Final exam

DECEMBER 9, 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: ______________________________

Question	Points	Score
1	15	
2	20	
3	20	
4	20	
5	15	
6	15	
7	20	
8	15	
9	10	
10	0	
Total:	150	

This exam has 10 questions, for a total of 150 points. The maximum possible score for each problem is given on the right side of the problem.

1. (a) Recall axiom M4: $\boxed{5}$

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 $a^{-1} \cdot a = 1$.

Circle the sets below which satisfy axiom M4. (No justification needed.)

$$\mathbb{Z}_2 \qquad \mathbb{Z}_3 \qquad \mathbb{Z}_4 \qquad \mathbb{Z}_5 \qquad \mathbb{Z}_6 \qquad \mathbb{Z}_7 \qquad \mathbb{Z}_8 \qquad \mathbb{Z}_9 \qquad \mathbb{Z}_{10}$$

(b) Recall the following theorem: $\boxed{10}$

"Let $a, b, c \in \mathbb{N}$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$."

Please use the theorem above to give a proof of Euclid's lemma, which is the following:

"Let $p, x, y \in \mathbb{N}$. If p is a prime and $p \mid xy$, then $p \mid x$ or $p \mid y$."

2. (a) Circle the numbers below that are relatively prime to 20: $\boxed{5}$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19

Let $\phi(20)$ be the number of numbers you circled. What is $\phi(20)$?

(b) Euler's theorem says that if $\gcd(x, 20) = 1$, then $x^{\phi(20)} \equiv 1 \pmod{20}$. Check that $7^{\phi(20)} \equiv 1 \pmod{20}$ and $11^{\phi(20)} \equiv 1 \pmod{20}$. $\boxed{10}$

(c) What is the remainder when 7^{1000} is divided by 20? $\boxed{5}$

3. (a) Write down three different *positive* numbers which satisfy $x \equiv 4 \pmod{20}$. $\boxed{2}$

   (b) Write down a *negative* number which satisfies $x \equiv 4 \pmod{20}$. $\boxed{2}$

   (c) What are *all* $x \in \mathbb{Z}$ which satisfy both $x \equiv 4 \pmod{20}$ and $x \equiv 5 \pmod{14}$? $\boxed{8}$

   (d) What are *all* $x \in \mathbb{Z}$ which satisfy both $x \equiv 4 \pmod{20}$ and $x \equiv 5 \pmod{13}$? $\boxed{8}$

4. Let $A = 1{,}120{,}021$.

   (a) What is the remainder when A is divided by 4? (No justification needed.) $\boxed{5}$

   (b) What is the remainder when A is divided by 9? (No justification needed.) $\boxed{5}$

   Let $B = 4 \cdot 6^6 + 2 \cdot 6^5 + 1 \cdot 6^3 + 2 \cdot 6^2 + 5 \cdot 6^1 + 3$.

   (c) What is the remainder when B is divided by 36? $\boxed{5}$

   (d) What is the remainder when B is divided by 5? $\boxed{5}$

5. (a) How many positive divisors does 100 have? $\boxed{3}$

   (b) How many positive divisors does 1,000,000,000 (one billion) have? $\boxed{7}$

   (c) How many positive divisors does 3,000,000,000 (three billion) have? $\boxed{5}$

6. For this problem, use the following letter-number pairing.

letter	A	B	C	D	E	F	G	H	I	J	K	L	M
number	0	1	2	3	4	5	6	7	8	9	10	11	12
letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
number	13	14	15	16	17	18	19	20	21	22	23	24	25

(a) I encrypted a message using the function $f(x) = x + 12 \pmod{26}$. The encrypted message is "`NKQ`." What is the original message? $\boxed{5}$

(b) Encrypt "`HI`" using the encryption function $f(x) = 5x + 1 \pmod{26}$. What is the decryption function g? $\boxed{10}$

(Hint: The following calculations may be useful: $4 \cdot 26 = 104$ and $5 \cdot 21 = 105$.)

