MAS 4203 – EXAM 1 – Spring 2016

Friday, Feb. 5

NAME: SOLUTION

Instructions: All work should be written in a proper and coherent manner, and in a way that any student in the class can follow your work. Show all necessary working and reasoning when giving proofs your reasoning should be clear. Only scientific or basic calculators are allowed.

TOTAL: 50 pts (also 2 optional bonus points)

1. [2+ (2+2+2+2) = 10 pts]

(a) Complete the definition: Let $a, b \in \mathbb{Z}$. Then

a divides b denoted $a \mid b$, if

$b = ac$ for some $c \in \mathbb{Z}$.

(b) Prove or disprove the following statements

(i) If $a \in \mathbb{Z}$ then $a \mid 0$.

Proof: Let $a \in \mathbb{Z}$. $a \mid 0$ since

$0 = a \cdot 0$ & $0 \in \mathbb{Z}$.

(ii) There are integers x, y such that

$$33x + 21y = 20.$$

$3 \mid 33$ & $3 \mid 21$ so $3 \mid 33x + 21y$ if $x, y \in \mathbb{Z}$.

$3 \nmid 20$ so the statement is FALSE.

(iii) If $a, b, c, d, e \in \mathbb{Z}$, $c \mid b$ and $a \mid c$ Then $a \mid (bd + ce)$.

Proof: Suppose $a \mid b$, $a \mid c$. Then $b = ax$, $c = ay$ for some $x, y \in \mathbb{Z}$. Then $bd + ce = axd + aye = a(xd + ye)$ & $a \mid bd + ce$ since x, d, y, e & hence $xd + ye \in \mathbb{Z}$.

(iv) If $a, b, c, d \in \mathbb{Z}$, $d \mid a$ and $d \mid b$ Then $(a, b) \mid d$. Statement is false

Let $a = 4$, $b = 8$. Then $(a, b) = 4$

But $d = 2 \mid 4$ & $d = 2 \mid 8$ but $4 \nmid 2$.

2. [2 + 6 = 8 pts]

(a) Complete the following

Proposition. Let $a, b \in \mathbb{Z}$ and suppose a and b are not both zero. Then

$$(a, b) = \text{MIN}\{ax + by : x, y \in \mathbb{Z} \text{ \& } ax + by > 0\}.$$

(b) Let $a, b, c \in \mathbb{Z}$ with $(a, b) = 1$ and $a \mid bc$.

PROVE $a \mid c$ using Prop. in (a) and NOT the Fundamental Theorem of Arithmetic.

Suppose $(a, b) = 1$. Then $ax + by = 1$ for some $x, y \in \mathbb{Z}$ by 2(a). $a \mid bc$ so $bc = ad$ for some $d \in \mathbb{Z}$.

$$c(ax + by) = c(1)$$
$$a(cx) + bcy = c,$$
$$a(cx) + ady = c \quad \text{since } bc = ad,$$
$$c = a(cx + dy) \text{ \& } a \mid c$$

since c, x, d, y & $cx + dy \in \mathbb{Z}$.

3. [3 + 3 = 6 pts]

(a) Use the Euclidean algorithm to compute (282, 76).

$$282 = (76)(3) + 54$$
$$76 = (54)\cdot(1) + 22$$
$$54 = 2(22) + 10$$
$$22 = 2(10) + 2$$
$$10 = 2\cdot 5 + 0$$

So $(282, 76) = 2$.

(b) Find integers x, y such that

$$282x + 76y = (282, 76).$$

Let $a = 282$, $b = 76$. Then

$$54 = a - 3b$$
$$22 = b - 54 = b - (a - 3b) = -a + 4b$$
$$10 = 54 - 2\cdot 22 = (a - 3b) - 2(-a + 4b)$$
$$= 3a - 11b$$
$$2 = 22 - 2\cdot 10 = (-a + 4b) - 2(3a - 11b)$$
$$= -7a + 26b.$$

So $x = -7$, $y = 26$ is a solution.

4. [2 + 4 + 3 + 5 = 14 pts]

(a) Complete the definition: p is prime (or a prime number) if $p > 1$, $p \in \mathbb{Z}$ and the only positive divisors of p are 1 & p.

(b) Use Qu. 2(b) to PROVE Euclid's Lemma

Let $a, b, p \in \mathbb{Z}$ with p prime.
If $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

PROOF: Suppose $a, b, p \in \mathbb{Z}$, p prime & suppose $p \mid ab$. The only positive divisors of p are 1 or p.
Case 1. $(a, p) = 1$. Then by Qu 2(b) $p \mid b$.
Case 2 $(a, p) = p$. Then $p \mid a$.
Hence either $p \mid a$ or $p \mid b$.

