Homework #4 Solutions

3.3.9. Assume for the moment that the formula $(ca, cb) = |c|(a, b)$ has been proved when c is positive. Then if c is negative, $|c|$ is positive, so

$$(ca, cb) = (|ca|, |cb|) = (|c||a|, |c||b|) = |c|(|a|, |b|) = |c|(a, b).$$

This means that it suffices to prove the formula for c positive, in which case the formula is reduced to $(ca, cb) = c(a, b)$. Let $d = (a, b)$ and $e = (ca, cb)$. We must show that $e = cd$, and we will do so by showing that e divides cd and vice versa. Since d is a common divisor of a and b, cd is a common divisor of ca and cb, which implies that $cd \mid e$ by Theorem 3.10. For the other divisibility, first note that because c is a common divisor of ca and cb, $c \mid e$ by Theorem 3.10. Now, since e divides ca, we may write $ca = ej$ for some integer j. Therefore $a = (e/c)j$, and because $c \mid e$, e/c is an integer, and this equation shows that a is divisible by e/c. Similar reasoning, beginning with the fact that e divides cb, shows that b is also divisible by e/c. So e/c is a common divisor of a and b, from which we may conclude, once again by Theorem 3.10, that $e/c \mid d$, hence that $e \mid cd$. This completes the proof.

Here is an alternative argument for the second divisibility in the solution to Exercise 3.3.9. By Bézout's theorem, there are integers r and s for which $ra + sb = d$. Multiplying both sides of this equation by c gives $r(ca) + s(cb) = cd$. So cd is a linear combination of ca and cb, which, by Theorem 3.9, implies that e divides cd. (The statement of Theorem 3.9 includes the assumption that a and b are positive but it is true, with the same proof, under the weaker assumption that a and b are not both zero.)

3.3.16. (a) Since $(a, b) = 1$, we may write $ra + sb = 1$ for some integers r and s. Similarly, as $(a, c) = 1$, we may write $ma + nc = 1$ for some integers m and n. Now we compute:

$$\begin{aligned} 1 &= (ra + sb)(ma + nc) \\ &= (ra)(ma) + (sb)(ma) + (ra)(nc) + (sb)(nc) \\ &= (rma + sbm + rnc)a + (sn)bc. \end{aligned}$$

Thus 1 is a linear combination of a and bc, so we may conclude using Corollary 3.8.2 that a and bc are relatively prime. Here is another argument. Let $d = (a, bc)$. Multiplying the equation $1 = ra + sb$ by c gives $c = rac + sbc$. Since d divides a and d divides bc, it follows that d divides c. Thus d is a common divisor of a and c, but we have assumed that $(a, c) = 1$, so $d = 1$.

(b) We argue by induction on n. The base case $n = 2$ is the assertion of part (a) (with different notation). Note that one could begin with the case $n = 1$; however, when $n = 1$ the assertion is a tautology (it says "if $(a_1, b) = 1$ then $(a_1, b) = 1$"), and, more importantly, for the inductive step, we really need the case $n = 2$. Assume now that $k \geq 2$ and that the assertion is true for k, and let $a_1, \ldots, a_{k+1}$ be integers such that that

$$(a_1, b) = \cdots = (a_k, b) = (a_{k+1}, b) = 1.$$

Date: February 17, 2018.

We wish to show that $(a_1 \cdots a_k a_{k+1}, b) = 1$. Let $a = a_1 \cdots a_k$. Then our inductive hypothesis gives $(a, b) = 1$. Since $(a_{k+1}, b) = 1$ by assumption, we may apply (a) (i.e. the base case) to conclude that

$$(a_1 \cdots a_k a_{k+1}, b) = (aa_{k+1}, b) = 1.$$

3.3.24. We observe that

$$5(3k + 2) - 3(5k + 3) = 15k + 10 - 15k - 9 = 1.$$

Thus $(3k + 2, 5k + 3) = 1$ by Corollary 3.8.2.

3.3.30. We will make repeated use of the fact that $(a, b) = (a + rb, b)$ for any integers a, b, and r with a and b not both zero. We have

$$\begin{aligned}(n + 1, n^2 - n + 1) &= (n + 1, n^2 - n + 1 - n(n + 1)) \\ &= (n + 1, -2n + 1) \\ &= (n + 1, -2n + 1 + 2(n + 1)) = (n + 1, 3).\end{aligned}$$

It follows that $(n + 1, n^2 - n + 1)$ divides 3, and therefore must be either 1 or 3.

3.4.2. (a) We have

$$\begin{aligned}87 &= 51 \cdot 1 + 36 \\ 51 &= 36 \cdot 1 + 15 \\ 36 &= 15 \cdot 2 + 6 \\ 15 &= 6 \cdot 2 + 3 \\ 6 &= 3 \cdot 2.\end{aligned}$$

Thus $(51, 87) = 3$.
(b) We have

$$\begin{aligned}300 &= 105 \cdot 2 + 90 \\ 105 &= 90 \cdot 1 + 15 \\ 90 &= 15 \cdot 6.\end{aligned}$$

Thus $(105, 300) = 15$.
(c) We have

$$\begin{aligned}1234 &= 981 \cdot 1 + 253 \\ 981 &= 253 \cdot 3 + 222 \\ 253 &= 222 \cdot 1 + 31 \\ 222 &= 31 \cdot 7 + 5 \\ 31 &= 5 \cdot 6 + 1 \\ 5 &= 1 \cdot 5.\end{aligned}$$

Thus $(981, 1234) = 1$.

3.4.4. (a) Working back through the steps of the Euclidean algorithm gives

$$\begin{aligned}
3 &= 15 - 2 \cdot 6 \\
&= 15 - 2(36 - 2 \cdot 15) \\
&= 5 \cdot 15 - 2 \cdot 36 \\
&= 5 \cdot (51 - 36) - 2 \cdot 36 \\
&= 5 \cdot 51 - 7 \cdot 36 \\
&= 5 \cdot 51 - 7 \cdot (87 - 51) = 12 \cdot 51 - 7 \cdot 87.
\end{aligned}$$

(b) Working back through the steps of the Euclidean algorithm gives

$$15 = 105 - 90 = 105 - (300 - 2 \cdot 105) = 3 \cdot 105 - 300.$$

(c) Working back through the steps of the Euclidean algorithm gives

$$\begin{aligned}
1 &= 31 - 6 \cdot 5 \\
&= 31 - 6 \cdot (222 - 7 \cdot 31) \\
&= 43 \cdot 31 - 6 \cdot 222 \\
&= 43 \cdot (253 - 222) - 6 \cdot 222 \\
&= 43 \cdot 253 - 49 \cdot 222 \\
&= 43 \cdot 253 - 49 \cdot (981 - 3 \cdot 253) \\
&= -49 \cdot 981 + 190 \cdot 253 \\
&= -49 \cdot 981 + 190 \cdot (1234 - 981) = -239 \cdot 981 + 190 \cdot 1234.
\end{aligned}$$