MATH 4023-1 **Exam 2 Review** **Spring 2014**

Exam 2 will take place on Thursday, April 10. It will cover material we've discussed since Exam 1: RSA Encryption [Lax §IV.5, Supplement 2, and related material], and the theory of groups (and related structures) [Lax Chapter III, §§1–4,8,9, Supplement 3, and related discussion]. The material is cumulative, and to some extent depends on previous material, which you should still know. A (not necessarily comprehensive) list of concepts etc. you should be familiar with is included below. In these remarks, all references refer to pages, sections, results, and so on in Lax.

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 and supplements we've covered.

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

Be comfortable encrypting and decrypting using the RSA cryptosystem (§IV.5, Supplement 2). This involves computing powers by successive squaring (as discussed in the relevant handout).

Know the definitions of *group*, *monoid*, and *semigroup*, and the differences between these structures (page 62). While our main focus is on groups, you should be aware of these other notions. Know the definition of an *abelian group* (page 62).

Know, and be comfortable working with, examples of groups such as the integers $(\mathbb{Z}, +)$, the integers modulo n $(\mathbb{Z}_n, +)$, the symmetric group S_n, the dihedral group D_n (§§III.1, III.2, III.8,III.9). What are the elements of these groups? What are the group operations? Which of these groups are abelian? For those of these groups that are finite, what is the order of the group?

Know the cancellation laws in a group (Proposition 2.7, page 64). For instance, if $ab = ac$ in a (multiplicative) group G, then $b = c$ in G.

Know exponential rules in a group (page 65). For instance, $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$, $(ab)^{-1} = b^{-1}a^{-1}$.

Know the definition of a *subgroup* (page 68). Know the criterion to be a subgroup, and be able to use it to check if a subset H is a subgroup of a group G (Proposition 3.8, page 70).

Know the definition of the *center* $Z(G)$ of a group G (page 71). Prove that $Z(G)$ is a subgroup of G.

What is a *cyclic group*? What is a *generator* of a cyclic group? A cyclic group is abelian. A subgroup of a cyclic group is cyclic. (pages 72, 74)

For brevity, denote an element $[a]_n$ in $\mathbb{Z}_n$ by simply a. Under what condition does a have a multiplicative inverse in $\mathbb{Z}_n$? (Answer: when a and n are relatively prime.) When a has a multiplicative inverse, able to find it (e.g., using the Euclidean algorithm). The set $\mathbb{Z}_n^*$ of all units in $\mathbb{Z}_n$ is a group, with group operation given by multiplication.

Know the definition of the *order* $|G|$ of a group G. Know the definition of the order $o(g)$ of an element $g \in G$. If G is a finite group, know the relationship between $o(g)$ and $|(g)|$, the order of g and the order of the cyclic subgroup generated by g. (page 73)

Know what the *left cosets* of a subgroup H of a group G are. For $a \in G$, $aH = \{ah \colon h \in H\}$. These are the equivalence classes of the equivalence relation $a \equiv_H b \iff a^{-1}b \in H$. (page 76). If there are finitely many distinct left cosets of H in G, the number of distinct left cosets is $[G \colon H]$, the *index* of H in G. (page 78)

Lagrange's Theorem (page 78): If G is a finite group and H is a subgroup of G, then $|G| = [G \colon H] \cdot |H|$.

Consequences of Lagrange's Theorem: If G is a finite group, the order of any subgroup divides the order of G. In particular, the order of any element of G divides the order of G; If $a \in G$, then $a^{|G|} = e$; if $|G| = p$ is prime, then G is cyclic. (page 78)

The *dihedral group* $D_n = \{e, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \beta, \alpha\beta, \alpha^2\beta, \ldots, \alpha^{n-1}\beta\}$ is the group of symmetries of a regular polygon with n sides, with operation given by composition of symmetries. $|D_n| = 2n$ (§III.1 and pages 106–107)

The *symmetric group* S_n is the group of all permutations of the set $[n] = \{1, 2, \ldots, n\}$, with operation given by composition of permutations. $|S_n| = n!$ (§III.1 and pages 108–112)

Know how to represent permutations in the two row notation, and know how to compose/multiply permutations in this notation. (page 56)

Know what a *cycle of length r* is (page 108). A cycle of length 2 is a *transposition* (page 111).

Know what it means for two cycles to be *disjoint*. Disjoint cycles commute (page 109). Know the algorithm for expressing an arbitrary permutation in S_n as a product of disjoint cycles (the "cycle decomposition" - see the proof of Lemma 8.5 on page 109).

Be comfortable going back and forth between the two row notation for permutations and cycle decompositions. Be able to multiply permutations in either format, and be able to express the result in either format.

Be able to compute the order of a permutation from the cycle decomposition (page 110).

