MATH 4023-1 **Exam 1 Review** **Spring 2014**

Exam 1 will take place on Thursday, February 27. It will cover material we've discussed from Chapter 1 in Lax and from Supplement 1. A list of concepts etc. you should be familiar with is included below. In the remarks, "page S.23" refers to page 23 of the Supplement, "Theorem S.1.2.3" refers to Theorem 1.2.3 in the Supplement, while "page L.23" refers to page 23 in Lax, "Theorem L.1.2.3" refers to Theorem 1.2.3 in Lax, etc.

You may use a calculator on the exam, but be sure to show all your work to receive full (or partial) credit.

If you have questions regarding this material, be ready to ask them in class next Tuesday. You may also make use of my office hours, and/or ask questions by email.

I anticipate that the problems on the exam will be of a similar nature to those you've encountered in the homework (both collected and uncollected) - some proofs, some calculations based on results we've obtained and methods derived from them. Some review problems are included on the next page. This is **not** a comprehensive list. Additional problems may be found in the Exercises of the sections we've covered.

Some concepts, results, definitions... you should know:

The *Well-ordering principle* (page L.9): Every nonempty subset of the natural numbers has a least element.

The *Principle of mathematical induction* (pages L.9–10). You should be prepared to do proofs by induction.

For a set X, the cardinality of is denoted by $|X|$. Some formulas (see section L.1.1): $|X \cup Y| = |X| + |Y| - |X \cap Y|$, $|X \times Y| = |X||Y|$, $|\mathcal{P}(X)| = 2^{|X|}$, where $\mathcal{P}(X)$ is the power set of X, the set of all subsets of X

The *Pigeonhole principle* (page L.5). You should be prepared to work with this.

The number of ways to choose k elements (without replacement) from an n element set is $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (page L.5).

The *Binomial theorem* (page L.5): for numbers a and b, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

The *Division algorithm* (page L.10)

The definition of "b divides a" (notation $b|a$) for integers a and b (page L.10)

The definition of "the greatest common divisor of integers a and b" (notation (a, b)) (page L.11)

The *Euclidean algorithm* (page L.11), and how to use it to compute the greatest common divisor of integers a and b. Be prepared to use the matrix algorithm we discussed to compute $d = (a, b)$, and to express d as a linear combination of a and b (see pages S.11–12)

The definitions of *relatively prime integers* and *prime numbers* (e.g., pages S.15–16)

Results relating relative primeness and various divisibility conclusions (see page L.14 and page S.16)

Euclid's Lemma (Corollary L.1.2.19, page L.14): if p is prime and $p|ab$ then $p|a$ or $p|b$

The definition of "the least common multiple of integers a and b (notation $[a, b]$) (page S.21), and the relationship between the greatest common divisor, least common multiple, and the product: $ab = (a, b)[a, b]$

The *Fundamental theorem of arithmetic* (page L.14, page S.18), and how to use it to compute (a, b) and $[a, b]$ for integers a and b (e.g., Proposition S.1.2.10)

What "a is congruent to b modulo n" (notation $a \equiv b (\mathrm{mod}\, n)$) means, for integers a, b, n with $n > 0$ (page S.25), how to do arithmetic modulo n (Proposition S.1.3.3), etc.

The definition of "the congruence class of a modulo n (notation $[a]_n$) (page S.35)

The criterion for solvability of a linear congruence $ax \equiv b (\mathrm{mod}\, n)$ (Theorem S.1.3.5). Know what it means to solve a such a congruence, and be able to carry this out using the algorithm discussed in class.

The *Chinese remainder theorem* (Theorem S.1.3.6). Be able to solve systems of linear congruences of the form $ax \equiv b (\mathrm{mod}\, n)$ $cx \equiv d (\mathrm{mod}\, m)$ (first reduce to the standard form covered by the Chinese remainder theorem)

The definition of the number system $\mathbb{Z}_n$, how to do arithmetic in $\mathbb{Z}_n$: $[a]_n + [b]_n = [a + b]_n$, $[a]_n[b]_n = [ab]_n$, etc. (pages S.35–37)

The definition "$[a]_n$ is a *unit* (or *invertible element*) in $\mathbb{Z}_n$" (page S.38). Be able to compute the multiplicative inverse $[a]_n^{-1}$ of a unit $[a]_n$ using the Euclidean algorithm and/or by analyzing powers.

