Math 1111 Math Exam Study Guide

The math exam will cover the mathematical concepts and techniques we've explored this semester. The exam will not involve any codebreaking, although some questions on the exam may draw on cryptography for context. You are encouraged to bring a calculator (scientific or graphing) to the test, but you will not be allowed to use a laptop during the test.

You should be able to do each of the tasks listed below and understand the concepts associated with each task.

- Modular Arithmetic
  - Determine if two integers are congruent modulo a given integer *m*.
  - Generate a set of integers all congruent to a given integer *x* modulo a given integer *m*.
  - Simplify or solve a modular arithmetic equation.
  - Solve a system of modular arithmetic equations.
  - Calculate *x* MOD *m*, given integers *x* and *m*.
  - Simplify algebraic expressions involving the MOD operator. (See next page.)
- Prime Numbers
  - Determine if a given number is prime.
  - Find the prime factorization of a given composite number.
  - Determine if two given numbers are relatively prime.
  - Find numbers that are relatively prime to a given number.
- Common Divisors
  - Find the common divisors of a set of integers (as in the Kasiski Test).
  - Determine the greatest common divisor of two integers using the Euclidean Algorithm.
  - Express the greatest common divisor of two integers as an integer multiple of one plus an integer multiple of the other.
- Combinatorics
  - Calculate the number of permutations of *r* objects from a set of *n* objects.
  - Determine the number of unique permutations of a sequence of letters, with or without repeated letters.
  - Calculate the number of combinations of *r* objects from a set of *n* objects.
  - Calculate the number of possibilities for a given scenario using a mix of permutations and/or combinations.
- Probability
  - Compute probabilities for experiments with equally likely outcomes.
  - Compute probabilities using the basic rules of probability. (See next page.)
- Binary Numbers
  - Convert a number from decimal to binary representation, and vice versa.
  - Add or subtract binary numbers.
  - More generally, convert from decimal representation to representation in a different base, and vice versa.

- Abstract Algebra
    - Given a set and an operation defined on that set, determine if the set and operation satisfy the conditions of a mathematical group: closure, associativity, identity, inverse.

Things You Can Do with MOD

- If a, b, and n are integers, then…
    - $((a \text{ MOD } n) + (b \text{ MOD } n)) \text{ MOD n} = (a + b) \text{ MOD } n$.
    - $((a \text{ MOD } n)(b \text{ MOD } n)) \text{ MOD n} = (ab) \text{ MOD } n$.
    - $(a \text{ MOD } n)^b \text{ MOD } n = (a^b) \text{ MOD } n$.

Basic Rules of Probability

- SUM RULE: If events A and B are mutually exclusive, then the probability of A **or** B occurring equals $P(A) + P(B)$.
- PRODUCT RULE: If events A and B are independent, then the probability of A **and** B occurring is $P(A) \cdot P(B)$.
- COMPLEMENT RULE: The probability of event A **not** occurring is $1-P(A)$.

Practice Problems

1. Determine five *integer* solutions to each of the following equations.
    a. $x - 4 \equiv 5 \pmod{26}$
    b. $x + 23 \equiv 1 \pmod{4}$
    c. $5x \equiv 1 \pmod{8}$
    d. $3x + 1 \equiv 4 \pmod{5}$

2. Calculate the following.
    a. 130 MOD 26
    b. -1 MOD 5
    c. -258 MOD 16

3. Determine the prime factorization of the following numbers.
    a. 961
    b. 2310
    c. 6517

4. Find three numbers that are relatively prime to each of the following numbers.
    a. 75
    b. 310
    c. 512

5. Find all common divisors for each of the following sets of numbers.
    a. 42, 70, 126, and 154
    b. 50, 125, 275, and 300
    c. 52, 130, 182, and 468

6. Use the Euclidean algorithm to find the greatest common divisor of each pair of integers. That is, find gcd(a, b).
    a. a = 667 and b = 437
    b. a = 3001 and b = 541
    c. a = 77897 and b = 3721

7. For each of the following pairs a and b, find integers s and t such that $as + bt$ = gcd(a, b).
    a. a = 667 and b = 437
    b. a = 3001 and b = 541
    c. a = 77897 and b = 3721

8. If the letters B, C, D, F, G, H, and J are written on seven index cards…
    a. How many three-letter "words" can be formed?
    b. How many five-letter "words"?
    c. In how many ways can three of these cards be selected?
    d. In how many ways can five of them be selected?