Every cycle in S_n is a product of transpositions (cycles of length 2). Every permutation in S_n is a product of transpositions. Know the definitions of *even* and *odd* permutations. (pages 111–112)

The *alternating group* A_n is the group of all even permutations in S_n. A_n is a subgroup of S_n, and $|A_n| = n!/2$. (page 112)

Know the definition of a left action of a group G on a set X. In this context, know what the *orbits* of G on X are, and that they form a partition of X. (pages 118–119)

If $x \in X$, the *orbit of* x is the set $\mathcal{O}_x = \mathrm{Orb}(x) = \{gx \colon g \in G\}$

If G acts on X and $x \in X$, the *stabilizer of* x is $G_x = \{g \in G \colon gx = x\}$. G_x is a subgroup of G. (page 120)

The *Orbit-Stabilizer Theorem*: If a finite group G acts on a finite set X and $x \in X$, then $[G \colon G_x] = |\mathcal{O}_x|$. (page 121, Proposition 9.11) This can be rephrased as $|\mathcal{O}_x| = |G|/|G_x|$ or $|\mathcal{O}_x| \cdot |G_x| = |G|$. A consequence: If x and y are in the same orbit, then $|G_x| = |G_y|$. (page 122)

If G acts on X and $g \in G$, the *fixed set of* g is $X_g = \{x \in X \colon gx = x\}$. X_g is a subset of X. (page 122)

Know the *Burnside Theorem* (stated on page 122): If a finite group G acts on a finite set X, then the number N of orbits of G on X is given by $N = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} |X_g|$. This can be thought of as saying that the number of orbits is the average (as g varies over G) of the number of elements of X fixed by the element g of G.

Be able to use the Burnside Theorem to solve "coloring" problems (as in §III.9 and Supplement 3).

Some review problems:

1. Let $e = 19$ and $n = 2759 = (31)(89)$.
   (a) Encrypt the message MATH. (b) Decrypt the ciphertext 1771.
2. Let G be a group and $a, b, c, d \in G$. If $a^{-1}bc^2 = d$:
   (a) find a in terms of b, c, d (b) find b in terms of a, c, d.
3. Let $\mathbb{C}^*$ be the multiplicative group of nonzero complex numbers. That is, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, and the group operation on $\mathbb{C}^*$ is multiplication. Let $G = \{1, i, -1, -i\} \subset \mathbb{C}^*$.
   (a) Make a multiplication table for G, and show that G is a subgroup of $\mathbb{C}^*$.
   (b) Show that $S = \{1, i\}$ is not a subgroup of G.
   (c) Show that G is cyclic, and find all generators of G.
4. Consider the permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ in S_4. Compute:
   (a) $\sigma\tau$ (b) $\tau\sigma$ (c) σ^2 (d) τ^2 (e) τ^3 (f) τ^4 (g) σ^{-1} (h) τ^{-1}
5. Consider the permutations $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$ in S_5.
   (a) If $\alpha\gamma = \beta$, find γ. (b) If $\delta\alpha = \beta$, find δ. (c) If $\alpha\nu\alpha^{-1} = \beta$, find ν.
6. Let G be a group, and a an element of G. The *centralizer* of a in G is $C(a) = \{g \in G \colon ga = ag\}$.
   (a) Show that $C(a)$ is a subgroup of G.
   (b) If $G = D_4$ and $a = \beta$ is horizontal reflection (see p. 58), find $C(\beta)$.
7. Let G be a group with $|G| = 21$.
   (a) What are the possible orders of elements of G?
   (b) If H is a subgroup of G and H is not equal to G, explain why H must be cyclic.
   (c) If G is a subgroup of a group K, and L is a subgroup of a group L, with $|L| = 105$, what are the possible values of $|K|$?

8. Let $H = 5\mathbb{Z} = \{5k : k \in \mathbb{Z}\}$. Check that H is a subgroup of $(\mathbb{Z}, +)$. Since the group operation is $+$, cosets of H are written as $a + H$ (as opposed to aH). Determine whether the following cosets of H are the same:

   (a) $11 + H$ and $26 + H$ (b) $13 + H$ and $-7 + H$ (c) $96 + H$ and $-1 + H$

9. Find all left cosets of H in G:

   (a) $G = \mathbb{Z}_{24}$, $H = (4)$ (b) $G = S_3$, $H = (\,(13)\,)$ (c) $G = D_4$, $H = (\beta)$ β is horizontal reflection, see p. 58

10. Write each of the following permutations as a product of disjoint cycles.

    (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 5 & 3 & 2 \end{pmatrix}$ (c) $(12)(13)(14)$ (d) $(13)^{-1}(24)(235)^{-1}$

    (e) $(145)(1234)(13)$ (f) $(123)^{-1}(23)(123)$

11. Consider the symmetric group S_n, and the permutations $\alpha = (123456)$ and $\beta = (12)(456)$.

    (a) Write α and β in two row notation.

