MAS 4203 - EXAM 1 - FALL 2017

Friday, February 3, 2017

NAME: SOLUTION

1. 10
2. 8
3. 10
4. 10
5. 12

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 proof your reasoning should be clear. Only scientific or basic calculators are allowed.

TOTAL 50 + (2 bonus pts)

1. [2 + (4 × 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 $0 \mid a$.

FALSE For example $0 \nmid 1$ since $1 \neq 0 \cdot c = 0$ for any $c \in \mathbb{Z}$.

(ii) If $a, b, c \in \mathbb{Z}$ and $a \mid bc$ then $a \mid b$ or $a \mid c$.

FALSE Let $a = 12$, $b = 4$, $c = 6$.

$12 \mid 24$ so $a \mid bc$ but $12 \nmid 4$ & $12 \nmid 6$.

(iii) If $a, b, c \in \mathbb{Z}$, $a \mid b$ and $b \mid c$ then $a \mid c$

PROOF: Suppose $a, b, c \in \mathbb{Z}$, $a \mid b$ & $b \mid c$.

So $b = ax$, $c = by$ for some $x, y \in \mathbb{Z}$.

$c = by = (ax)y = a(xy)$ & $a \mid c$ since x, y & $xy \in \mathbb{Z}$.

(iv) If $a, b, c \in \mathbb{Z}$, with a, b not both zero and $c \mid a$ and $c \mid b$, then $c \mid (a, b)$.

PROOF Suppose $a, b, c \in \mathbb{Z}$, a, b not both zero & $c \mid a$ & $c \mid b$. By Prop in Ch 2

$(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.

Since $c \mid a$ & $c \mid b$, $c \mid ax + by$ & $c \mid (a, b)$.

□

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

$(a, b) =$ MIN $\{am + bn : m, n \in \mathbb{Z}$ & $am + bn > 0\}$.

(b) Suppose $a, b, c \in \mathbb{Z}$ with $(a, b) = 1$. PROVE that if $a \mid c$ and $b \mid c$ then $ab \mid c$ using the Proposition in (a) (and NOT the Fundamental Theorem of Arithmetic). Suppose $a, b, c \in \mathbb{Z}$ & $(a, b) = 1$.

Then $ax + by = 1$ for some $x, y \in \mathbb{Z}$ by (a).

Suppose $a \mid c$ & $b \mid c$. Then

$c = ad$ & $c = be$ for some $d, e \in \mathbb{Z}$.

So $c(ax + by) = c$, $cax + cby = c$,

$(be)ax + (ad)by = c$, &

$c = ab(ex + dy)$. Hence $ab \mid c$ since e, x, d, y & $ex + dy \in \mathbb{Z}$.

3. [2 + 2 + 6 = 10 pts]

(a) Complete the Definition: Let $p \in \mathbb{Z}$ and $p > 1$. Then p is said to be prime if the only positive divisors of p are 1 and p.

(b) Let $a, b \in \mathbb{Z}$. Prove that if a and b are expressible in the form $6n+1$ where n is an integer, then ab is also expressible in that form.

Suppose $a = 6n_1 + 1$, $b = 6n_2 + 1$ where $n_1, n_2 \in \mathbb{Z}$. Then

$$\begin{aligned} ab &= (6n_1+1)(6n_2+1) \\ &= 36n_1n_2 + 6n_1 + 6n_2 + 1 \\ &= 6(6n_1n_2 + n_1 + n_2) + 1 \end{aligned}$$

which has the desired form since $n_1, n_2 \in \mathbb{Z}$ & $6n_1n_2 + n_1 + n_2 \in \mathbb{Z}$.

(c) COMPLETE THE FOLLOWING PROOF that there are infinitely many primes of the form $6n+5$ where n is an integer.

PROOF: Suppose by way of contradiction that there are only finitely many primes of the form $6n+5$ say

$$p_0 = 5, p_1, p_2, \ldots, p_k.$$

Let

$$N = 6(p_1 p_2 \cdots p_k) + (5).$$

Then N is an integer > 5 & N is odd. $3 \nmid N$ since $3 \mid 6(p_1 \cdots p_k)$ & $3 \nmid 5$. Hence all prime divisors of N have the form $6n+1$ or $6n+5$ (where $n \in \mathbb{Z}$) (since by the division alg $6n, 6n+2, 6n+4$ are not prime, 2 is the only prime of the form $6n+2$,

and 3 is the only prime of the form $6n+3$, & $2 \nmid N$, $3 \nmid N$). All the prime divisors of N can not be of the form $6n+1$ since then (5) would imply N is of the form $6n+1$ which is a contradiction since N is of the form $6n+5$. Therefore N must have at least one prime divisor p of the form $6n+5$.

Case 1 $p = p_0 = 5$. Then
$p \mid N$ & $p \mid 5$ so $p = p_0 \mid 2 \cdot 3 \cdot p_1 p_2 \cdots p_k$
which is impossible since $p \neq 2, 3, p_1, \ldots, p_k$.

