MATH 3320, HOMEWORK #1 – SOLUTIONS

1.

(a) (5 points) Use the Euclidean algorithm to find $\gcd(1287, 403)$.

Solution: We apply the Euclidean algorithm:

$$1287 - 3(403) = 78$$
$$403 - 5(78) = 13$$
$$78 - 6 * 13 = 0$$

Since 13 was our last non-zero value in our algorithm, $\gcd(1287, 403) = 13$.

(b) (10 points) Find all the integer solutions of $1287x + 403y = 104$.

Solution: We apply back substitution to the above sequence of equations to find successive ways of expressing 13:

$$13 = 1(403) - 5(78)$$
$$13 = 1(403) - 5(1287 - 3(403)) = 16(403) - 5(1287)$$

Notice that we do not use the final equation of the Euclidean algorithm (which had merely signaled that we were done). We start with the second-to-last equation, which will have the gcd, 13, as its right-hand side.

2.

(a) (5 points) Give a definition for the greatest common divisor of three integers a, b, c.

Answer: $\gcd(a, b, c) = \max\{d \in \mathbb{N} : d|a, d|b, d|c\}$.

(b) (15 points) Prove that $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$ for any integers a, b, c.

Answer: Let $d = \gcd(a, b, c)$.

$d|a,\ d|b \ \Rightarrow\ d|\gcd(a, b)$.

$d|\gcd(a, b),\ d|c \ \Rightarrow\ d|\gcd(\gcd(a, b), c) \ \Rightarrow\ d \leq \gcd(\gcd(a, b), c)$.

On the other hand, $\gcd(\gcd(a, b), c)|\gcd(a, b)|a, b$, and $\gcd(\gcd(a, b), c)|c$. So $\gcd(\gcd(a, b), c) \leq d$.

Therefore, $d = \gcd(\gcd(a, b), c)$.

Comment: The only proposition you can use about $\gcd(a, b, c)$ is from your definition in (a). The corollaries of $\gcd(a, b, c)$ similar to those of $\gcd(a, b)$ cannot be used without proof.

(c) (5 points) Use the Euclidean algorithm to find the greatest common divisor of 408, 884, and 1071.

Answer: $\gcd(408, 884, 1071) = \gcd(\gcd(408, 884), 1071)$.

$$884 = \mathbf{408} * 2 + \mathbf{68}$$
$$408 = \mathbf{68} * 6$$

So $\gcd(408, 884) = 68$.

$$1071 = \mathbf{68} * 15 + \mathbf{51}$$
$$68 = \mathbf{51} + \mathbf{17}$$
$$51 = \mathbf{17} * 3$$

$\gcd(408, 884, 1071) = \gcd(68, 1071) = \mathbf{17}$.

(d) (10 points) Do there exist integers x, y, z such that $408x + 884y + 1071z = 123$? (Hint: You don't have to solve the equation.)

Answer: No, because $17 = \gcd(408, 884, 1071)|408x + 884y + 1071z$, but 17123.

3. (10 points) Find all the integer solutions of $6x + 15y + 10z = 8$.

Solution 1: We see by inspection that $(x, y, z) = (-2, 0, 2)$ is a (particular) solution of the equation. Now let (x', y', z') be an arbitrary solution. Observe that the difference $(x_0, y_0, z_0) = (x' - (-2), y' - 0, z' - 2)$ is a solution to the equation $6x_0 + 15y_0 + 10z_0 = 0$, since $6x_0 + 15y_0 + 10z_0 = 6(x' - (-2)) + 15(y' - 0) + 10(z' - 2) = (6x' + 15y' + 10z') - (6(-2) + 15(0) + 10(2)) = 8 - 8 = 0$.

Next we move $10z_0$ to the right-hand side, to obtain $6x_0 + 15y_0 = -10z_0$. Observe that, if we choose x_0 and y_0 to be any integers, then the possible values for the left-hand side are precisely multiples of $\gcd(6, 15) = 3$. Let us thus write the right-hand side as $3w_0$. Now, collapsing the first two terms into one, our equation becomes $3w_0 + 10z_0 = 0$. If we introduce an integer parameter n, we may write the solutions of this equation as $(w_0, z_0) = (10n, -3n)$. Now, going back to our variables x_0 and y_0, we have $6x_0 + 15y_0 = 30n$. Considering n as fixed, we can find by inspection that $(x_0, y_0) = (0, 2n)$ is a valid solution. Thus the totality of solutions of this last equation is given by $(x_0, y_0) = (5m, -2m + 2n)$ where m is an additional parameter. Thus $(x_0, y_0, z_0) = (5m, -2m + 2n, -3n)$ are the solutions to $6x_0 + 15y_0 + 10z_0 = 0$, where m and n are integer parameters, and so our initial equation has $(x, y, z) = (-2 + 5m, -2m + 2n, 2 - 3n)$ as its solutions (obtained by adding our particular solution to the general solution of the homogeneous equation).