    (b) Express α^{-1} and α^2 as products of disjoint cycles.

    (c) Express β as a product of transpositions. Is β even or odd?

    (d) If n is large, there are disjoint cycles λ and μ in S_n of orders 9 and 6. What is the order of $\theta = \lambda\mu$?

12. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, and let $G = \{e, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$ be the subgroup of S_4 generated by α and β. G acts on the set $X = \{1, 2, 3, 4\} \times \{1, 2, 3, 4\}$: if $\sigma \in G$, then $\sigma(i, j) = (\sigma(i), \sigma(j))$.

    (a) For $x = (1, 1)$, $y = (1, 3)$, and $z = (1, 4)$ in X, find the orbits $\mathcal{O}_x$, $\mathcal{O}_y$, $\mathcal{O}_z$, and the stabilizers G_x, G_y, G_z.

    (b) Find the partition of X given by the orbits of G.

    (c) For elements $g = \alpha^2\beta$ and $h = \alpha^3\beta$ of G, find the fixed sets X_g and X_h.

13. Find the number of different regular pentagons with vertices colored red, white, or blue.

14. A wheel is divided evenly into 5 compartments. Each compartment can be painted red, white, or blue. The back of the wheel is painted black. How many different such color wheels are there?

15. Find the number of distinct bracelets consisting of six beads, where each bead is either red, white, or blue.

16. Let X be the set of all 6-digit binary words–strings of length 6 composed of 0's and 1's, e.g., 010110. In some applications, two such words are considered equivalent if one can be obtained from the other by applying the cyclic permutation σ

$$a_1a_2a_3a_4a_5a_6 \mapsto a_6a_1a_2a_3a_4a_5$$

    some number of times. For instance, 010110 is equivalent to 110010 (apply σ to the first word 3 times). Find the number of non-equivalent words.

Answers to the review problems:

1. (a) 0123 0265 (b) UP

2. (a) $a = bc^2d^{-1}$ (b) $b = adc^{-2}$

3. (a) From the multiplication table for G, check that ab^{-1} is in G for all $a, b \in G$. So G is a subgroup of $\mathbb{C}^*$.

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

   (b) Note that $i^{-1} = -i$. Since $1 \cdot i^{-1} = -i$ is not in S, S is not a subgroup of G.

   (c) Since $(i) = \{i^0, i^1, i^2, i^3\} = \{1, i, -1, -i\}$, we have $G = (i)$. That is, i is a generator of the cyclic group G. Similarly, $-i$ is another generator of G.

4. (a) $\sigma\tau = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$ (b) $\tau\sigma = \begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$ (c) $\sigma^2 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ (d) $\tau^2 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$

   (e) $\tau^3 = \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$ (f) $\tau^4 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ (g) $\sigma^{-1} = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$ (h) $\tau^{-1} = \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$

5. Check that $\alpha^{-1} = \begin{pmatrix}1&2&3&4&5\\3&1&4&5&2\end{pmatrix}$.

   (a) $\gamma = \alpha^{-1}\beta = \begin{pmatrix}1&2&3&4&5\\2&3&4&1&5\end{pmatrix}$ (b) $\delta = \beta\alpha^{-1} = \begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix}$ (c) $\nu = \alpha^{-1}\beta\alpha = \begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix}$

6. (a) Fix $a \in G$. Note that $C(a)$ is nonempty since the identity element e of G is in $C(a)$ (as $ea = a = ae$). Let $g, h \in C(a)$. To show that $C(a)$ is a subgroup of G, it is enough to show that gh^{-1} is in $C(a)$. We have $ga = ag$ and $ha = ah$ since $g, h \in C(a)$. Using the group cancellation laws, the second of these equalities shows that $ah^{-1} = h^{-1}a$, so $h^{-1} \in C(a)$. Now compute $(gh^{-1})a = g(h^{-1}a) = g(ah^{-1}) = (ga)h^{-1} = (ag)h^{-1} = a(gh^{-1})$. This shows that $gh^{-1} \in C(a)$, and $C(a)$ is a subgroup of G.

   (b) $C(\beta) = \{e, \alpha^2, \beta, \alpha^2\beta\}$.

7. (a) For $g \in G$, since $o(g) = |(g)|$ divides $|G|$, the possible orders of elements of G are $1, 3, 7, 21$.

   (b) If H is a "proper" subgroup of G (that is, $H \neq G$), and $|H|$ divides $|G|$ by Lagrange's Theorem, the order of H must be 1, 3, or 7. If $|H| = 1$, then $H = \{e\}$ is cyclic. If $|H|$ is 3 or 7, then $|H|$ is prime, and H must be cyclic (see Corollary 4.11, page 78).

