Math 331: Homework Due Sept 23

1. Given a and b below, use the Euclidean algorithm to find $d = \gcd(a, b)$. Find n and m so that $d = am + bn$.

   (a) $a = 2322, b = 654$

   (b) $a = 1536, b = 1152$

2. Determine if the set

$$J = \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} : a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$$

   is a subring, ideal, both or neither. Justify your answer.

   Solution: There are lists of things to check but here are the main points for showing that J is a subring.

   - It is pretty clear that if $A, B \in J$ then $A \pm B \in J$.
   - If $A = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \in J$ and $B = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \in J$ then $AB = \begin{pmatrix} a^2 + ab & a^2 + ab \\ ab + b^2 & ab + b^2 \end{pmatrix} \in J$.

   J is not an ideal, which can be shown by finding an element in $A \in J$ and an element in $B \in R$ such that $AB \notin J$. Here are two such elements:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \notin J$$

3. Determine if the set

$$J = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$$

   is a subring, ideal, both or neither. Justify your answer.

   Solution: Again we have a list of things to check. If $A = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \in J$ and $B = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in J$ then it is easy to see that $A + B \in J$ and $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in J$. Thus, J will be a subring (yes, there are more things to check, but these are the main issues).

   To see that J is not an ideal, here is an $A \in J$ and an element in $B \in R$ such that $AB \notin J$:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \notin J$$

4. Prove that a and b are relatively prime integers if and only if $1 \in I(a,b)$.

   Solution: This was essentially proved in class.

   In class we proved that $I(a,b) = \gcd(a,b)\mathbb{Z}$.

   Thus, if $\gcd(a,b) = 1$ then we have $I(a,b) = \mathbb{Z}$ and therefore $1 \in I(a,b)$.

   If $1 \in I(a,b)$ then notice that the smallest positive integer in $\gcd(a,b)\mathbb{Z}$ is $\gcd(a,b)$. Thus, $1 = \gcd(a,b)$.

5. Prove that p is prime and $a \neq 0$ then then either p divides a or p and a are relatively prime.

   Solution: The only numbers that divide p are 1 and p, thus we must have either $\gcd(a,p) = 1$ (in which case a, p are relatively prime) or else $\gcd(a,p) = p$ (in which case $p|a$).

6. The least common multiple of two nonzero integers a and b, denoted by $\text{lcm}(a,b)$, is a nonnegative integer m such that both a and b divide m, and if a and b both divide any other integer n, then m also divides n.

   Prove that any two integers a and b have a unique least common multiple.

   Solution: Uniqueness: Suppose n and m are both least common multiples. Since they are both least common multiples, we must have both $n|m$ and $m|n$ and therefore (by a theorem in text) we must have $n = m$.

   Existence: Let $A = \{x \in \mathbb{N} : a|x \text{ and } b|x\}$. A is not empty ($|ab| \in A$) and therefore there is a smallest element of A, call it m. Since $m \in A$, $a|m$ and $b|m$. Suppose n is such that $a|n$ and $b|n$ (we need to show that $m|n$). Divide $nbym$: $n = mq + r$ with $0 \leq r < m$. Then $r = n - mq$. Since $a|n$ and $a|m$ we must also have $a|r$. Similarly, $b|r$ and this forces $r = 0$ (why?). Therefore $m|n$ and we are done.

7. If $d = \gcd(a,b)$ and $m = \text{lcm}(a,b)$, prove that $dm = |ab|$.

   Solution: This can be a bit tricky and there are several approaches. My preference is to not use unique factorization into primes (since we haven't talked about that yet). Here is an outline of one approach (you can fill in the details).

   Lets assume that $a, b > 0$ so we don't have to worry about absolute values.

   (i) If $\gcd(a,b) = 1$ then $\text{lcm}(a,b) = ab$.

   Proof. Since $a|m$ we have $m = au$ for some u. Since m is the lcm we have $m = au \leq ab$ and thus $u \leq b$.

   $b|m$ so therefore $b|au$. Since $\gcd(a,b) = 1$ we must have $b|u$ and therefore $b \leq u$.

   Putting these together gives $b = u$ and $m = ab$. □

   (ii) For any integers $a, b, u > 0$ we have $\text{lcm}(au, bu) = u\text{lcm}(a,b)$.

   Let $n = \text{lcm}(au, bu)$. Show that mu is a common multiple of au and bu and therefore $n \leq mu$. Now show that (n/u) is a common multiple of a and b and therefore $(n/u) \geq m$.

(iii) Now so that that $\text{lcm}(a,b)\gcd(a,b) = ab$.

Write $a = dx$ and $b = dy$ for some x, y. Note that $\gcd(x,y) = 1$ (why?). From the previous work, we have

$$\gcd(a,b)\text{lcm}(a,b) = d\text{lcm}(dx,dy) = d \cdot d\text{lcm}(x,y) = d^2xy = (dx)(dy) = ab$$

8. Show that $\text{lcm}(a,b) = ab$ if and only if $\gcd(a,b) = 1$.

Solution: Use previous problem.

9. Let $a, b, c \in \mathbb{Z}$. Prove that $\gcd(a,c) = \gcd(b,c) = 1$ if and only if $\gcd(ab,c) = 1$.

Solution: If $\gcd(ab,c) = 1$ then we can write $abx + cy = 1$ for some xy. But, this says that $a(bx) + cy = 1$ which shows that $\gcd(a,c) = 1$. Similarly, we have $b(ax) + cy = 1$ which shows that $\gcd(b,c) = 1$.

Now assume that $\gcd(a,c) = \gcd(b,c) = 1$. Thus we have, for some u, v, x, y:

$$1 = au + cv = bx + cy$$

Multiplying these

$$1 = (au + cv)(bx + cy) = ab(ux) + (auy + bvx + cvy)c$$

and thus $\gcd(ab,c) = 1$.