The definition "$[a]_n$ is a *zero divisor* in $\mathbb{Z}_n$" (page S.38)

Every (nonzero) element in $\mathbb{Z}_n$ is either a unit or a zero divisor (Proposition S.1.4.5)

$\mathbb{Z}_n^* = \{\text{units in } \mathbb{Z}_n\}$; $\mathbb{Z}_n^*$ is closed under multiplication; if p is prime, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]_p\}$ (page S.41, Corollary S.1.4.6)

Fermat's ("little") theorem (Corollary S.1.4.12)

The definition of the *Euler ϕ-function*, $\phi(n)$ (page S.40). Be able to compute $\phi(n)$ from the prime factorization of n (Proposition S.1.4.8). Know the significance of $\phi(n)$ for $\mathbb{Z}_n^*$

Euler's theorem (Theorem S.1.4.11)

Be able to compute powers of elements in $\mathbb{Z}_n$ (in various ways)

Some review problems:

1. Let X and Y be sets with cardinalities $|X| = 3$ and $|Y| = 5$.
   (a) What are the cardinalities of the sets $X \times Y$, $\mathcal{P}(X)$, and $\mathcal{P}(Y)$?
   (b) If $|X \cup Y| = 7$, what is $|X \cap Y|$?
   (c) Recall that a function $f\colon X \to Y$ is a rule which assigns to each element $x \in X$ exactly one element $f(x) \in Y$. If $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4, 5\}$, how many functions $f\colon X \to Y$ are there?
   (d) A function $f\colon X \to Y$ is injective (or one-to-one) if $f(x_1) \neq f(x_2)$ in Y whenever $x_1 \neq x_2$ in X. For $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4, 5\}$, how many injective functions $f\colon X \to Y$ are there?
2. How many LSU students would you need to insure that at least two students have the same last two digits in their LSU student ID numbers?
3. Use mathematical induction to prove that $\sum_{i=1}^{n}(3i - 2) = \frac{n(3n-1)}{2}$ for every positive integer n
4. Use mathematical induction to prove that $3^{2n} - 1$ is divisible by 8 for every positive integer n
5. Find the remainder when a is divided by b when
   (a) $a = 37$ and $b = 8$ (b) $a = -37$ and $b = 8$
6. Find the greatest common divisor $d = (4307, 1121)$ of 4307 and 1121 using the Euclidean algorithm. Express d as a linear combination of 4307 and 1121. Find the least common multiple $[4307, 1121]$ of 4307 and 1121.
7. Find the prime factorizations of 360 and 756, and use them to compute $(360, 756)$ and $[360, 756]$.
8. Determine if each of the following statements is true or false. If true, give a proof. If false, give a counterexample (an example which illustrates that it is false). In the statements, a, b, c, d, s, t are integers.
   (a) If $ab \equiv ac (\mathrm{mod}\, n)$, then $b \equiv c (\mathrm{mod}\, n)$.
   (b) If $b|a$ and $c|a$, then $bc|a$.
   (c) If $(a, b) = 1$, then $(a + b, ab) = 1$.
   (d) If $as + bt = d$, then $d = (a, b)$.
   (e) a^2 is equivalent to either 0 or 1 modulo 4.
9. This involves arithmetic modulo 16. Express answers in the form $[a]_{16}$, where a is an integer with $0 \leq a < 16$.
   (a) Compute $[5]_{16} + [13]_{16}$
   (b) Compute $[5]_{16}[13]_{16}$
   (c) Compute $[5]_{16}^{-1}$
   (d) How many elements does $\mathbb{Z}_{16}^*$ have? List them, and find their multiplicative inverses.
   (e) Find all zero divisors in $\mathbb{Z}_{16}$
10. Find all the solutions (when there are any) of the following linear congruences:
    (a) $8x \equiv 6 (\mathrm{mod}\, 14)$ (b) $66x \equiv 100 (\mathrm{mod}\, 121)$ (c) $12x \equiv 14 (\mathrm{mod}\, 91)$
11. Solve the systems of congruences:
    (a) $x \equiv 7 (\mathrm{mod}\, 11)$ $x \equiv 4 (\mathrm{mod}\, 24)$ (b) $3x \equiv 11 (\mathrm{mod}\, 17)$ $2x \equiv 3 (\mathrm{mod}\, 13)$
12. Does a system of congruences $x \equiv a (\mathrm{mod}\, n)$ $x \equiv b (\mathrm{mod}\, m)$ always have a solution?
13. Compute the Euler ϕ-function $\phi(n)$ for the natural numbers $n = 360$ and $n = 756$
14. Compute $10^{195} (\mathrm{mod}\, 97)$ and $11^{195} (\mathrm{mod}\, 360)$ note: 97 is prime
    Find expressions for the multiplicative inverses of $[10]_{97}$ in $\mathbb{Z}_{97}$ and $[11]_{360}$ in $\mathbb{Z}_{360}$ if possible.

