Steven Rosendahl
Homework 2

1. Calculate $gcd(5,7)$ and find two pairs of integers (u,v) such that $gcd(5,7) = 5u + 7v$.

   By the definition of the gcd, we have that $gcd(5,7) = 1$.

$$5(3) + 7(-2) = 1$$
$$5(10) + 7(-7) = 1$$

2. Show that $c|a$ and $c|b$ if and only if $c|gcd(a,b)$.

   Assume $c|a$ and $c|b$. Then c is a common factor of a and b. We know that $gcd(a,b)$ is also a common factor of both a and b. Since both $gcd(a,b)$ and c are common factors of a and b, then they must also be common factors of each other. Therefore, $c|gcd(a,b)$.

   Let $d = gcb(a,b)$, and assume that $c|d$. Then $d = cn$ for some $n \in \mathbb{Z}$. By the definition of gcd, we know that $d|a$. Therefore, $cn|a$, which means that $a = cnm$ for some $m \in \mathbb{Z}$. Then $a = cj$, where $j = nm \in \mathbb{Z}$. Therefore $c|a$. We also know that $d|b$ by the definition of gcd. By the same argument, we know that $c|b$ as well. Therefore $c|b$ and $c|a$.

   $\triangle$

3. Suppose $a_1, a_2, \ldots, a_n$ are integers not all equal to 0. We define $gcd(a_1, a_2, ..., a_n)$ to be the largest integer which divides a_k for all $1 \leq k \leq n$. Prove that $gcd(a_1, a_2, \ldots, a_n) = gcd(gcd(a_1, a_2), a_3, ..., a_n)$.

   Let $gcd(a_1, a_2, \ldots, a_n) = d$ and $gcd(gcd(a_1, a_2), a_3, \ldots, a_n) = \alpha$. We know that, by the definition of gcd, that $d|a_k$ for $1 \leq k \leq n$. We know that $d|a_1$ and $d|a_2$, so it must also divide $gcd(a_1, a_2)$. Therefore, $d|gcd(gcd(a_1, a_2), a_3, \ldots, a_n)$, so $d|\alpha$. We also know that $\alpha|gcd(a_1, a_2)$, and that $\alpha|a_k$ for $2 < k \leq n$. Since α divides $gcd(a_1, a_2)$, it must divide a_1 and a_2. Therefore $\alpha|a_k$ for $1 \leq k \leq n$, so $\alpha|gcd(a_1, a_2, \ldots, a_n)$, or $\alpha|d$. We know that if $d|\alpha$ and $\alpha|d$, then $|d| = |\alpha|$. In this case, both α and d are positive, so we know that $\alpha = d$.

   $\triangle$

4. Use your answer to the previous problem, along with the Euclidian Algorithm, to determine $gcd(1092, 1155, 2002)$ (It's possible that you'll need a calculator to do the arithmetic on this problem).

$$1155 = 1(1092) + 63$$
$$1092 = 17(63) + 21$$
$$63 = 3(21) + 0$$
$$\therefore gcd(1155, 1092) = gcd(21, 0) = 21$$
$$2002 = 95(21) + 7$$
$$21 = 3(7) + 0$$
$$\therefore gcd(21, 2002) = gcd(7, 0) = 7$$

5. Let $a_1, a_2, \ldots, a_n \in \mathbb{N}$ and consider the two following definitions:

   - We say that $a_1, a_2, \ldots, a_n$ are relatively prime if $gcd(a_1, a_2, \ldots, a_n) = 1$.
   - We say that $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $gcd(a_i, a_j) = 1$ for all $i \neq j$.

   (a) If $a_1, a_2, \ldots, a_n$ are pairwise relatively prime can we conclude that $a_1, a_2, \ldots, a_n$ are relatively prime? Either prove your answer or give a counterexample.

   Let $(a_n) = (a_1, a_2, \ldots, a_n)$, and assume (a_n) is pairwise relatively prime. Then for any $i, j \leq n$ we have that $gcd(a_i, a_j, =)1$. This means that if we take any to distinct elements in (a_n), they will have no common factors except for 1. As a result, the greatest common factor is 1, or $gcd((a_n)) = 1$, which is the definition of begin relatively prime.

$\triangle$

(b) If $a_1, a_2, \ldots, a_n$ are relatively prime can we conclude that $a_1, a_2, \ldots, a_n$ are pairwise relatively prime? Either prove your answer or give a counterexample.

Consider $(a_n) = (2, 3, 4)$. We know that $gcd((a_n)) = 1$, but $gcd(2, 4) \neq 1$. Therefore, we can conclude that (a_n) being relatively prime does not necessarily mean that (a_n) is pairwise relatively prime.

$\triangle$

6. Suppose that $a|c$ and $b|c$. Do we necessarily have that $ab|c$? Either prove your answer or give a counterexample.

Let $a, b = 4$ and $c = 8$. We know that $4|8$, but $(4 \cdot 4) \nmid 8$. Therefore ab does not divide c.

$\triangle$

7. If $a|c$ and $b|c$ prove that $lcm(a, b)|c$. Conclude that if a and b are relatively prime, then $ab|c$.

We know that since $a|c$ and $b|c$, c is a common factor of both a and b. If we assume that c is the smallest common factor of both a and b, then $c = lcm(a, b)$, and $c|c$. Otherwise, let $\delta = lcm(a, b)$. Then, by the definition of the lcm, we know that δ is a common factor of a and b, and that $\delta < c$. Since both c and δ are common factors of a and b, it follows that $\delta|c$.

Since a and b are relatively prime, $gcd(a, b) = 1$. We also know that $ab = lcm(a, b)\, gcd(a, b)$, which means that $ab = lcm(a, b)$. Therefore, $ab|c$.

$\triangle$