9. Given a standard 52-card deck (that is, cards ranked Ace, 2, 3, 4, 5, 6, 7, 8, 9, 10, Jack, Queen, and King, in each of four different suits—hearts, diamonds, clubs, and spades), determine the number of each type of hand listed below that are possible on a 5-card draw.
    a. Full House – 3 cards of one rank, 2 cards of another rank
    b. Flush – 5 cards of the same suit
    c. Straight – 5 cards of consecutive ranks (ex.: 8, 9, 10, Jack, Queen)
    d. Three-of-a-Kind – 3 cards of one rank, 2 cards of other ranks

10. Tennessee auto license plates have three letters followed by three digits.
    a. How many different Tennessee plates are possible?
    b. If two Tennessee plates are selected at random, what is the probability that they will have the same three digits in the same order?
    c. How many different Tennessee plates include the letters Q, X, and Z?
    d. What is the probability that a randomly selected Tennessee plate will include the letter D?

11. Using binary representations, calculate $a + b$ and $a - b$.
    a. a = 11 011, b = 10 101
    b. a = 1 111 11, b = 101

12. Decimal representations use base 10. Binary representations use base 2. Find the decimal representation of each of the following numbers represented in base 3.
    a. 201
    b. 111
    c. 21 001

13. Find all integer solutions to the system of modular arithmetic equations:
    $y \equiv 3x + 2 \pmod 8$
    $y \equiv 5x + 4 \pmod 8$

14. Suppose a certain cipher machine has a set of five scramblers, each of which can be set in one of 26 orientations (A-Z), like the Enigma machine. Unlike the Enigma machine, these scramblers are bolted into the machine and can't be rearranged. However, each scrambler can be set to "active," in which case it affects encryption, or "inactive," in which case it doesn't. Thus, a key for this cipher machine consists of some subset of the five scramblers that are active, along with an orientation (A-Z) for each active scrambler.
    a. How many possible keys are there in which three of the scramblers are active?
    b. Suppose one of the scramblers is broken and stuck on the J orientation. Then how many possible keys are there in which three of the scramblers are active? (Note that the broken scrambler might be active, but it might not.)

15. Suppose the 8 letters V, I, G, E, N, E, R, and E are each written on a tile and placed in a bag. (You can imagine the game Scrabble, if that helps.) If you reach into the bag and draw <u>five</u> tiles at random (without replacement), what is the probability that…
    a. You draw no Es?
    b. You draw exactly 1 E?
    c. You draw at least one E?

16. Suppose the 8 letters V, I, G, E, N, E, R, and E are each written on a tile and placed in a bag. (You can imagine the game Scrabble, if that helps.) If you reach into the bag and draw <u>six</u> tiles at random (without replacement), what is the probability that…
    a. You draw all three Es?
    b. You draw exactly 2 Es?
    c. You draw no Es?

17. The largest possible 3-digit decimal number is 999. Let x be the largest possible 9-digit binary number.
    a. Represent x as a decimal number.
    b. Represent x as a base-5 number.
    c. How many digits does x have when represented as an octal (base-8) number?

18. A certain website requires that users create passwords that have exactly 8 characters. Each character can be a lowercase letter (a-z) or a digit (0-9). A password cannot consist entirely of letters, nor can it consist entirely of digits. How many possible passwords are there?

19. A military radio operator is intercepting communications from opposing forces. There's a 40% chance that a given intercept is encrypted. (Encrypted communications are sent by the radio operator to his unit's codebreaking division; unencrypted ones aren't interesting and are discarded.) If the radio operator gets to take a break after he intercepts four encrypted communications, what is the probability that he will get to take a break immediately after the eighth intercept he makes during his shift?

20. Find values for a, b, and c such that $ab \equiv ac \pmod{12}$, but it's not true that $b \equiv c \pmod{12}$. That is, find values such that you can't "cancel" the as in the equation $ab \equiv ac \pmod{12}$.

