MAS 4203 – QUIZ 2 – SUMMER 2015

Tuesday, July 14

NAME:

Instructions: All work should be written in a proper and coherent manner, and in a way that any student 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: 30 pts = 100%. (also 2 bonus pts)

1(a) Complete the following [2 + 4×2 pts]

Theorem: Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$,

$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$,

be prime factorizations with each $a_i, b_j \geq 0$.

Then $a \mid b$ if and only if $a_i \leq b_i$ for all $1 \leq i \leq n$.

(b) Prove or disprove the following statements:

(i) If $a, b \in \mathbb{Z}$, $a, b > 0$ and $a^2 \mid b^3$ then $a \mid b$.

FALSE.

Let $a = 2^3$, $b = 2^2$.

Then $a^2 = 2^6 = b^3$ & $a^2 \mid b^3$

but $a \nmid b$, since $8 \nmid 4$.

(ii) If $a, b \in \mathbb{Z}$, $a, b > 0$ and $a^2 \mid b^2$ then $a \mid b$.

PROOF. Let a, b be as in (a). Then

$$a^2 = p_1^{2a_1} p_2^{2a_2} \cdots p_n^{2a_n}, \quad b^2 = p_1^{2b_1} p_2^{2b_2} \cdots p_n^{2b_n}$$

are prime factorizations. Since $a^2 \mid b^2$

Thm $2a_i \leq 2b_i$ for each i

by Prop (a). So $a_i \leq b_i$ for each i &

Thm $a \mid b$

again by Prop (a). □

(iii) If $a \in \mathbb{Z}$, $a > 0$, p is a prime number, and $p^4 \mid a^3$, then $p^2 \mid a$.

PROOF. Let $a = p^e p_1^{e_1} \cdots p_r^{e_r}$ be the prime fact. of a.

Then $a^3 = p^{3e} p_1^{3e_1} \cdots p_r^{3e_r}$ is a prime factorization.

Since $p^4 \mid a^3$, $4 \leq 3e$ (by Thm (a)).

So $e \geq 4/3 = 1\frac{1}{3}$.

But $e \in \mathbb{Z}$ so $e \geq 2$ & $p^2 \mid a$

by Thm (a). □

(iv) If $a \in \mathbb{Z}$ and a is odd then $a^2 \equiv 1 \pmod 8$.

Proof: Let $a \in \mathbb{Z}$, a odd. Then $a = 2k+1$ for some $k \in \mathbb{Z}$.

$$a^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1$$
$$= 4k(k+1)$$

Either k or $k+1$ is even so $8 \mid a^2 - 1$ &

$a^2 \equiv 1 \pmod 8$.

□

2. [2+3+2+3 = 10 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: If $a,b,c,d \in \mathbb{Z}$ and $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $ac \equiv bd \pmod m$.

PROOF: Suppose $a,b,c,d \in \mathbb{Z}$, $a \equiv b \pmod m$ & $c \equiv d \pmod m$.
Then $m \mid (a-b)$ & $m \mid (c-d)$.
Therefore
$m \mid c(a-b) + b(c-d) = ac - bd$, &
$ac \equiv bd \pmod m$.

(c) Complete the following

Proposition Let $a,b \in \mathbb{Z}$ and suppose $a \equiv b \pmod m$.
Then $a^n \equiv b^n \pmod m$ if $n \geq 1$ & $n \in \mathbb{Z}$.

(d) PROVE that

$$125^{101} + 260^{100}$$

is divisible by 7. [Hint: Find 125^{101} and $260^{100} \pmod 7$].

$125 = 17 \cdot 7 + 6$ & $125 \equiv 6 \equiv -1 \pmod 7$.
$\therefore 125^{101} \equiv (-1)^{101} \equiv -1 \pmod 7$.
$260 = 37 \cdot 7 + 1 \equiv 1 \pmod 7$.
$260^{100} \equiv 1^{100} \equiv 1 \pmod 7$. $\therefore$
$125^{101} + 260^{100} \equiv (-1) + 1 \equiv 0 \pmod 7$, &

$$7 \mid 125^{101} + 260^{100}.$$

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

(a) Complete the Definition. Let $a, m \in \mathbb{Z}$ with $m > 1$. The integer a has a multiplicative inverse mod m if $ab \equiv 1 \pmod{m}$ for some $b \in \mathbb{Z}$.

(b) Complete the following

Corollary (to a Theorem) Let $a, m \in \mathbb{Z}$ with $m > 1$. The integer a has a multiplicative inverse mod m if and only if $(a, m) = 1$.

(c) Find the multiplicative inverse of 47 mod 863.

[HINT: Use the Euclidean algorithm to find $x, y \in \mathbb{Z}$: $863x + 47y = 1$.]

$863 = 18 \cdot 47 + 17$ $\qquad 17 = a - 18b$

$47 = 2 \cdot 17 + 13$ $\qquad 13 = b - 2(a - 18b)$

$17 = 13 + 4$ $\qquad = 37b - 2a$

$13 = 3 \cdot 4 + 1$ $\qquad 4 = (a - 18b) - (37b - 2a)$

$= 3a - 55b$

$1 = (37b - 2a) - 3(3a - 55b)$

$1 = 202b - 11a$ $\qquad (9494 - 9493 = 1)$

$\therefore 47 \cdot 202 \equiv 1 \pmod{863}$ &

202 is the multiplicative inverse of 47 mod 863.

4. [Bonus 2pts]

(a) This guy is

J_____? G_____

L_____.

(b) State his famous THEOREM about primes:

(c) Complete the following quote from Ore's biography:

"He was an _____ teacher, always expressing himself with great _____. His manner was _____; in his later years he was ___ and at times _____."