Midterm

NOVEMBER 2, 2016
ALAN CHANG

Please present your solutions clearly and in an organized way. Answer the questions in the space provided on the question sheets. If you run out of room for an answer, continue on the back of the page. **Please note that use of a calculator is not allowed.**
Good luck!! ◡̈

Full Name: Sample solutions

Question	Points	Score
1	20	
2	30	
3	10	
4	10	
5	20	
6	10	
Total:	100	

This exam has 6 questions, for a total of 100 points. The maximum possible score for each problem is given on the right side of the problem.

20

1. Recall the following axioms:

   A3. (Additive identity) There is a unique element 0 such that for any element a of the set, $0 + a = a$ and $a + 0 = a$.

   A4. (Additive inverse) If a is any element of the set, then there is a unique corresponding element $-a$ such that $a + (-a) = 0$ and $(-a) + a = 0$.

   M3. (Multiplicative identity) There is a unique element $1 \neq 0$ such that for any element a of the set, $1 \cdot a = a$ and $a \cdot 1 = a$.

   M4. (Multiplicative inverse) If a is any nonzero element of the set, then there is a unique corresponding element a^{-1} such that $a \cdot a^{-1} = 1$ and $a^{-1} \cdot a = 1$.

   Which of the following sets satisfy which axioms? For each box in the following table, place a $\times$ if the set satisfies the particular axiom. (You do not need to justify.)

	A3 (add. id.)	A4 (add. inv.)	M3 (mult. id.)	M4 (mult. inv.)
$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$			X	
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$	X	X	X	
$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$	X	X		
$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$	X	X	X	X
$\mathbb{Z}_{10}$	X	X	X	

2. (a) Using the Euclidean algorithm, find the GCD of 89 and 100. [10]

   (b) Using the extended Euclidean algorithm, find a solution to $89x + 100y = 1$, with $x, y \in \mathbb{Z}$. [10]

   (c) Solve for w in $\mathbb{Z}_{100}$: [10]

$$89 \cdot w + 97 = 27$$

For parts (a) and (b), you do not need to justify, but please show your calculations.

(a)
$$100 = 1 \cdot 89 + 11$$
$$89 = 8 \cdot 11 + \boxed{1} \longrightarrow \boxed{\text{The GCD is } 1.}$$
$$11 = 11 \cdot 1 + 0$$

(b)
$$\begin{aligned} 1 &= 89 - 8 \cdot 11 \\ &= 89 - 8 \cdot (100 - 1 \cdot 89) \\ &= 89 - 8 \cdot 100 + 8 \cdot 89 \\ &= 9 \cdot 89 - 8 \cdot 100 \implies \boxed{\begin{array}{l} x = 9 \\ y = -8 \end{array}} \end{aligned}$$

(c)
$$89 \cdot w + 97 = 27$$
$$(89 \cdot w + 97) + 3 = 27 + 3$$
$$89 \cdot w = 30$$
$$9 \cdot 89 \cdot w = 9 \cdot 30$$
$$1 \cdot w = 70$$
$$\boxed{w = 70}$$

(from (b), we know $89^{-1} = 9$ in $\mathbb{Z}_{100}$.)

3. Find all the fourth roots of 1 in $\mathbb{Z}_5$. [10]

We want to solve $x^4 = 1$ in $\mathbb{Z}_5$.

Let's try all possible values.

$0^4 = 0$

$1^4 = 1$

$2^4 = 2 \cdot 2 \cdot 2 \cdot 2 = 4 \cdot 4 = 1$

$3^4 = 3 \cdot 3 \cdot 3 \cdot 3 = 4 \cdot 4 = 1$

$4^4 = 4 \cdot 4 \cdot 4 \cdot 4 = 1 \cdot 1 = 1$

So the 4th roots of 1 are $\boxed{1, 2, 3, 4}$

4. Use the definition of "$a \mid b$" to show the following.

(a) $12 \mid (-36)$. [5]

(b) $0 \mid 0$. [5]

"$a \mid b$" means there exists a $k \in \mathbb{Z}$ such that $ak = b$.

(a). $12 \cdot (-3) = 36$. (let $k = -3$.)

(b) $0 \cdot 0 = 0$ (let $k = 0$.)

5. Determine if the following statements are true or false.
If a statement is true, give a proof. If it is false, give a counterexample. (Here, $a, b, c, d \in \mathbb{Z}$.)

(a) If $a \mid b$ and $c \mid d$, then $ac \mid bd$. $\boxed{10}$

(b) If $a \mid bc$, then $a \mid b$ or $a \mid c$. $\boxed{10}$

(a) TRUE: Suppose $a|b$ and $c|d$.
Then there exist $k, \ell \in \mathbb{Z}$ such that
$a \cdot k = b$ and $c \cdot \ell = d$.
Multiply these together to get
$(ac) \cdot (k\ell) = bd$.
Since $k\ell \in \mathbb{Z}$, $ac | bd$.

(b) FALSE: Let $a=4$, $b=2$, $c=2$.
Then $a|bc$ but $a \nmid b$ and $a \nmid c$.

10

6. Let $H = \{4k+1 \mid k \geq 0, k \in \mathbb{Z}\} = \{1, 5, 9, 13, 17, \ldots\}$.

Recall that an element $h \in H$ is called a *Hilbert prime* if $h > 1$ and the only way it can be written as a product of two integers in H is $h \cdot 1$ or $1 \cdot h$. (For example, 21 is not an ordinary prime, since $27 = 3 \cdot 7$, but it is a Hilbert prime since 3 and 7 are not in H.)

Show that every element of H greater than 1 can be factored into Hilbert primes. (In other words, show that every element of H greater than 1 can be written as a product $p_1 \cdot p_2 \cdot \cdots \cdot p_n$, where $n \geq 1$ and each p_i is a Hilbert prime.)

I'll start you off: Let

$$S = \{h \in H \mid h > 1 \text{ and } h \text{ cannot be factored into Hilbert primes}\}.$$

Suppose for contradiction that S is not empty.

By the well-ordering principle, S has a smallest element. Let's call it k.

Since k cannot be factored into Hilbert primes, it is not a Hilbert prime itself.

So there are $a, b \in H$ such that: $\begin{cases} k = a \cdot b \\ 1 < a < k \\ 1 < b < k \end{cases}$

Since k is the smallest element of S and $a < k$, we know a can be factored into Hilbert primes. Similarly, b can be factored into Hilbert primes.

So $a \cdot b$ can be factored into Hilbert primes. (Just multiply the two products together.)

Thus, $k \notin S$. Contradiction! $\rightarrow\leftarrow$

We conclude that S is empty. $\square$