Math 255 - Spring 2017
Homework 3 Solutions

1. First note that for the equality to really be true, we would need to write

$$|ab| = \operatorname{lcm}(a, b) \gcd(a, b).$$

This is because both $\operatorname{lcm}(a, b)$ and $\gcd(a, b)$ are defined to be positive, whereas a and b could be negative. (The problem arises when exactly one of a or b is negative.) To avoid this small sign problem, we assume that a and b are positive, which will prove even the correct assertion above because

$$\operatorname{lcm}(a, b) = \operatorname{lcm}(|a|, |b|) \quad \text{and} \quad \gcd(a, b) = \gcd(|a|, |b|).$$

We consider the quantity

$$\frac{ab}{\gcd(a, b)}$$

and show that it is the least common multiple of a and b. This will prove the claim.

By definition of the greatest common divisor, there are $r, s \in \mathbb{Z}$ such that

$$a = \gcd(a, b)r \quad \text{and} \quad b = \gcd(a, b)s.$$

We note here that $\gcd(b, r) = 1$ (if this were not the case $\gcd(a, b)\gcd(b, r)$ would be a common divisor of a and b which is strictly greater than $\gcd(a, b)$, a contradiction). Therefore,

$$\frac{ab}{\gcd(a, b)} = \gcd(a, b)rs.$$

From this we may conclude that $\frac{ab}{\gcd(a,b)}$ is a multiple of both a and b, since

$$\frac{ab}{\gcd(a, b)} = as \quad \text{and} \quad \frac{ab}{\gcd(a, b)} = br.$$

We now show that it is the smallest positive integer that is a multiple of a and b. Let m be another positive common multiple of a and b. Because m is a multiple of a, there is $t \in \mathbb{Z}$ such that

$$m = at,$$

and therefore we may write

$$m = \gcd(a, b)rt.$$

Because m is also a multiple of b by assumption, we have that b divides $\gcd(a, b)rt$. Because $\gcd(b, r) = 1$, as remarked above, we can conclude that b divides $\gcd(a, b)t$.

Therefore, because all of the integers in this problem are positive, we have

$$\begin{aligned} b &\leq \gcd(a,b)t \\ br &\leq \gcd(a,b)rt \\ \frac{ab}{\gcd(a,b)} &\leq m. \end{aligned}$$

Since $\frac{ab}{\gcd(a,b)}$ is smaller than any other positive multiple of a and b, it must be $\operatorname{lcm}(a,b)$ and the claim is proved.

2. This follows immediately from the transitive property of "divides:"
Since $\gcd(a,b)|a$ and $a|\operatorname{lcm}(a,b)$, it follows that $\gcd(a,b)|\operatorname{lcm}(a,b)$.

3. We begin by proving that $\gcd(a+b, a-b)$ is a common divisor of $2a$ and $2b$, from which we conclude that

$$\gcd(a+b, a-b) \leq \gcd(2a, 2b).$$

We then show that

$$\gcd(2a, 2b) = 2\gcd(a, b).$$

After this we are done since

$$\gcd(a+b, a-b) \leq \gcd(2a, 2b) = 2\gcd(a, b) = 2.$$

Since $\gcd(a+b, a-b)$ is a positive integer by definition, it follows that $\gcd(a+b, a-b) = 1$ or 2.

We first prove our first claim. Recall that $\gcd(a+b, a-b)$ divides any integer linear combination $(a+b)x + (a-b)y$ of $a+b$ and $a-b$. If we choose $x = y = 1$, we get

$$(a+b)x + (a-b)y = (a+b) + (a-b) = 2a.$$

Therefore $\gcd(a+b, a-b)$ divides $2a$. We now choose $x = 1$, $y = -1$ and obtain

$$(a+b)x + (a-b)y = (a+b) - (a-b) = 2b.$$

Therefore $\gcd(a+b, a-b)$ also divides $2b$. Since $\gcd(a+b, a-b)$ is a common divisor of $2a$ and $2b$,

$$\gcd(a+b, a-b) \leq \gcd(2a, 2b).$$

We now prove the second claim. To show that $2\gcd(a, b)$ is $\gcd(2a, 2b)$, we must show that $2\gcd(a, b)$ divides both $2a$ and $2b$ and that if c is another common divisor of $2a$ and $2b$, then $c \leq 2\gcd(a, b)$.

