MTH 310– Midterm Exam I
Abstract Algebra and Number Theory I

Instructor: D. Weng

October 4, 2019

Name: Answer

This exam contains 9 pages (including this cover page) and 7 questions. You have 50 minutes to complete the exam. Total of points is 100.

No textbooks, lecture notes, cell phones, calculators, or computers are allowed.

Good luck!

Distribution of Points

Question	Points	Score
1	10	
2	10	
3	11	
4	20	
5	15	
6	10	
7	24	
Total:	100	

1. Each of the following relations is NOT an equivalence relation. Please identify which of the three defining properties (reflexive, symmetric, and transitive) each of them fails to satisfy. They may fail to satisfy more than one defining properties. You need to list ALL the failing ones together with a brief explanation in order to receive full credit.

   (a) (5 points) The inclusion relation on subsets of $\mathbb{Z}$.

   Reflexive ✓

   Symmetric ✗ $\emptyset \subseteq \mathbb{Z}$ but $\mathbb{Z} \nsubseteq \emptyset$

   Transitive ✓

   (b) (5 points) The diplomatic relation between countries.

   Reflexive ✗ A country does not have diplomatic relation with itself.

   Symmetric ✓

   Transitive ✗. A and B are allies and B and C are allies does not imply A and C are allies.

2. (10 points) Solve the following equation in $\mathbb{Z}_{19}$. To receive full credit, please provide justification for key steps.

$$x^2 - 21x - 100 = 0.$$

$x^2 - 21x - 100 = (x-25)(x+4)$

Since 19 is a prime.

$\mathbb{Z}_{19}$ is an integral domain.

In an integral domain, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Therefore $x - 25 = 0$ or $x + 4 = 0$

$x = 25 = 6$ or $x = -4 = 15$

3. Consider the ring $R = \mathbb{Z}_8 \times \mathbb{Z}_6$.

(a) (3 points) How many elements are there in R?

$8 \times 6 = 48$

(b) (3 points) Compute $(4,4) \cdot (5,5)$ in the ring R.

$(4,4) \cdot (5,5) = (20,20) = (4,2)$

(c) (5 points) Is $(4,4)$ a unit in R? Why or why not?

No. Because $(4,4) \cdot (2,3) = (0,0)$

So $(4,4)$ is a zero divisor.

Therefore it cannot be a unit.

4. (20 points) Suppose m and n two positive integers with $(m, n) = 1$. Suppose a is an integer and $am = 0$ in $\mathbb{Z}_n$. Prove that $n|a$.

Proof. $(m,n)=1 \Rightarrow \exists\, x, y$ s.t. $mx + ny = 1$

$am = 0$ in $\mathbb{Z}_n \Rightarrow am = nz$ for some z.

$$a = a \cdot 1 = a(mx+ny)$$
$$= amx + any$$
$$= nzx + any$$
$$= n(zx + ay)$$

$\Rightarrow n|a$. $\square$

Alternative Proof. $(m,n)=1 \Rightarrow m$ is a unit in $\mathbb{Z}_n$.

$\Rightarrow \exists\, m^{-1} \in \mathbb{Z}_n$.

$$am = 0 \Rightarrow \underset{a}{\underset{\parallel}{amm^{-1}}} = 0 \cdot m^{-1} = 0.$$

$\Rightarrow a = 0$ in $\mathbb{Z}_n$

$\Rightarrow n|a$. $\square$

5. (15 points) Let x and y be two integers. Prove that

$$x^3 + y^3$$

CANNOT be congruent to 3, 4, 5, or 6 modulo 9. (Hint: there was a homework problem about the remainder of the cube of an integer when divided by 9; you may quote results from this homework problem.)

Proof $x^3, y^3 \equiv 8, 0, 1 \mod 9$ (From HW)

x^3+y^3 (y^3 \ x^3)	0	1	8
0	0	1	8
1	1	2	0
8	8	0	7

Therefore $x^3+y^3 \not\equiv 3, 4, 5$ or 6 in $\mathbb{Z}_9$. □

6. (10 points) Please fill in the blanks inside the statements below with words from the following list. You DO NOT have to use all the words, and each word may be used MULTIPLE times. NO justification is needed.

non-empty, non-zero, positive, negative, prime, composite, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$,

(a) Well Ordering Axiom: any non-empty subset of $\mathbb{N}$ has a smallest element.

(b) Division Algorithm: let a be an integer and let b be a positive integer. Then there exist unique integers q and r with $0 \leq r < b$ such that $a = bq + r$.

(c) Any integer $a \neq 0, \pm 1$ can be factored into a product of prime numbers, unique up to sign changing and permutation of factors.

(d) For any integer $n > 1$, $\mathbb{Z}_n$ is NOT an integral domain if and only if n is a composite number.

7. (24 points) Please determine whether the following statements are true or false based on your best judgement. In the parentheses in front of each statement, write "T" if you think it is true, and write "F" if you think it is false. NO justification is needed.

   (a) (F) Any integer is either a prime number or a composite number.

   (b) (F) If $d = (a, b)$, then there exist unique integers u and v such that $d = au + bv$.

   (c) (F) n is a zero divisor in $\mathbb{Z}_n$.

   (d) (F) $\mathbb{Z}_n$ is a subring of $\mathbb{Z}$.

   (e) (F) $\mathbb{Z}_n$ inherits an ordering $\leq$ from $\mathbb{Z}$.

   (f) (F) In a ring R, multiplication is always commutative.

   (g) (T) Fields are all integral domains.

   (h) (F) Every commutative ring has a multiplicative identity.

This page is intentionally left blank to accommodate scratch work.