MAS 4203 - QUIZ 2 — 1/30/17

GROUP & TAKE HOME

Please complete and return to LIT 408
by 4 PM, Jan 31 (Tuesday).
Slip under door if Dr G not in.

Please submit <u>one</u> EXAM per group

GROUP MEMBERS:

1.
2.
3.
4.

Use additional paper if necessary

MAS 4203 – EXAM 1 – Spring 2016

Friday, Feb. 5

NAME: ____________________

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 <u>a divides b</u> denoted ____, if

________________________________.

(b) Prove or disprove the following statements

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

(ii) There are integers x, y such that
$$33x + 21y = 20.$$

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

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

2. [2 + 6 = 8 pts]

(a) Complete the following

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

$$(a, b) = \text{MIN}\{\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\}.$$

(b) Let $a, b, c \in \mathbb{Z}$ with $(a, b) = 1$ and $a \mid bc$.
<u>PROVE</u> $a \mid c$ using Prop. in (a) and
<u>NOT</u> the Fundamental Theorem of Arithmetic.

3. [3 + 3 = 6 pts]

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

(b) Find integers x, y such that

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

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

(a) Complete the definition: p is prime (or a prime number) if $p >$ __, $p \in \mathbb{Z}$ and the only ________________________.

(b) Use Qu. 2(a) 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:

(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.

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

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

(a) Complete the Definition. Let $m > 0$, $m \in \mathbb{Z}$ & $a, b \in \mathbb{Z}$.
We say <u>a is congruent to b modulo m</u> and write ________ if ____________.

(b) <u>Prove</u> the following

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

<u>Proof</u>:

(c) Find a prime divisor of $2^{44} + 1$.
<u>Hint</u>: What is $x^{11} + 1 = ?$

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