21. Let S = {0, 1, 2, 3, 4, 5, 6}. Prove that if a is a non-zero element of S, then there is some element b in S such that $ab \equiv 1 \pmod{7}$. (You can show this by brute force, checking each of the integers in S, but there's an Euclidean algorithm argument that's more elegant.)

22. Consider the following cipher. Take the 26 letters in the English alphabet and omit one of your choice. Then arrange the remaining letters in a 5x5 grid, one letter per cell, in any way you wish. To encipher a plaintext letter, replace it with the row and column number of its position in the grid. For example, here is one possible key:

	1	2	3	4	5
1	G	J	A	Z	P
2	E	T	L	Y	B
3	C	S	I	O	W
4	R	U	D	F	H
5	K	M	N	V	X

Note that the Q was omitted in this key. The plaintext "ONE" would be encrypted as "34 53 21".

a. How many possible keys does this cipher have?
b. How many possible keys does this cipher have in which the letters C, R, I, and B are in the four corners of the grid (in any order)?

23. Suppose a certain cipher machine has a set of six unique scramblers, like the Enigma machine. Unlike the Enigma machine, each scrambler consists of 31 characters: the English letters A through Z, as well as the Greek letters α, β, γ, δ, and ε. To use the cipher machine, four of these scramblers are selected and inserted into slots in the cipher machine in any order. Then each scrambler is set to any one of 31 initial orientations.

Before English plaintext reaches the scramblers, it passes through a device called a splitting board. Five English letters are selected to be split. Each of these five letters is assigned to one of the Greek letters α, β, γ, δ, and ε. (No two of these five English letters can be assigned to the same Greek letter.) When the five English letters are typed into the cipher machine, the splitting board replaces each one with its assigned Greek letter 50% of the time. This converts plaintext written in English to new text written in a mix of English and Greek letters, which then passes through the scramblers.

How many different initial settings are possible for this cipher machine?

24. A saboteur has infiltrated a chemical plant behind enemy lines. There are 24 giant holding tanks in the plant, six of which contain extremely flammable material. The saboteur has four bombs in her backpack she can use to blow up the tanks. She wants to blow up as many of the flammable tanks as she can, but she doesn't know which six contain flammable materials. (She should know, but she failed to decrypt the message that headquarters sent her.) So she places her four bombs at random on the 24 tanks.
    a. What is the probability that the saboteur will place exactly two of her bombs on the flammable tanks?
    b. What is the probability that the saboteur will place at least one of her bombs on the flammable tanks? (All she needs is one, and she'll blow up the plant, so this is the probability that she completes her mission.)

25. Suppose a certain cipher machine is set up with scramblers, each of which can be set in one of 26 orientations (A-Z), like the Enigma machine. The scramblers come in four varieties: Alpha, Bravo, Charlie, and Delta. Each of these is unique, but the machine has four copies of the Alpha scrambler, three copies of the Bravo scrambler, three copies of the Charlie scrambler, and one copy of the Delta scrambler. That makes a total of 11 scramblers, all of which are used in some sequence in the 11 slots built in the machine. A key, then, consists of a sequence of the 11 scramblers, along with an orientation (A-Z) for each scrambler.
    a. How many unique (that is, functionally different) keys are there for this cipher machine? (Note that swapping, say, an Alpha scrambler for another Alpha scrambler doesn't produce a functionally different key.)
    b. If a key is selected at random for this cipher machine, what is the probability that the Delta scrambler will be in the middle (6th) slot?

26. Consider the affine cipher $y = (mx + b) \text{ MOD } 26$, where x is an integer between 0 and 25 representing a letter in the plaintext (in the usual fashion), y is an integer between 0 and 25 representing the corresponding letter in the ciphertext, and m and b are constants, each integers between 0 and 25.

    Suppose that the plaintext “me” corresponds to the ciphertext ”PB”' under this cipher. To what

ciphertext does the plaintext ``yo'' correspond?