Solution 2: Observe that we may take the vector $\begin{bmatrix} 6 & 15 & 10 \end{bmatrix}$ consisting of the coefficients of our equation and perform on it a generalization of the Euclidean algorithm to three numbers, by means of multiplying on the right by invertible matrices. Our first matrix

$$\begin{bmatrix} 1 & -2 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

has the effect of subtracting 2(6) from 15 and 1(6) from 10, to yield the vector $\begin{bmatrix} 6 & 3 & 4 \end{bmatrix}$. The second matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

subtracts 2(3) from 6 and 1(3) from 4, so we are left with $\begin{bmatrix} 0 & 3 & 1 \end{bmatrix}$. Finally, we take the matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3 & 1 \end{bmatrix},$$

which gives us $\begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$. Since the gcd of the (three) numbers is preserved at each step, we must in fact eventually reach a vector having one entry equal to the gcd and the rest zero–as has happened here.

Suppose now that we had started with an equation where the coefficients were given by $\begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$. Then it would be easy to find the set of all solutions: Just take the column vector $\begin{bmatrix} m & n & 8 \end{bmatrix}^T$, where m and n are integer parameters. It is easy to check that this gives us precisely the set of column vectors whose dot product with our row vector is 8, and thus that it describes the solutions to our congruence.

The reality, of course, is that our equation has coefficients given by $\begin{bmatrix}6 & 15 & 10\end{bmatrix}$. But the much nicer $\begin{bmatrix}0 & 0 & 1\end{bmatrix}$ may be written as

$$\begin{bmatrix}6 & 15 & 10\end{bmatrix}\begin{bmatrix}1 & -2 & -1\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\-2 & 1 & -1\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & -3 & 1\end{bmatrix}.$$

Thus

$$\left(\begin{bmatrix}6 & 15 & 10\end{bmatrix}\begin{bmatrix}1 & -2 & -1\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\-2 & 1 & -1\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & -3 & 1\end{bmatrix}\right)\begin{bmatrix}m\\n\\8\end{bmatrix}=8.$$

Multiplying the column vector on the right through the matrices yields

$$\begin{bmatrix}6 & 15 & 10\end{bmatrix}\begin{bmatrix}5m-5n+8\\-2m+4n-8\\-3n+8\end{bmatrix}=8.$$

Since all our matrices were invertible, the map

$$\begin{bmatrix}m\\n\\8\end{bmatrix}\mapsto\begin{bmatrix}5m-5n+8\\-2m+4n-8\\-3n+8\end{bmatrix}$$

takes solutions of $0x+0y+1z=8$ to solutions of $6x+15y+10z=8$ in a one-to-one and onto manner (i.e. bijectively). Thus $\begin{bmatrix}5m-5n+8 & -2m+4n-8 & -3n+8\end{bmatrix}^T$ specifies all the integer solutions of $6x+15y+10z=8$.

Note: There is more than one way to parametrize the solution sets, as the answers given by the above two methods illustrate. Can you see how they relate to one another?

4. (15 points) Determine the number of *positive* integer solutions of $2x+3y=300$.

Answer: $3y=300-2x=2(150-x)$, so $2|3y$. Because $(2,3)=1$, we have $2|y$. Similarly, $3|x$.

Let $x=3a$, $y=2b$. $6a+6b=300 \Rightarrow a+b=50$. a,b should be positive integers, and there are **49** combinations: $a=1,2,\cdots,49$, and $b=49,48,\cdots,1$.

Comment: The corner cases $(a,b)=(0,50)$ and $(50,0)$ should be excluded, and you should **explicitly** give the number of combinations.

5. Recall that the Fibonacci seqeucne $\{F_n\}_{n\geq 1}$ is defined by the recurrence relation

$$F_{n+2}=F_{n+1}+F_n$$

for $n\geq 1$, with initial values $F_1=1$ and $F_2=1$.

(a) (10 points) Find $\gcd(F_{n+2},F_n)$.

Solution: We start with a lemma.

Lemma: $\gcd(F_{n+1},F_n)=1$

We prove this for all $n\geq 1$ by induction. The base case is trivial: $\gcd(F_2,F_1)=\gcd(2,1)=1$. Now suppose the claim is true for $n=k\geq 1$. That is, $\gcd(F_{k+1},F_k)=1$. We may write

$$\gcd(F_{k+2},F_{k+1})=\gcd(F_{k+1}+F_k,F_{k+1})=\gcd(F_k,F_{k+1})=\gcd(F_{k+1},F_k)=1,$$

using the property $\gcd(a+b,b)=\gcd(a,b)$. This proves the lemma.

Now we have $\gcd(F_{n+2},F_n)=\gcd(F_{n+1}+F_n,F_n)=\gcd(F_{n+1},F_n)$, as required.

