M417 Homework 1 Solutions Spring 2004

(1) #4, p. 23: Let $a = 11$ and $b = 7$. Then $gcd(a, b) = 1$ and $2a - 3b = 1$. Every possible expression of 1 as a linear combination of a and b is given by $(2 + 7t)a - (3 + 11t)b = 1$, for some integer t.

(2) #5, p. 23: See the back of the book for the answer.

(3) Let a and b be positive integers. Let $g = gcd(a, b)$, and let $\alpha = a/g$ and $\beta = b/g$. For each of the following statements, if it is false, give a counterexample; otherwise give a proof.

   (a) $gcd(\alpha, \beta) = 1$: by Theorem 0.2 we know that $g = ax+by$ for some integers x and y. Hence, $g = ax+by = g\alpha x+g\beta y$, so $1 = \alpha x + \beta y$. But by Theorem 0.2, $gcd(\alpha, \beta)$ is the least positive linear combination, which must be 1, since we now know 1 is a linear combination of α and β. Thus $gcd(\alpha, \beta) = 1$.

   (b) $gcd(\alpha, b) = 1$: this is false. Take $a = 12$ and $b = 18$. Then $g = 6$, $\alpha = 2$ and $gcd(\alpha, b) = 2$, not 1.

   (c) $gcd(a, b) = 1$ if and only if there are integers x and y such that $ax + by = 1$: By Theorem 0.2, $gcd(a, b)$ is a linear combination of a and b, so if $gcd(a, b) = 1$, then there are integers x and y such that $ax + by = 1$. Conversely, if there are integers x and y such that $ax + by = 1$, then, since $gcd(a, b)$ divides both a and b, it divides $ax + by$ and hence 1. Thus $gcd(a, b)$ is a positive integer which, since it divides 1, is a most 1. Thus $gcd(a, b) = 1$.

(4) Let a and b be positive integers. Let $g = gcd(a, b)$, $m = lcm(a, b)$, and let $\alpha = a/g$ and $\beta = b/g$ and define a' and b' such that $m = aa' = bb'$.

   (a) Show that $m \leq g\alpha\beta$. Conclude that $gm \leq ab$: Since $g\alpha\beta = a\beta = b\alpha$, we see that $g\alpha\beta$ is a positive common multiple of a and b. Hence $m \leq g\alpha\beta$ since m is the least common (positive) multiple. Thus $gm \leq g^2\alpha\beta = ab$, as claimed.

   (b) Show that $ab(a'x + b'y) = m(bx + ay)$ holds for all integers x and y and that $m(bx + ay) = gm$ holds for some integers x and y. Conclude that $ab \leq gm$: First, for any x and y we have $ab(a'x + b'y) = (baa'x + abb'y) = (bmx+amy) = m(bx+ay)$. By Theorem 0.2 (as before), we know $bx+ay = g$ holds for some integers x and y, and hence $m(bx + ay) = gm$ holds for some integers x and y. Thus $ab(a'x + b'y) = m(bx + ay) = gm$ holds for some x and y, so $ab|gm$, which shows that $ab \leq gm$.

   (c) Conclude that $gm = ab$: This is clear, since by (a) we have $gm \leq ab$ and by (b) we have $ab \leq gm$.

(5) Using the error correcting "circle" code discussed in class, determine the correct message encoded by the following code words: 1010101, 1101011, 1100101, 1100011, 1111111: the corrected codewords are 1010100, 0101011, 1100001, 1100001, 1111111. Taking the data bits only, the message is: 1010=10="J", 0101=5="E", 1100=12="L", 1100=12="L", 1111=15="O", or JELLO. (I actually meant it to be HELLO, but I typed the first codeword incorrectly. I was lucky that I still got a recognizable word!)