Case 2 $p = p_j$ some $j \geq 1$. Then
$p \mid N$ & $p = p_j \mid 6 \cdot p_1 p_2 \cdots p_k$ &
$p \mid (N - 6 p_1 \cdots p_k) = 5$ which is impossible
since $p = p_j \neq 5$ for $j \geq 1$.

In all cases we have a contradiction. Hence there must be infinitely many primes of the form $6n+5$. □

4. [2 + 4 + 4 = 10 pts]

(a) Complete the following Theorem:
Let $a = p_1^{e_1} \cdots p_r^{e_r}$
$b = p_1^{f_1} \cdots p_r^{f_r}$
be prime factorizations where each $e_i, f_i \geq 0$.
Then $a \mid b$ if and only if $e_j \leq f_j$ for $1 \leq j \leq r$.

(b) Prove or disprove the following statement.
If $a \in \mathbb{Z}$, $a > 0$, p is prime and $p^4 \mid a^3$ then $p^2 \mid a$.

PROOF: Suppose $a \in \mathbb{Z}$, $a > 0$, p prime & $p^4 \mid a^3$.

Let $a = p^{e_0} p_1^{e_1} \cdots p_r^{e_r}$ be prime factorization of a where each $e_j \geq 0$. Then

$$p^4 \mid a^3 = p^{3e_0} p_1^{3e_1} \cdots p_r^{3e_r} \quad \&$$
$$4 \leq 3e_0 \quad \text{by (a)}.$$

Since $e_0 \in \mathbb{Z}$ this implies that $e_0 \geq 2$ &
$p^2 \mid a$.

(c) Find integers x, y such that

$$\underset{a}{377}x + \underset{b}{101}y = 1.$$

$377 = 3 \cdot 101 + 74$
$101 = 74 + 27$
$74 = 2 \cdot 27 + 20$
$27 = 20 + 7$
$20 = 2 \cdot 7 + 6$
$7 = 6 + 1$

$74 = a - 3b$
$27 = b - (a - 3b)$
$= 4b - a$
$20 = (a - 3b) - 2(4b - a)$
$= 3a - 11b$
$7 = (4b - a) - (3a - 11b)$
$= 15b - 4a$
$6 = (3a - 11b) - 2(15b - 4a)$
$= 11a - 41b$
$1 = (15b - 4a) - (11a - 41b)$
$= 56b - 15a$

So $x = -15$, $y = 56$ is a sol^n.

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

(a) Complete the Definition Let $a, b, m \in \mathbb{Z}$ with $m \geq 1$. Then a is said to be congruent to b modulo m denoted $a \equiv b \pmod{m}$, if $m \mid a-b$.

(b) PROVE: If $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{Z}$, $m \geq 1$, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a+c \equiv b+d \pmod{m}$.

Suppose $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$.

Then $m \mid (a-b)$ & $m \mid (c-d)$.

$\therefore$ $m \mid (a-b)+(c-d) = (a+c)-(b+d)$ &

$a+c \equiv b+d \pmod{m}$.

(c) PROVE or DISPROVE the following statements:

(i) There are infinitely many primes p such that $p+2$ and $5p+2$ are both prime.

FALSE. We show that for all $p > 3$

either $3 \mid p+2$ or $3 \mid 5p+2$.

Since $p > 3$ is prime

$p = 3q + r$

where $q, r \in \mathbb{Z}$ & $r = 1, 2$ ($r \neq 0$ since $3 \nmid p$).

Case 1 $r = 1$. Then $p = 3q+1$

$p+2 = 3q+3 = 3(q+1)$ & $3 \mid (p+2)$.

Case 2 $r = 2$. Then $p = 3q+2$ &

$5p+2 = 5(3q+2)+2 = 15q+12 = 3(5q+4)$ &

$3 \mid 5p+2$.

Hence either $3 \nmid p+2$ OR $3 \mid 5p+2$.

(ii) If $n \in \mathbb{Z}$ and $n \geq 2$ then $n^{40}+1$ is composite.

Proof.

$x^5+1 = (x+1)(1-x+x^2-x^3+x^4)$.

Let $n \in \mathbb{Z}$, $n \geq 2$.

Let $x = n^8$. Then

$$n^{40}+1 \equiv (n^8+1)(1-n^8+n^{16}-n^{24}+n^{32})$$

& $n^8+1 \mid n^{40}+1$ but

$1 < n^8+1 < n^{40}+1$ since $n > 1$ &

hence

$n^{40}+1$ is composite.

6. [2 bonus pts OPTIONAL]

This is
M _ _ _ _
M _ _ _ _ _ _ _ _.

He was born in _ _ 8 8.
At the Sorbonne he obtained a degree of Magister Atrium in _ _ _ _ _ _ _ _ _ _ y
He was ordained a priest in the Order of M _ _ _ s.

After his death letters in his cell were found from _ _ different correspondents including F _ _ _ _ _, Huygens, Pell, G _ _ _ _ _ _ _, ad Torricelli.