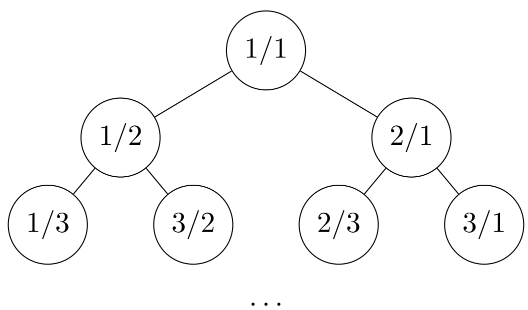
(b) (10 points) Show that $\gcd(F_{n+3},F_n)=\gcd(F_n,2)$ for $n\geq 1$.

Solution: We first note that $F_{n+3}=F_{n+2}+F_{n+1}=(F_{n+1}+F_n)+F_{n+1}=2F_{n+1}+F_n$. Thus $\gcd(F_{n+3},F_n)=\gcd(2F_{n+1}+F_n,F_n)=\gcd(2F_{n+1},F_n)$. Recall that by our lemma for part (a), F_{n+1} and F_n are relatively prime. It follows that, if a divisor d of F_n divides $2F_{n+1}$, then it must divide 2 (as d is relatively prime to F_{n+1}). Thus the only possible (positive) common divisors of $2F_{n+1}$ and F_n are 1 and 2. It follows that $\gcd(2F_{n+1}, F_n)$ must be either 1 or 2. In particular $\gcd(2F_{n+1}, F_n) = 2$ if $2|F_n$, and $\gcd(2F_{n+1}, F_n) = 1$ otherwise. But $\gcd(F_n, 2)$ is of course equal to 2 if F_n is even and equal to 1 otherwise. Hence $\gcd(2F_{n+1}, F_n) = \gcd(F_n, 2)$ in both circumstances.

(c) (5 points) Use (b) to prove that F_{3m} is an even number for $m \geq 1$.

Solution: We prove this by induction. For the base case $m = 1$, we have $F_{3m} = F_3 = 2$, hence even. Suppose that F_{3k} is even for some $k \geq 1$. Then $\gcd(F_{3k+3}, F_{3k}) = \gcd(F_{3k}, 2) = 2$. Hence 2 is a common divisor of F_{3k+3} and F_{3k}, so in particular F_{3k+3} must be even. This completes the proof.

6. (Extra Credit) Consider a binary tree obtained by starting with the fraction $1 = \frac{1}{1}$ and iteratively adding $\frac{a}{a+b}$ and $\frac{a+b}{b}$ below each fraction $\frac{a}{b}$ as "children". For example, the top of such a tree looks like this:



and keeps on going. It is infinitely long and infinitely wide, and every node corresponds to a rational number.

Prove the following properties of this tree:

(a) (10 points) Every fraction in this tree is in reduced form (i.e. its denominator and numerator are relatively prime).

Answer: Every fraction a/b in this tree satisfies $a \geq 1, b \geq 1$, therefore $a + b \geq 2$. So we use induction to prove every fraction is in reduced form:

1) If $a + b = 2$, then the only case is $a = 1, b = 1$. It is obvious a/b is in reduced form.
2) If for all fraction a/b in the tree where $2 \leq a + b \leq n$, a/b is in reduced form, then for any node a/b where $a + b = n + 1$, suppose its parent node is c/d, we have
   i if a/b is the left child, then $a = c, b = c + d$. Thus $c = a, d = b - a$. $c + d = b < a + b = n + 1$. So $\gcd(c, d) = 1$, and $\gcd(a, b) = \gcd(c, c + d) = \gcd(c, d) = 1$.
   ii if a/b is the right child, then $a = c + d, b = d$. Similarly, we can prove $\gcd(a, b) = \gcd(c, d) = 1$.

By induction, every node is in reduced form.

(b) (20 points) Every positive rational number appears exactly once in this tree.

Answer: We use induction to prove every positive reduced fraction a/b appears exactly once in the tree.

1) There is only one reduced fraction $a/b = 1/1$ satisfying $a + b = 2$, and it appears once in the tree.
2) If every reduced fraction a/b where $2 \leq a + b \leq n$ appears exactly once in the tree, then for any reduced fraction a/b where $a + b = n + 1$, we have $a \neq b$. Otherwise, it is not reduced. Then there are two cases:
   i $a < b$.
   We have $\gcd(a, b - a) = \gcd(a, b) = 1$. So $a/(b - a)$ is in reduced form. In addition, $2 \leq a + (b - a) = b \leq n$. According to our assumption, $a/(b - a)$ is in the tree. We can verify a/b is the left child of $a/(b - a)$.

On the other hand, suppose c/d has a/b as its child. Then a/b has to be the left child. $a = c, b = c + d$. Solving them we get $c = a, d = b - a$. Therefore, $a/(b-a)$ is the unique parent of a/b.

ii $a > b$. We can prove it in a similar way. a/b has to be a right child, and its parent is $(a-b)/b$.

By induction, every reduced form fraction appears exactly once in the tree.

Comment: In (b), do not forget to show that $a/(b-a)$ or $(a-b)/b$ is in reduced form.