Answers to the review problems:

1. (a) $|X \times Y| = 15 \quad |\mathcal{P}(X)| = 2^3 = 8 \quad |\mathcal{P}(Y)| = 2^5 = 32$
   (b) $|X \cap Y| = |X| + |Y| - |X \cup Y| = 1$
   (c) There are $5^3 = 125$ functions $f\colon X \to Y$ (5 possibilities for each of $f(a)$, $f(b)$, and $f(c)$)
   (d) There are $5 \cdot 4 \cdot 3 = 60$ injective functions $f\colon X \to Y$ (5 possibilities for $f(a)$, then 4 possibilities for $f(b) \neq f(a)$, then 3 possibilities for $f(c) \neq f(a), f(b)$)

2. There are $10 \cdot 10 = 100$ possible last two digits, so by the pigeonhole principle, if you had 101 students, at least two would have the same last two digits.

3. For $n \in \mathbb{P}$, a natural number, let $P(n)$ be the statement $\sum_{i=1}^{n}(3i-2) = \frac{2(3n-1)}{2}$, that is,

   $(3 \cdot 1 - 2) + (3 \cdot 2 - 2) + \cdots + (3 \cdot n - 2) = \frac{n(3n-1)}{2}$.

   Since $1 = 3 \cdot 1 - 2 = \frac{1(3 \cdot 1 - 1)}{2} = 1$, it follows that $P(1)$ is true, which establishes the base step for induction.

   Assume that $P(k)$ is true for some $k \in \mathbb{P}$. That is, $\sum_{i=1}^{k}(3i-2) = \frac{k(3k-1)}{2}$. Then

   $$\sum_{i=1}^{k+1}(3i-2) = \sum_{i=1}^{k}(3i-2) + (3(k+1)-2) = \frac{k(3k-1)}{2} + (3(k+1)-2) = \frac{3k^2+5k+2}{2} = \frac{(k+1)(3k+2)}{2}$$

   Since $\frac{(k+1)(3k+2)}{2} = \frac{(k+1)(3(k+1)-1)}{2}$, we see that $P(k+1)$ is true whenever $P(k)$ is true, which verifies the inductive step. So, by the principle of mathematical induction, the statement $P(n)$ is true for all $n \in \mathbb{P}$, that is $\sum_{i=1}^{n}(3i-2) = \frac{2(3n-1)}{2}$.

4. For $n \in \mathbb{P}$, let $P(n)$ be the statement $8|(3^{2n}-1)$. Since $3^2 - 1 = 8$ is divisible by 8, it follows that $P(1)$ is true. Assume that $P(k)$ is true, that is, $8|(3^{2k}-1)$. Then $3^{2k} - 1 = 8q$ for some $q \in \mathbb{Z}$. Then $3^{2(k+1)} - 1 = 9 \cdot 3^{2k} - 1 = 9 \cdot 3^{2k} - 9 + 9 - 1 = 9(3^{2k}-1) + 8 = 9(8q) + 8 = 8(9q+1)$. Thus, 8 divides $3^{2(k+1)} - 1$, and we see that $P(k+1)$ is true whenever $P(k)$ is true. So, by induction, $P(n)$ is true for all $n \in \mathbb{P}$, that is, $8|(3^{2n}-1)$.

5. (a) $37 = 8 \cdot 4 + 5$ so the remainder is 5 (b) $-37 = 8(-5) + 3$ so the remainder is 3

6. $\begin{bmatrix} 1 & 0 & 4307 \\ 0 & 1 & 1121 \end{bmatrix} \xrightarrow{R1-3R2} \begin{bmatrix} 1 & -3 & 944 \\ 0 & 1 & 1121 \end{bmatrix} \xrightarrow{R2-R1} \begin{bmatrix} 1 & -3 & 944 \\ -1 & 4 & 177 \end{bmatrix} \xrightarrow{R1-5R2} \begin{bmatrix} 6 & -23 & 59 \\ -1 & 4 & 177 \end{bmatrix} \xrightarrow{R2-3R2} \begin{bmatrix} 6 & -23 & 59 \\ -19 & 73 & 0 \end{bmatrix}$

