MAS 4203 - EXAM - Summer 2015

Thursday, July 16

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

1. [2 + 4×2 = 10 pts]

(a) Complete the definition: Let $a, b \in \mathbb{Z}$. Then a divides b denoted ______, if ________________.

(b) Prove or disprove the following statements:

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

FALSE Let $a=1$. Then $a = 1 \mid 0$ since $0 = 1 \cdot 0$ & $0 \in \mathbb{Z}$. $a \neq 0$.

(ii) There are integers x, y such that
$$3x - 453y = 347.$$

FALSE $3 \mid 453 = 3 \cdot 151$ So if $x, y \in \mathbb{Z}$ & $3x - 453y = 347$ then $3 \mid 347$ but $347 = 115 \cdot 3 + 2$ & $3 \nmid 347$.
This is a contradiction. So the statement is false.

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

FALSE $8 \mid 4 \cdot 2 = 8$ but $8 \nmid 4$ & $8 \nmid 2$.

(iv) If $a, b, c, d \in \mathbb{Z}$, $a \mid b$ and $c \mid d$ then $ac \mid bd$.

TRUE PROOF: Suppose a, b, c, d, $a \mid b$ & $c \mid d$.
Then $b = ae$ & $d = cf$ for some $e, f \in \mathbb{Z}$.
So $bd = aecf = (ac)(ef)$, &
$ac \mid bd$ since $e, f \in \mathbb{Z}$ & $ef \in \mathbb{Z}$. $\square$

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

(a) Complete the following

Theorem: Let $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$,
$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$
be prime factorizations with each $e_i, f_j \geq 0$.
Then $a \mid b$ if and only if $e_i \leq f_i$ for all $1 \leq i \leq r$.

(b) Prove or disprove the following statements

(i) If $a, b \in \mathbb{Z}$ $a, b > 0$ and $a^3 \mid b^4$ then $a \mid b$.

FALSE

Let $a = 2^4$, $b = 2^3$.
$a^3 = 2^{12} = b^4$ so $a^3 \mid b^4$
but
$a = 2^4 \nmid b = 2^3$.

(ii) If $a \in \mathbb{Z}$, $a > 0$, p is prime & $p^5 \mid a^2$ then $p^3 \mid a$.

TRUE. Let $a = p^e p_1^{a_1} \cdots p_r^{a_r}$ be the prime fact. of a where $e, a_i \geq 0$. Then $a^2 = p^{2e} p_1^{2a_1} \cdots p_r^{2a_r}$ (prime fact)

Suppose $p^5 \mid a^2$. Then

$$5 \leq 2e, \; e \geq 2\tfrac{1}{2}.$$

Since $e \in \mathbb{Z}$ this implies $e \geq 3$ &

$$p^3 \mid a.$$

(c) Complete the

Proposition: Let $a, b \in \mathbb{Z}$ with a, b not both zero

Then

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

(d) PROVE OR DISPROVE

If a, b, c are positive integers such that $(a, c) = (b, c) = 1$, then for any positive integers m and n

$$(am + bn, c) = 1.$$

FALSE Let $a = b$ ~~= c = 1~~ $= 3$, $c = 2$. Then $(a, c) = (b, c) = 1$.

But for $m = n = 1$ $(am + bn, c) = (6, 2) = 2 \neq 1$.

3. [2 + 3 + 5 = 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 & p.

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

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

$$ab = (6n_1+1)(6n_2+1)$$
$$= 36n_1n_2 + 6n_1 + 6n_2 + 1$$
$$= 6(6n_1n_2 + n_1 + n_2) + 1$$

as required since $n_1, n_2 \in \mathbb{Z}$ & hence $6n_1n_2 + n_1 + n_2 \in \mathbb{Z}$.

(5) (c) Prove that there are infinitely many primes of the form $6n+5$ where n is a integer as follows:

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

$$N = 6(\underline{p_1 p_2 \cdots p_k}\,\_\_) + (\underline{5}\,\_\_).$$

$N > 1$ is an integer. Clearly N is odd & $3 \nmid N$. any prime > 3 has the form $6n+1$, or $6n+5$ (where $n \in \mathbb{Z}$). N must have a prime divisor. $p \neq 2$, $p \neq 3$. all the prime divisors of N can not have the form $6n+1$ ($n \in \mathbb{Z}$) since otherwise N would have the the form $6n+1$ by (b). This is a contradiction since N is the form $6n+5$ ($n \in \mathbb{Z}$).

Hence N must have a prime divisor p of the form $6n+5$ $(n\in\mathbb{Z})$. So

$$p=p_i$$

for some $0\le i\le k$.

<u>Case 1</u> $i=0$. Then $p=p_0=5$.

$$p\mid N \text{ so } p=5\mid (N-5)=6p_1p_2\cdots p_k$$

This is impossible since $p_i\neq 5$ for $1\le i\le k$.

<u>Case 2</u> $i\ge 1$. Then $p=p_i\mid 6(p_1p_2\cdots p_k)$ &

$$p\mid N-6(p_1p_2\cdots p_k)=5.$$ This is impossible since $p\neq 5$.

In both cases we have a contradiction. Hence there must be infinitely many primes of the form $6n+5$ $(n\in\mathbb{Z})$.

4. $[2+4+2+2=10\text{ pts}]$

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

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

Proof Suppose $a\equiv b\pmod m$ & $c\equiv d \pmod m$.
Then $m\mid (a-b)$ & $m\mid (c-d)$.
So $m\mid (a-b)+(c-d)=(a+c)-(b+d)$, &

$$(a+c)\equiv(b+d)\pmod m.$$

(c) Complete the <u>Definition</u>: Let $m\in\mathbb{Z}$, $m\ge 1$. A complete residue system modulo m is a set of integers such that every integer is congruent mod m to one & only one element of the set.

