Midterm Exam May 3

Your name:____

Indicate your Identify your Team:

1PM	**32-082 Table (1–13):**	_______
1PM	**32-044 Table (A–K):**	_______
2:30PM	**32-044 Table (A–K):**	_______

- This exam is **closed book** except for a 2-sided cribsheet. Total time is 90 minutes.
- Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem.
- In answering the following questions, you may use without proof any of the results from class or text.
- GOOD LUCK!

DO NOT WRITE BELOW THIS LINE

Problem	Points	Grade	Grader
1	20		
2	20		
3	20		
4	20		
5	20		
Total	100		

Problem 1 (Number Theory and RSA) (20 points).
Indicate whether the following statements are **true** or **false** by circling **T** or **F**. Provide a brief argument justifying your choice for each statement.

(a) Let n and a be positive integers. If n and a are relatively prime, then

$a^{(\phi(n)^2)} \equiv 1 \pmod{n}$. **T** **F**

(b) If n and m are positive integers with $\phi(n) = \phi(m)$, then $n = m$. **T** **F**

(c) For positive integers a, b, and n, we have

$n \equiv 5 \pmod{ab}$ if and only if $n \equiv 5 \pmod{a}$ and $n \equiv 5 \pmod{b}$. **T** **F**

(d) An efficient algorithm for FACTORING would render RSA insecure. **T** **F**

Problem 2 (Modular Arithmetic and Euler's Theorem) (20 points).

Definition. Define the *order of k modulo n*, written as $\text{ord}(k, n)$, to be the smallest positive power of k congruent to 1 modulo n, that is,

$$\text{ord}(k, n) ::= \min\{m > 0 \mid k^m \equiv 1 \text{ mod } n\}.$$

If k^m is *never* congruent to 1 mod n for any positive integer m, then $\text{ord}(k, n) ::= \infty$.

(a) For integers k and n, show that if $\text{ord}(k, n)$ is finite then k and n are relatively prime.

(b) Show conversely that if k and n are relatively prime then $\text{ord}(k, n)$ is finite.

(c) Prove that if k and n are relatively prime, then $\text{ord}(k, n)$ divides $\phi(n)$.

Hint: Let $m = \text{ord}(k, n)$ and divide $\phi(n)$ by m. So

$$\phi(n) = q \cdot m + r \text{ where } 0 \leq r < m.$$

Problem 3 (**Asymptotic Notation**) (**20 points**).
Include brief **explanations** with your answers to each of following questions.

(a) Let $h(x) = (\log_2 x)^3 \cdot (x + 2)^3$. Is $h(x) = O(x^3)$? Is $h(x) = O(x^{3.1})$?

(b) Is it true that $x \log_2 x \sim x \ln x$? Is it true that $x \log_2 x = \Theta(x \ln x)$?

ppart If $f, g : \mathbb{N}^+ \to \mathbb{N}^+$ and $f \sim g$, must f^2 and g^2 be asymptotically equal?

(c) If $f, g : \mathbb{N}^+ \to \mathbb{N}^+$ and $f \sim g$, must 2^f and 2^g be asymptotically equal? *Hint:* No.

Problem 4 (Bijections and Binomial Coefficients) (20 points).
Answer the following questions with a number or a simple formula involving factorials and binomial coefficients. Briefly explain your answers.

(a) There is a robot that steps between integer positions in 2-dimensional space. Each step of the robot increments one coordinate and leaves the other one unchanged. Now, the robot got special gear that allows him to also make a limited number of "diagonal" steps, in which both coordinates are incremented.

We would like to calculate the number of paths the robot can follow going from the origin $(0, 0)$ to the position (M, N) if he makes exactly K diagonal steps. Assume that $K \leq \min(M, N)$.

(i) Let 0 correspond to a diagonal step, 1 to a step along the first coordinate, and 2 to a step along the second coordinate. Demonstrate a set of strings of 0's, 1's, and 2's that has a bijection to the set of possible robot paths, and describe this bijection.

(ii) How many possible paths can the robot take?

(b) How many ways are there to order the 26 letters of the alphabet (with each letter used exactly once) so that no two of the vowels `a`, `e`, `i`, `o`, `u` appear consecutively and the last letter in the ordering is not a vowel?

Hint: Every vowel appears to the left of a consonant.

Problem 5 (**Counting Integer Solutions**) (**20 points**).

Please give **numerical answers** together with brief **explanations** for each of the following questions.

(a) How many *positive* integer solutions are there to equation (sumx)?

$$x_1 + x_2 + x_3 + x_4 + x_5 = 20 \tag{sumx}$$

(b) How many nonnegative *even* integer solutions are there to (sumx)?

(c) How many nonnegative *odd* integer solutions are there to (sumx)?