27. Jeff just read *The Code Book* by Simon Singh, and he's really excited about creating his own cipher. He selects 20 symbols from the nomenclator used by Mary Queen of Scots, 12 symbols appearing in a pigpen cipher, and 10 symbols from the ``Dancing Men'' cipher used in a Sherlock Holmes story. From this pool of symbols, he selects 26 to use in a monoalphabetic substitution cipher.
    a. How many unique cipher alphabets can Jeff create using this pool of symbols?
    b. How many unique cipher alphabets can Jeff create using this pool of symbols in which at least one symbol from each group (nomenclator, pigen, Dancing Men) is used?

Solutions to Practice Problems

1.
   a. …, -43, -17, 9, 35, 61, …
   b. …, -22, -18, -14, -10, -6, …
   c. …, 5, 13, 21, 29, 37, …
   d. …, 1, 6, 11, 16, 21, …

2.
   a. 0
   b. 4
   c. 14

3.
   a. 31^2
   b. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$
   c. $7^3 \cdot 19$

4.
   a. Any numbers that lack 3 or 5 as a factor
   b. Any numbers that lack 2, 5, or 31 as a factor
   c. Any numbers that lack 2 as a factor

5.
   a. 1, 2, 7, 14
   b. 1, 5, 25
   c. 1, 2, 13, 26

6.
   a. 23
   b. 1
   c. 61

7.
   a. $s = 2$, $t = -3$
   b. $s = -53$, $t = 294$
   c. $s = 15$, $t = -314$

8.
   a. 210
   b. 2520
   c. 35

d. 21

9.

a. 3744
b. 5148 (if you also count straight flushes and royal flushes)
c. 10240 (if you count straight flushes and allow both Ace-2-3-4-5 and 10-Jack-Queen-King-Ace)
d. 54912

10.

a. 17,576,000
b. 1/1000, assuming order matters, and fudging just a bit—it's actually $(26^3-1)/17{,}576{,}000$, which is just a hair under 1/1000, since you can't pick the exact same license plate twice
c. 6000
d. ≈11.1%. Hint: How many license plates have exactly one D? How many have exactly two Ds? How many have exactly three Ds?

11.

a. 110 000
b. 1 000 100

12.

a. 19
b. 13
c. 190

13. Either x = …, 3, 11, 19, …; y = …, 3, 11, 19, … or x = …, -1, 7, 15, …; y = …, -1, 7, 15, … That is, either x and y are both congruent to 3 (mod 8), or they're both congruent to 7 (mod 8).

14.

a. $C(5,3)\ 26^3 = 175{,}760$
b. $C(4,2)\ 26^2 + C(4,3)\ 26^3 = 74{,}360$

15.

a. $1/C(8,5) = 1/56$
b. $C(3/1)\ C(5,4) / C(8,5) = 15/56$
c. $1 – 1/C(8,5) = 55/56$

16.

a. $C(3,3)\ C(5,3) / C(8,6) = 5/14$
b. $C(3,2)\ C(5,4) / C(8/6) = 15/28$

c. 0

17.

a. 511
b. 4021_5
c. 3 digits

18. $36^8-26^8-10^8 = 2{,}612{,}182{,}842{,}880$

19. $C(7,3)\ (.4)^4\ (.6)^4 \approx 0.116$

20. Look for values for a that have factors in common with 12. For instance, $a = 3$, $b = 4$, $c = 8$ satisfies the given conditions.

21. If a is an element of S, then a is relatively prime to 7. It follows that $\gcd(a,7) = 1$. Using the Euclidean algorithm, we can find integers s and t such that $as + 7t = 1$. Thus $as = (-t)7 + 1$, and so $as \equiv 1 \pmod 7$. Let $b = s$ MOD 7.

22.

a. 26!
b. 4! 22!

23. $C(26,5) \cdot 5! \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 31^4 = (26! / 21!) \cdot (6! / 2!) \cdot 31^4$

24.

a. 21.6%
b. 71.2%

25.

a. $C(11,4) * C(7,3) * C(4,3) * 26^{11} \approx 1.696 \times 10^{20}$
b. 1/11

26. XZ

27.

a. $P(42,26) \approx 6.715 \times 10^{37}$
b. $P(42,26) - P(30,26) – P(32,26) \approx 6.715 \times 10^{37}$