(c) Let $a, b \in \mathbb{Z}$. Prove that if a and b are expressible in the form $4n+1$, where n is an integer, then ab is also expressible in that form.

Let $a = 4n+1$, $b = 4m+1$ where $m, n \in \mathbb{Z}$. Then

$$ab = (4n+1)(4m+1) = 16mn + 4n + 4m + 1$$
$$= 4(4mn + n + m) + 1$$ which has the desired form since $m, n,$ & $4mn+n+m \in \mathbb{Z}$.

(d) Prove that there are infinitely many primes of the form $4n+3$ where n is an integer.

Suppose by way of contradiction that there are only finitely many primes of the form $4n+3$, say $p_0 = 3, p_1, p_2, \ldots, p_n$.

Let $N = 4(p_1 p_2 \cdots p_n) + 3$.

Then N is an integer > 1, & N is odd.

So any prime divisor of N has the form $4n+1$ or $4n+3$ (since $4n+2, 4n$ are even).

N must have at least one prime divisor p, of the form $4n+3$ since if all the prime divisors of N were of the form $4n+1$ part (a) would imply N would be of the form $4n+1$ & clearly it is not.

Therefore $p = p_j$ some $0 \le j \le n$ & $p \mid N$.

Case 1 $p = p_0 = 3$.

Then $p = 3 \mid N$ & $p = 3 \mid N - 3 = 2 \cdot p_1 p_2 \cdots p_n$ which is impossible since $p_0 \neq 2$ & p_j $j \ge 1$.

Case 2 $p = p_j$ some $j \ge 1$.

$p \mid N$ & $p = p_j \mid 4(p_1 p_2 \cdots p_n)$.

$\Rightarrow p \mid N - 4(p_1 p_2 \cdots p_n) = 3$ & $p = 3 = p_j$ which is impossible since $p_j \neq p_0 = 3$ for $j \ge 1$.

We have a contradiction in both cases. Hence there must be infinitely many primes of the form $4n+3$.

5. [2+4+3+3 = 12 pts]

(a) Complete the Definition. Let $m>0$, $m\in\mathbb{Z}$ & $a,b\in\mathbb{Z}$. We say a is congruent to b modulo m and write $a\equiv b \pmod m$ if $m \mid (a-b)$.

(b) Prove the following

Proposition: Let $m\in\mathbb{Z}$, $m>1$, $a,b,c,d\in\mathbb{Z}$. If $a\equiv b \pmod m$ and $c\equiv d \pmod m$ then $ac\equiv bd \pmod m$.

Proof: Suppose $a\equiv b \pmod m$ & $c\equiv d \pmod m$. Then $m\mid(a-b)$ & $m\mid(c-d)$.

$\therefore$ $m \mid c(a-b)+b(c-d)$ by 1(iii)

But $c(a-b)+b(c-d) = ac-bd$,

$m \mid ac-bd$, &

$ac\equiv bd \pmod m$.

(c) Find a prime divisor of $2^{44}+1$.

Hint: What is $x^{11}+1 = ?$ $(x+1)(1-x+x^2-+\cdots+x^{10})$

Let $x=2^4$. Then $2^{44}+1 = (2^4+1)(\underbrace{1-2^4+-\cdots+2^{40}}_{\in\mathbb{Z}})$

$\therefore$ $17 \mid (2^{44}+1)$.

(d) Show that $815^{95} - 817^{95} \equiv 6 \pmod 8$.

$816 = 8\cdot 102$. $\therefore$ $815 = 8\cdot 102 - 1 \equiv -1 \pmod 8$,

$817 = 8\cdot 102+1 \equiv 1 \pmod 8$. Therefore

$815^{95} - 817^{95} \equiv (-1)^{95} - 1^{95} \pmod 8$

$\equiv -1-1 \pmod 8$ $\equiv -2 \pmod 8$

$\equiv 6 \pmod 8$ (since $-2 = 6-8$).

6. [2 bonus points]

(a) This _ i _ _ _ _
_ _ _ e _ _ _ _ _.

(b) He went to Orléans where he studied _ _ _ at the university.

(c) He claimed that _ e _ _ _ _ _ _ s had not correctly deduced his law of r _ _ _ _ _ _ _ _ _ n

(d) He is best remembered for his "theorem" which states

_ _ + _ _ = _ _

has no non-zero integer solutions for x, y, z when $n >$ _ _.