MATH 333 — MIDTERM EXAM 1

March 9, 2016

NAME: Solutions

1. Do not open this exam until you are told to begin.
2. This exam has 11 pages including this cover. There are 7 problems.
3. Write your name on the top of EVERY sheet of the exam at the start of the exam!
4. If you separate pages of this exam and include additional pages, please be sure to staple them in the correct order before turning the exam in.
5. You may quote major theorems, but nothing that trivializes a problem.

PROBLEM	POINTS	SCORE
1	10	
2	10	
3	15	
4	20	
5	20	
6	15	
7	10	
TOTAL	100	

1. (10 points) Find the greatest common divisor of 137 and 825. Express the greatest common divisor as a linear combination of 137 and 825.

We use the Euclidean algorithm here:

$$\begin{aligned} 825 &= 137(6) + 3 \\ 137 &= 3(45) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2). \end{aligned}$$

Thus, $\gcd(137, 825) = 1$. We substitute to find a linear combination of 137 and 825 that gives 1:

$$\begin{aligned} 1 &= 3 + 2(-1) \\ &= 3 + (-1)(137 + 3(-45)) = 3(46) + 137(-1) \\ &= 46(825 + 137(-6)) + 137(-1) \\ &= 825(46) + 137(-277). \end{aligned}$$

2. (10 points) Write out addition and multiplication tables for $\mathbb{Z}/5\mathbb{Z}$. (You can write a instead of $[a]_5$ as it is clear from context what you mean.) What are the units in $\mathbb{Z}/5\mathbb{Z}$? What are the zero divisors in $\mathbb{Z}/5\mathbb{Z}$?

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

From the tables we see there are no zero divisors in $\mathbb{Z}/5\mathbb{Z}$ and the elements $1, 2, 3, 4$ are all units.

3. (10 + 5 points)

   (a) Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$. Prove that if $\gcd(a,n) = 1$ there is a solution to the equation $ax \equiv 1 \pmod{n}$.

Proof. The fact that $\gcd(a,n) = 1$ implies there exists integers x, y so that $ax + ny = 1$. Considering this equation modulo n gives

$$ax \equiv 1 \pmod{n},$$

which is what we were trying to prove. □

   (b) Let $a = 137$ and $n = 825$. Find a solution to the equation $137x \equiv 1 \pmod{825}$.

We saw in problem 1 that $825(46) + 137(-277) = 1$. Thus, $x = -277 \equiv 558 \pmod{825}$ is a solution.

4. (10 points each) Define a function $f : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ by $f(x) = 2x$.

   (a) Is f injective? Be sure to justify your answer.

Proof. The function is not injective. One can never have a function from an infinite set to a finite set be injective. In particular, we see here that $f(0) = [0]_6 = f(3)$ but $0 \neq 3$. □

   (b) Is f surjective? Be sure to justify your answer.

Proof. To say f is surjective means each element in $\mathbb{Z}/6\mathbb{Z}$ is in the image of f. Suppose that $[1]_6 = [2x]_6$ for some $x \in \mathbb{Z}$. This gives that $[1]_6 = [2]_6[x]_6$. This would give that $[2]_6$ is a unit, which it is not. Another way to see this cannot happen is to observe if there is such an x, then multiplying both sides of the equation by $[3]_6$ we have $[3]_6 = [3]_6[2]_6[x]_6 = [0]_6[x]_6 = [0]_6$, but $[3]_6 \neq [0]_6$ so we have a contradiction. □

5. (10 points each)

   (a) Let p be a prime and $a, b \in \mathbb{Z}$. Prove that if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Let $p \mid ab$, i.e., there exists an integer c so that $pc = ab$. If $p \mid a$ we are done, so assume $p \nmid a$. Since p is prime this gives $\gcd(a,p) = 1$. Thus, there are integers m, n so that $1 = am + pn$. Multiplying both sides of this equation by b we obtain $b = abm + bpn$. Replacing ab with pc we obtain $b = pcm + bpn = p(cm + bn)$. Thus, $p \mid b$ as desired. □

(b) Let p be a prime and $a_1, \dots, a_n \in \mathbb{Z}$. Prove that if $p \mid a_1 \cdots a_n$ then $p \mid a_j$ for some $1 \leq j \leq n$.