(d) Prove or disprove that set $\{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2\}$ is a complete residue system mod 7.

$1^2 = 1 \equiv 1 \pmod 7$.

$6^2 = 36 \equiv 1 \pmod 7$ (since $7 \mid 35$).

Since $1^2 \equiv 6^2 \pmod 7$ the set can not be a complete residue system mod 7.

5. [2 + 5 + 3 = 10 pts]

(a) Complete

Fermat's Little Theorem Let $a \in \mathbb{Z}$, p be prime and suppose $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(b) Prove

Corollary to Fermat's Little Theorem

Let $a \in \mathbb{Z}$ and p be prime. Then

$$a^p \equiv a \pmod{p}.$$

PROOF: Let $a \in \mathbb{Z}$, & p prime.

Case 1 $p \mid a$. Then $p \mid a^p$ ($p > 1$) so

$a^p \equiv 0 \pmod p$ & $a \equiv 0 \pmod p$, &

$a^p \equiv a \pmod p$.

Case 2 $p \nmid a$. By Fermat's Little Theorem

$a^{p-1} \equiv 1 \pmod p$.

$a^p = a^{p-1} \cdot a \equiv 1 \cdot a \pmod p$, and

$a^p \equiv a \pmod p$.

Result holds in all cases. D

(c) Suppose $x \in \mathbb{Z}$, $x \not\equiv 0 \pmod 5$, and $x \not\equiv 1 \pmod 5$. Prove that

$$x^3+x^2+x+1 \equiv 0 \pmod 5.$$

Let $x \in \mathbb{Z}$, suppose $x \not\equiv 0 \pmod 5$, & $x \not\equiv 1 \pmod 5$

Then $x \equiv 2, 3$ or $4 \pmod 5$.

Case 1. $x \equiv 2 \pmod 5$. Then $x^3+x^2+x+1 \equiv 2^3+2^2+2+1 \pmod 5$

$\equiv 8+4+2+1 \equiv 15 \equiv 0 \pmod 5$.

Case 2 $x \equiv 3 \pmod 5$. Then $x \equiv -2 \pmod 5$, $x^3+x^2+x+1 \equiv -8+4-2+1$

$\equiv -5 \equiv 0 \pmod 5$.

Case 3 $x \equiv 4 \pmod 5$. Then $x \equiv -1 \pmod 5$ & $x^3+x^2+x+1 \equiv -1+1-1+1 = 0 \equiv 0 \pmod 5$

Result holds in all cases.

(d) [BONUS 5 pts]

Generalize the result of (c) to any odd prime p and prove your result.

Let p be any odd prime & suppose $x \in \mathbb{Z}$, $x \not\equiv 0 \pmod p$ & $x \not\equiv 1 \pmod p$. So $p \nmid x$ &

$$x^{p-1} \equiv 1 \pmod p$$ by Fermat's Little Thm.

So $p \mid (x^{p-1}-1) = (x-1)(x^{p-2}+\cdots+x+1)$.

$p \nmid (x-1)$ since $x \not\equiv 1 \pmod p$. So

$p \mid x^{p-2}+\cdots+x+1$ by Euclid's Lemma, and

$$\boxed{x^{p-2}+\cdots+x+1 \equiv 0 \pmod p.}$$

6. [2+8 = 10 pts]

(a) Complete the Definition. Let n be a composite integer. If $2^n \equiv 2 \pmod n$ then n is said to be pseudoprime.

(b) Prove only ONE part:

(i) $645 = (3)(5)(43)$ is pseudoprime.

(ii) If p is prime and $n = 2^p - 1$ is composite then n is pseudoprime.

(iii) Let $a \in \mathbb{Z}$ and suppose p and q are distinct primes. Then
$$a^{pq} + a \equiv a^p + a^q \pmod{pq}.$$

(i) $645 = (3)(5)(43)$ is composite.

We show $2^{645} \equiv 2 \pmod m$ for $m = 3, 5$ & 43.

By FLT, $2^2 \equiv 1 \pmod 3$ (since $3 \nmid 2$, 3 prime).

So $2^{645} = (2^2)^{322} 2^1 \equiv 1^{322} 2^1 \equiv 2 \pmod 3$.

Also $2^2 = 4 \equiv -1 \pmod 5$.

So $2^{645} = (2^2)^{322} \cdot 2 \equiv (-1)^{322} \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod 5$

By FLT, $2^{42} \equiv 1 \pmod{43}$ since 43 is prime & $43 \nmid 2$.

$$2^{645} = (2^{42})^{15} 2^{15} \quad (\text{since } 645 = (42+1)(15))$$
$$\equiv 1^{15} 2^{15} \pmod{43}$$
$$\equiv 2^{15} \pmod{43}.$$

$2^3 = 8$, $2^6 = 8^2 = 64 \equiv 21 \pmod{43}$.

$2^7 \equiv 2 \cdot 21 \equiv 42 \equiv -1 \pmod{43}$

So $2^{15} = (2^7)^2 \cdot 2 \equiv (-1)^2 \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod{43}$.

So $2^{645} \equiv 2 \pmod m$ for $m = 3, 5, 43$.

So $m \mid (2^{645} - 2)$ for $m = 3, 5, 43$. Since $3, 5, 43$ are pairwise rel. prime $645 \mid (2^{645} - 2)$, $2^{645} \equiv 2 \pmod{645}$ & 645 is pseudoprime.

7. [3 bonus points]

(a) This is ___________
C____ F___________
____

(b)
D________________es
A______________ae.
is the title of his famous book on Number Theory

(c) He left G________en in 1798 without a diploma, but by this time he had made one of his most important discoveries — the construction of the regular __-gon by ruler and compasses.