MATH2710 **Name:**________________________

Exam 1 **Date:**________________________

This exam contains 7 pages (including this cover page) and 6 problems. Check to see if any pages are missing. Enter all requested information on the top of this page, and put your initials on the top of every page, in case the pages become separated.

You may *not* use your books, notes, or any unapproved calculator on this exam.

You are required to show your work on each problem on this exam. The following rules apply:

- **Organize your work**, in a reasonably neat and coherent way, in the space provided. Work scattered all over the page without a clear ordering will receive very little credit.
- **Mysterious or unsupported answers will not receive full credit**. A correct answer, unsupported by calculations, explanation, or algebraic work will receive no credit; an incorrect answer supported by substantially correct calculations and explanations might still receive partial credit.
- If you need more space, ask for an extra sheet of paper to continue the problem on; clearly indicate when you have done this.

Do not write in the table to the right.

Problem	Points	Score
1	4	
2	4	
3	5	
4	3	
5	4	
6	5	
Total:	25	

1. (a) (1 point) State a definition of the $\gcd(a, b)$ for $a, b \in \mathbb{Z}$.

Solution:

The greatest common divisor of two integers a and b not both zero, is the largest positive integer dividing both a and b.

Alternatively: An integer d is the $\gcd(a, b)$ if and only if

(i) $d \geq 0$

(ii) d divides both a and b

(iii) any divisor of a and b also divides d.

(b) (2 points) State the Unique Factorization Theorem.

Solution:

Every integer greater than 1 can be expressed as a product of primes and, apart from the order of the factors, this expression is unique.

(c) (1 point) Complete the following theorem:

Theorem. *If a and b are integers, with b positive, then there exist* ___*unique*___ *integers q and r such that*

$$a = \underline{\quad qb + r \quad}, \qquad \textit{where } \underline{\quad 0 < r \leq b \quad}$$

2. (4 points) Solve the following linear Diophantine equation.

$$21x + 15y = 12$$

Solution:

x	y	r_i	q_i	Euclid Alg
1	0	21	-	-
0	1	15	-	-
1	-1	6	1	21=15(1)+6
-2	3	3	2	15=6(2)+3
5	-7	0	2	6=3(2)+0

So we have that

$$21(-2) + 15(3) = 3$$

therefore

$$21(-8) + 15(12) = 12$$

and $x_0 = -8$ and $y_0 = 12$ are particular solutions. The general solutions are

$$x = -8 + n\left(\frac{15}{3}\right) \qquad \text{where } n \in \mathbb{Z}$$

and

$$y = 12 + n\left(\frac{21}{3}\right) \qquad \text{where } n \in \mathbb{Z}.$$

3. (5 points) Let a and b be two positive even integers. Prove that

$$\gcd(a,b) = 2\gcd\left(\frac{a}{2}, \frac{b}{2}\right)$$

Solution:

Since a and b are positive even integers we have that $a = 2n$ and $b = 2m$ for some integers m and n. Let

$$m = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$$
$$n = p_1^{b_1} \cdot \ldots \cdot p_n^{b_n}$$

be prime factorizations of m and n allowing some exponents to be zero. We have,

$$a = 2 \cdot p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$$

$$b = 2 \cdot p_1^{b_1} \cdot \ldots \cdot p_n^{b_n}.$$

are prime factorizations of a and b. We have that

$$\gcd(a,b) = 2^1 \cdot p_1^{d_1} \cdot \ldots \cdot p_n^{d_n} \quad \text{where } d_i = \min(a_i, b_i) \text{ for all } i \in \{1, \ldots n\}$$

Since $\gcd(m,n) = \gcd\left(\frac{a}{2}, \frac{b}{2}\right)$ we have that

$$\gcd\left(\frac{a}{2}, \frac{b}{2}\right) = p_1^{d_1} \cdot \ldots \cdot p_n^{d_n} \quad \text{where } d_i = \min(a_i, b_i) \text{ for all } i \in \{1, \ldots n\}$$

and the result is clear.

4. True or False. Briefly justify your answers
   (a) (1 point) The linear Diophantine equation $ax = b$ has a solution if and only if $a \nmid b$

   (b) (1 point) The only even prime number is 2.

   (c) (1 point) The integer d is the $\gcd(a, b)$ if $d = ax + by$ for some integers x and y.

Solution:

(a) *False*: The linear Diophantine equation $ax = b$ has a solution if and only if $a \mid b$.

(b) *True*: Let $p \neq 2$ be a prime and suppose p is even. Then $p = 2m$ for some $m \in \mathbb{Z}$ and $2 \mid p$. This is a contradiction.

(c) *False*: If d is negative then d cannot be the greatest common divisor. This condition does not exclude d being negative.

5. (4 points) Prove the following theorem

Theorem. *An integer $x > 1$ is either prime or contains a prime factor $p \leq \sqrt{x}$.*

Solution:

Suppose that p is the smallest factor of x. If x is composite, we can write $x = ab$, where a and b are positive integers and $1 < a \leq b < x$. Since p is the smallest prime factor $a \geq p$, $b \geq p$ and $x = ab \geq p^2$. Hence $p \leq \sqrt{x}$.

6. (5 points) Let A, B and U be sets such that $A \subseteq U$ and $B \subseteq U$. The complement of the set A denoted A^c is the following set

$$A^c = \{x \in U \mid x \notin A\}.$$

The complement of B is defined similarly. Prove the following identity

$$(A \cap B)^c = A^c \cup B^c$$

Solution:

We must show that $(A \cap B)^c \subseteq A^c \cup B^c$ and $A^c \cup B^c \subseteq (A \cap B)^c$. To show that $(A \cap B)^c \subseteq A^c \cup B^c$ let $x \in (A \cap B)^c$ be arbitrary, then $x \notin (A \cap B)$. Thus we have $x \notin A$ or $x \notin B$. Hence $x \in A^c \cup B^c$. Since $x \in (A \cap B)^c$ was arbitrary we have $(A \cap B)^c \subseteq A^c \cup B^c$.

To show $A^c \cup B^c \subseteq (A \cap B)^c$ we let $y \in A^c \cup B^c$ be arbitrary. Then $y \notin A$ or $y \notin B$ and hence $y \notin (A \cap B)$. So $y \in (A \cap B)^c$. Since y was arbitrary $A^c \cup B^c \subseteq (A \cap B)^c$.