Math 255 - Spring 2018
Homework 2 Solutions

1. To simplify the notation, let $d = (a, b)$. Therefore we must show that $d = (d, b)$. For d to be the greatest common divisor of d and b, it suffices to show that it satisfies both conditions given in the definition of greatest common divisor.

   We begin by showing that $d|d$ and $d|b$. We have that $d|d$ because $d = d \cdot 1$, and 1 is an integer. We also have that $d|b$, since d is the greatest common divisor of a and b. Indeed, by definition d must be a common divisor of a and b, and therefore in particular a divisor of b.

   Now assume that c is any integer such that $c|d$ and $c|b$. We must show that $c \leq d$. As shown in class, since d is a greatest divisor, $d \geq 1$, and in particular $d = |d|$. We have also shown in class that the divisors of d are bounded above by $|d| = d$. Therefore if c is a divisor of d, then $c \leq d$.

   This completes the proof: d satisfies both conditions so that $d = (d, b)$.

2. This is an "if and only if" statement, so we must show both implications.

   We begin by assuming that $(k, n + k) = 1$. Let $d = (k, n)$. Since d is a greatest common divisor, $d \geq 1$. We now show that d divides $n + k$. Indeed, since d is the greatest common divisor of k and n, by definition there are integers s and t such that $k = sd$ and $n = td$. Therefore we have

   $$n + k = td + sd = (t + s)d,$$

   using the distributive property of integers. Since a sum of integers is an integer, d divides $n + k$.

   Now we are in the situation that d divides $n + k$ and d divides k (recall that d is the greatest common divisor of n and k and therefore certainly a divisor of k). By the definition of the greatest common divisor, it follows that d must be less than or equal to the greatest common divisor of $n + k$ and k. This greatest common divisor is 1, so we conclude that $d \leq 1$.

   We finally recall from above that since d is a greatest common divisor, $d \geq 1$. Since $d \geq 1$ and $d \leq 1$, it follows that $d = 1$, so $(n, k) = 1$.

   We now do the other direction, and assume that $(n, k) = 1$. Let $d = (k, n + k)$. Again we note that $d \geq 1$ since it is a greatest common divisor. We show that d divides n. Indeed, since d is a common divisor of k and $n + k$, there are integers s and t[1] such that $k = sd$ and $n + k = dt$. Therefore we have

   $$n = (n + k) - k = dt - ds = d(t - s),$$

[1] Warning: This is not the same t as before! Whenever we say "there exist" or "there are" we might be conjuring new quantities (or not).

again using the distributive property of integers. Since a difference of integers is an integer, d divides n.

We now conclude similarly as above: d is a common divisor of k and n, and therefore $d \leq (k, n) = 1$. Since at the same time $d \geq 1$ since it is a greatest common divisor, we conclude that again $d = (k, n + k) = 1$.

3. Suppose that $a|b$ and $a > 0$. Then since $a|a$ (because $a = 1 \cdot a$ and 1 is an integer), certainly a is a common divisor of a and b.

   Suppose now that c is any common divisor of a and b. Then in particular c is a divisor of a. As was shown in class, then c is bounded above by $|a|$, i.e., $c \leq |a|$. Since $a > 0$, it follows that $c \leq a$.

   Since a is a common divisor of a and b and any other common divisor of a and b is less than or equal to a, we may conclude that a is the greatest common divisor of a and b.

4. For simplicity, let $d = (a, b)$, where here we use the greatest common divisor definition from the book. By Theorem 4, there are integers x and y such that

$$d = ax + by.$$

   Now let c be a common divisor of a and b. In other words, there exist integers r and s such that $a = rc$ and $b = sc$. Substituting this into the equation above, we obtain

$$d = (rc)x + (sc)y = c(rx + sy),$$

   and since $rx + sy \in \mathbb{Z}$ because r, x, s and y are all integers, it follows that $c|d$.