   $(4307, 1121) = 59 \quad 4307(6) + 1121(-23) = 59 \quad [4307, 1121] = \frac{4307 \cdot 1121}{59} = 81833$

7. $360 = 2^3 \cdot 3^2 \cdot 5 \quad 756 = 2^2 \cdot 3^3 \cdot 7 \quad (360, 756) = 2^2 \cdot 3^2 = 36 \quad [360, 756] = 2^3 \cdot 3^3 \cdot 5 \cdot 7 = 7560$

8. (a) false: For example, $2 \cdot 3 \equiv 2 \cdot 1 (\mathrm{mod}\, 4)$, but $3 \not\equiv 1 (\mathrm{mod}\, 4)$.
   (b) false: For example, $6|12$ and $4|12$, but 24 does not divide 12.
   (c) true: Let $d = (a+b, ab)$. Then there are integers s, t so that $d = (a+b)s + abt$. Since $(a+b)s + abt = a(s+bt) + bs$, we see that d is a common divisor of a and b. Since $(a, b) = 1$, we must have $d = 1$.
   (d) false: For example, $5 = 2 \cdot 1 + 3 \cdot 1$, but $(2, 3) = 1$.
   (e) true: a is either even or odd. If $a = 2k$ is even, then $a^2 = 4k^2 \equiv 0 (\mathrm{mod}\, 4)$. If $a = 2k+1$ is odd, then $a^2 = 4k^2 + 4k + 1 \equiv 1 (\mathrm{mod}\, 4)$.

9. (a) $[5]_{16} + [13]_{16} = [2]_{16}$
   (b) $[5]_{16}[13]_{16} = [1]_{16}$
   (c) $[5]_{16}^{-1} = [13]_{16}$
   (d) $|\mathbb{Z}_{16}^*| = 8 \quad \mathbb{Z}_{16}^* = \{[1]_{16}, [3]_{16}, [5]_{16}, [7]_{16}, [9]_{16}, [11]_{16}, [13]_{16}, [15]_{16}\} \quad [1]_{16}^{-1} = [1]_{16}$, $[3]_{16}^{-1} = [11]_{16}$, $[5]_{16}^{-1} = [13]_{16}$, $[7]_{16}^{-1} = [7]_{16}$, $[9]_{16}^{-1} = [9]_{16}$, $[11]_{16}^{-1} = [3]_{16}$, $[13]_{16}^{-1} = [5]_{16}$, $[15]_{16}^{-1} = [15]_{16}$
   (e) $[2]_{16}$, $[4]_{16}$, $[6]_{16}$, $[8]_{16}$, $[10]_{16}$, $[12]_{16}$, $[14]_{16}$

10. (a) $[6]_{14}$, $[13]_{14}$ (b) no solution (c) $[77]_{91}$

11. (a) $[172]_{264}$ (b) $[151]_{221}$

12. No. If m and n are not relatively prime, there may be no solution.

    For example, $x \equiv 0 (\mathrm{mod}\, 2)$ $x \equiv 1 (\mathrm{mod}\, 2)$ has no solution.

13. $\phi(360) = 96$ $\phi(756) = 216$

14. Since 97 is prime, by Fermat's little theorem, $10^{97} \equiv 10 (\mathrm{mod}\, 97)$. So $10^{96} \equiv 1 (\mathrm{mod}\, 97)$. Since $195 = 96 \cdot 2 + 3$, we have $10^{195} = 10^{96 \cdot 2 + 3} = (10^{96})^2 \cdot 10^3 \equiv 10^3 (\mathrm{mod}\, 97) \equiv 30 (\mathrm{mod}\, 97)$.

    Since $\phi(360) = 96$ and $(11, 360) = 1$, by Euler's theorem, $11^{96} \equiv 1 (\mathrm{mod}\, 360)$. Since $195 = 96 \cdot 2 + 3$, we have $11^{195} = 11^{96 \cdot 2 + 3} = (11^{96})^2 \cdot 11^3 \equiv 11^3 (\mathrm{mod}\, 360) \equiv 251 (\mathrm{mod}\, 360)$

    Since $10^{96} \equiv 1 (\mathrm{mod}\, 97)$, we have $[10]_{97}^{-1} = [10^{95}]_{97}$. This turns out to be equal to $[68]_{97}$.

    Since $11^{96} \equiv 1 (\mathrm{mod}\, 360)$, we have $[11]_{360}^{-1} = [11^{95}]_{360}$. This turns out to be equal to $[131]_{360}$.