remainder on the left ($6 = 18 - 1 \cdot 12$) and substitute what we got for 12 on its own ($12 = 30 - 1 \cdot 18$) in its place, like so:

$$6 = 18 - 1 \cdot (30 - 1 \cdot 18).$$

Then the book rearranges so that all multiples of 18 are together, and so are all multiples of 30; in this case, there is $1 - (-1)$ copies of 18, so we get

$$6 = 2 \cdot 18 - 1 \cdot 30.$$

Then we do the same thing again, except we take the only remainder we haven’t used yet, in the form $18 = 78 - 2 \cdot 30$, and substitute it in. The book makes this clear; then we rearrange so that all multiples of 30 are together and all multiples of 78 are together, which gives

$$6 = -5 \cdot 30 + 1 \cdot 78.$$

But this is precisely a way of writing the greatest common divisor as a combination of 30’s and 78’s! You can always do this (because of the previous exercise), writing $(a, b) = ma + nb$ for some (which you have to figure out) integers $m$ and $n$.

In particular, you can use precisely the same method. Do the Euclidean algorithm; rewrite each equation with the remainder alone; and substitute each one in, step by step, from the last one on up, until you have $(a, b) = ma + nb$. Don’t forget to rearrange each time like in the example! So do it now, for one of the pairs of integers listed below.

4.9

First off, forget about Bruce Willis. Use the Euclidean algorithm to find a solution to $3m + 5n = 4$. How? The Euclidean algorithm only gives the gcd of $(3, 5)$, which is 1 (though you should say why). By the previous exercise, we can sort of back-engineer the Euclidean algorithm and write the gcd in the form $1 = 3k + 5\ell$ for some integers $k$ and $\ell$. That’s all we know. You have to write $4 = 3m + 5n$. What should you take for $m$ and $n$?

Now remember Bruce Willis; how would you use this information to disarm the bomb? Remember, you can’t fill a water can past all the way full, so in order to keep filling from another can, you’d have to dump out the water you’ve already poured.