Proof. We prove this by induction on n. The case $n = 1$ is obvious and the case $n = 2$ is part (a), so our base case is done. Assume the result is true for some $k \in \mathbb{Z}_{\geq 1}$, i.e., if $p \mid a_1 \dots a_k$ then $p \mid a_j$ for some j with $1 \leq j \leq k$. Now suppose that $p \mid a_1 \dots a_k a_{k+1}$. This can be rewritten as $p \mid (a_1 \cdots a_k) \cdot a_{k+1}$. Applying the base case of $n = 2$ gives that $p \mid a_1 \cdots a_k$ or $p \mid a_{k+1}$. If $p \mid a_{k+1}$ we are done, so assume $p \mid a_1 \dots a_k$. We now apply our induction hypothesis to conclude that $p \mid a_j$ for some j with $1 \leq j \leq k+1$. Thus, the result follows by induction. $\square$

6. (10 + 5 points)

(a) Let p be a prime number and $1 \leq k \leq p-1$ an integer. Recall that $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is an integer. Prove that $\left[\binom{p}{k}\right]_p = [0]_p$. (You are not allowed to quote a homework problem that makes this trivial!)

Proof. We have that $\binom{p}{k} \in \mathbb{Z}$, i.e., $\binom{p}{k} = c$ for some $c \in \mathbb{Z}$. This gives $p! = k!(p-k)!c$. Our goal is to show that $p \mid c$. Observe that since p is prime and $p \mid ck!(p-k)!$ we have $p \mid c$ or $p \mid k!(p-k)!$. However, since we assume that $1 \leq k \leq p-1$ we have $\gcd(p, k!) = 1$ and similarly $\gcd(p, (p-k)!) = 1$. Thus, $p \mid c$. $\square$

(b) Recall that $(x+y)^k = \displaystyle\sum_{j=0}^{k} \binom{k}{j} x^j y^{k-j}$. Use this to prove the "freshmen's dream" that $([a]_p + [b]_p)^p = [a]_p^p + [b]_p^p$ for all $a, b \in \mathbb{Z}$. (Do you see why a "freshmen" wishes this was true in general?)

Proof. We have

$$
\begin{aligned}
([a]_p + [b]_p^p &= \sum_{k=0}^{p} \left[\binom{p}{k}\right]_p [a]_p^k [b]_p^{p-k} \\
&= \left[\binom{p}{0}\right]_p [b]_p^p + \left[\binom{p}{p}\right]_p [a]_p^p \\
&= [a]_p^p + [b]_p^p
\end{aligned}
$$

where the second equality follows because in $\mathbb{Z}/p\mathbb{Z}$ we have $\left[\binom{p}{k}\right]_p = [0]_p$ for all $1 \leq k \leq p-1$ by part (a).

This is a dream because many students often forget to "foil" and treat the middle terms as if they do not exist. $\square$

7. (10 points) Let $a, b \in \mathbb{Z}$ and let $c \in \mathbb{Z}_{>1}$. Prove that $\gcd(ac, bc) = c \cdot \gcd(a, b)$.

Proof. Let $d = \gcd(ac, bc)$ and $e = \gcd(a, b)$. Observe since $e \mid a$ and $e \mid b$, we have $ce \mid ac$ and $ce \mid bc$. Since ce is a common divisor of ac and bc and d is the greatest common divisor, we must have $ce \leq d$. Write $e = am + bn$ for some $m, n \in \mathbb{Z}$. Multiplying this by c we obtain $ce = acm + bcn$. Since $d \mid ac$ and $d \mid bc$, d divides any linear combination of ac and bc. In particular, $d \mid ce$. Thus, $d \leq ce$. Since we have inequalities in each direction we must have $d = ce$ as claimed. $\square$