7. Recall the RSA algorithm:

- Step 1: Bob chooses 2 distinct primes p and q. He computes $n = pq$.
- Step 2: Bob chooses e with $\gcd(e, (p-1)(q-1)) = 1$.
- Step 3: Bob finds d with $de \equiv 1 \pmod{(p-1)(q-1)}$.
- Step 4: Bob makes the two following numbers public: n and e. (He keeps p, q, d secret.)
- Step 5: The encryption function is $f(x) = x^e \pmod{n}$.
- Step 6: The decryption function is $g(x) = x^d \pmod{n}$.

(a) In step 2, why does e need to satisfy $\gcd(e, (p-1)(q-1)) = 1$? (Why can't Bob choose any e?) $\boxed{5}$

(b) In one short sentence, what makes RSA secure (in present times, at least)? $\boxed{5}$

(c) Now, suppose we do RSA with $n = 77$ and $e = 11$. What is the decryption function? $\boxed{10}$

8. (a) Suppose $a, b \in \mathbb{Z}_8$. Write what "$a \mid b$ (in $\mathbb{Z}_8$)" means. $\boxed{2}$

(b) In $\mathbb{Z}_8$, the statement "if $a^3 \mid b^3$, then $a \mid b$" is not true. Please find a counterexample to the statement. $\boxed{6}$

(Hint: Choose $b \in \mathbb{Z}_8$ so that $b^3 = 0$.)

(c) In $\mathbb{Z}$, the statement "if $a^3 \mid b^3$, then $a \mid b$" is true. What theorem from class can we use to prove this? (Just state the name of the theorem.) $\boxed{3}$

(d) Recall that using the axioms A1--A4, M1--M3, D, we can prove statements like "if $a \mid b$, then $a^2 \mid b^2$." $\boxed{4}$

Why is there no proof of the statement in (c) that uses only these axioms?

(Recall that these axioms are: commutativity of addition, associativity of addition, additive identity, additive inverse, commutativity of multiplication, associativity of multiplication, multiplicative identity, distributive property.)

9. Recall that 10

$$\mathbb{N} \times \mathbb{N} = \{(x, y) \mid x \in \mathbb{N} \text{ and } y \in \mathbb{N}\}.$$

That is, the set $\mathbb{N} \times \mathbb{N}$ consists of all ordered pairs of natural numbers. You can view this set as a grid of squares extending infinitely upwards and to the right:

$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$\cdots$
$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$\cdots$
$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$\cdots$
$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$\cdots$

Is the set $\mathbb{N} \times \mathbb{N}$ countable? Please justify.

10. The set $\{1,2,3\}$ has 8 subsets: **10 (bonus)**

$$\{\}, \quad \{1\}, \quad \{2\}, \quad \{3\}, \quad \{1,2\}, \quad \{1,3\}, \quad \{2,3\}, \quad \{1,2,3\}.$$

How many subsets does $\mathbb{N}$ have? Let's show that it has uncountably many! Help me complete the following proof, which uses a variation of Cantor's diagonalization argument.

Step 1: Suppose for contradiction that $\mathbb{N}$ has only countably many subsets. Then we can list out *all subsets* of $\mathbb{N}$ in a sequence $S_1, S_2, S_3, \ldots$. (Each S_i is a subset of $\mathbb{N}$.)

For example:

S_1	$\{3,5,7\}$	
S_2	$\mathbb{N}$	
S_3	$\{\}$	(the empty set)
S_4	$\{1,4,9,16,25,36,\ldots\}$	(the perfect squares)
S_5	$\{2,4,6,8,10,\ldots\}$	(the even numbers)
$\vdots$	$\vdots$	

Step 2: Given a sequence $S_1, S_2, S_3, \ldots$, we define a new set T by

$$T = \{n \in \mathbb{N} \mid n \notin S_n\}.$$

In words: for each natural number n, we check to see if n is in S_n. If it is, then we include n in the set T. If it is not, then we do not include n in the set T.

In our example above, $1 \notin S_1, 2 \in S_2, 3 \notin S_3, 4 \in S_4, 5 \notin S_5$, so T contains $1,3,5$ but not $2,4$.

Step 3: Using our set T, we get a contradiction. How?