As usual, let $r, s \in \mathbb{Z}$ be such that $a = \gcd(a, b)r$ and $b = \gcd(a, b)s$. Then we have

$$2a = 2\gcd(a, b)r \quad \text{and} \quad 2b = 2\gcd(a, b)s,$$

and $2\gcd(a, b)$ is shown to divide both $2a$ and $2b$.

Now let c be a common divisor of $2a$ and $2b$. We treat the case of c even and odd separately. Let's start with c odd. In this case, $\gcd(c, 2) = 1$, and therefore $c|2a$ implies $c|a$. Similarly, $c|2b$ implies $c|b$. Therefore when c is odd, c is a common divisor of a and b, from which it follows that

$$c \leq \gcd(a, b) < 2\gcd(a, b).$$

Now consider the case of c even. Since c divides $2a$, we may choose $u \in \mathbb{Z}$ such that $2a = cu$. Dividing both sides by 2, we obtain

$$a = \frac{c}{2}u,$$

where $\frac{c}{2} \in \mathbb{Z}$ since c is even. Therefore $\frac{c}{2}$ divides a. In the same way, writing $2b = cv$ for $v \in \mathbb{Z}$ (recall that c divides $2b$ as well), we obtain

$$b = \frac{c}{2}v$$

and $\frac{c}{2}$ also divides b. Therefore $\frac{c}{2}$ is a common divisor of a and b, from which it follows that

$$\frac{c}{2} \leq \gcd(a, b)$$

or

$$c \leq 2\gcd(a, b).$$

Therefore whether c is even or odd, if it is a common divisor of $2a$ and $2b$, we obtain that $c \leq 2\gcd(a, b)$. This completes our proof that $\gcd(2a, 2b) = 2\gcd(a, b)$.

As mentioned above this completes the proof since now we have established that

$$\gcd(a + b, a - b) \leq \gcd(2a, 2b) = 2\gcd(a, b) = 2,$$

and since $\gcd(a + b, a - b)$ is a positive integer by definition, $\gcd(a + b, a - b) = 1$ or 2.

4. Let N be the number of coins, x be the number of coins in a full pile when attempting to divide into 77 piles, and y be the number of coins in each pile when the coins are divided into 78 piles. Then we have

$$N = 77x - 50 \quad \text{and} \quad N = 78y.$$

(Note that it is also acceptable to use the equation $N = 77t+27$ instead of $N = 77x-50$. However, in that case t is not the number of coins in any pile; $t = x - 1$ which is one less than the number of coins in each full pile.)

This gives us the equation

$$77x - 50 = 78y$$

or

$$77x - 78y = 50.$$

Since the greatest common divisor of 77 and 78 is 1 (consecutive integers always have a gcd of 1), this equation does have integer solutions.

We first solve the equation

$$77x - 78y = \gcd(77, 78) = 1.$$

By inspection, this has solution $x_0 = -1$ and $y_0 = -1$. Therefore the equation

$$77x - 78y = 50$$

has particular solution $x_p = -50$ and $y_p = -50$.

We may now apply our theorem to obtain that all integer solutions of the equation $77x - 78y = 50$ are

$$\begin{aligned} x &= -50 - 78t \\ y &= -50 - 77t, \end{aligned}$$

for $t \in \mathbb{Z}$.

Since x and y are quantities of coins, they both must be nonnegative. We now solve for the values of t that give $x \geq 0$ and $y \geq 0$. We first look at x only:

$$\begin{aligned} 0 \leq x &= -50 - 78t \\ 78t &\leq -50 \\ t &\leq \frac{-50}{78}. \end{aligned}$$

Since t is an integer, this implies $t \leq -1$. We now look at y only:

$$\begin{aligned} 0 \leq y &= -50 - 77t \\ 77t &\leq -50 \\ t &\leq \frac{-50}{77}. \end{aligned}$$

Since t is an integer, this implies $t \leq -1$. Thankfully it is easy to reconcile the conditions given by x and y: If $t \leq -1$ and $t \leq -1$, then $t \leq -1$!

Now this means that any value of t that is $-1, -2, -3, -4 \ldots$ will give a valid solution to the problem. Therefore, the best solution to the problem is "The number of coins I have is any of the following:

$$N = 78(-50 - 77t) = 6006t - 3900, \quad \text{where } t \text{ is any negative integer,"}$$

but $N = 2106$ (this is N when $t = -1$) or any other one of the valid answers will be accepted for full credit.