   (c) Since G is a subgroup of K, $|K|$ must be a multiple of $|G| = 21$. Since K is a subgroup of L, $105 = |L|$ must be a multiple of $|K|$. So $|K|$ is a multiple of 21 which divides 105, and the possible values of $|K|$ are 21 and 105.

8. Note that $0 = 5 \cdot 0$ is in H (so $H \neq \emptyset$). If $a = 5k$ and $b = 5l$ are in H, then $a - b = 5(k - l)$ is in H, so H is a subgroup of $\mathbb{Z}$.

   (a) Since $11-26 = -15 = -3\cdot5 \in H$, $11+H = 26+H$ (b) Since $13+7 = 20 = 4\cdot5 \in H$, $13+H = -7+H$

   (c) Since $96 + 1 = 97 \notin H$, $96 + H \neq -1 + H$

9. (a) $H = \{0, 4, 8, 12, 16, 20\}$, $1+H = \{1, 5, 9, 13, 17, 21\}$, $2+H = \{2, 6, 10, 14, 18, 22\}$, $3+H = \{3, 7, 11, 15, 18, 23\}$
   Note: $H = 4 + H = 8 + H = 12 + H = \ldots$, $1 + H = 5 + H = 9 + H = 1 \ldots$, etc.

   (b) $H = \{e, (13)\}$, $(12)H = \{(12), (132)\}$, $(23)H = \{(23), (123)\}$ writing (all 6) elements of S_3 as cycles
   Note: $(123)H = (23)H$, $(132)H = (12)H$

   (c) $H = \{e, \beta\}$, $\alpha H = \{\alpha, \alpha\beta\}$, $\alpha^2 H = \{\alpha^2, \alpha^2\beta\}$, , $\alpha^3 H = \{\alpha^3, \alpha^3\beta\}$
   Note: $\alpha^k\beta H = \alpha^k H$ (for $k = 1, 2, 3$)

10. (a) $(136)(25)$ (b) $(26)(345)$ (c) (1432) (d) (13425) (e) $(15)(23)$ (f) (12)

11. (a) $\alpha = \begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix}$ $\beta = \begin{pmatrix}1&2&3&4&5&6\\2&1&3&5&6&4\end{pmatrix}$

    (b) $\alpha^{-1} = (165432)$ $\alpha^2 = (135)(246)$

    (c) $\beta = (12)(46)(45)$ is an odd permutation

    (d) The order of $\theta = \lambda\mu$ is the least common multiple of 9 and 6, which is 18

12. (a) $\mathcal{O}_x = \{(1,1), (2,2), (3,3), (4,4)\}$ $\mathcal{O}_y = \{(1,3), (3,1), (2,4), (4,2)\}$
    $\mathcal{O}_z = \{(1,4), (4,1), (1,2), (2,1), (2,3), (3,2), (3,4), (4,3)\}$ $G_x = \{e, \alpha^3\beta\}$ $G_y = \{e, \alpha^3\beta\}$ $G_z = \{e\}$

    (b) The three orbits found in part (a) exhaust X and are disjoint. $X = \mathcal{O}_x \cup \mathcal{O}_y \cup \mathcal{O}_z$

    (c) No element of X is fixed by g, so $X_g = \emptyset$. $X_h = \{(1,1), (1,3), (3,1), (3,3)\}$.

13. Let X be the set of all 3-colorings of the vertices of the pentagon. Then, $|X| = 3^5 = 243$. The group of symmetries of the pentagon is $D_5 = \{e, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta, \alpha^4\beta\}$, where α^k, $k = 1, 2, 3, 4$, are nontrivial rotations, and $\alpha^k\beta$, $k =, 01, 2, 3, 4$, are reflections. The identity e in D_5 fixes every element of X, so $|X_e| = 243$. Each nontrivial rotation α^k fixes only those colorings where every vertex has the same color, so $X_{\alpha^k}| = 3$ for $k = 1, 2, 3, 4$. Each reflection fixes those colorings for which the vertices permuted by the reflection are colored the same, so $|X_{\alpha^k\beta}| = 3^3 = 27$ for $k = 0, 1, 2, 3, 4$. By the Burnside Theorem, the number of different colorings is $N = (243 + 4 \cdot 3 + 5 \cdot 27)/10 = 39$.

14. Let X be the set of all 3-colorings of the (front of the) wheel. Then, $|X| = 3^5 = 243$. Since the back of the wheel is painted black, the group of symmetries here is the subgroup $G = \{e, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ of D_5 consisting only of rotations. As above, the identity $e \in G$ fixes every coloring, $|X_e| = 243$, and each nontrivial rotation fixes the colorings where each compartment has the same color, $|X_{\alpha^k}| = 3$ for $k = 1, 2, 3, 4$. So by the Burnside Theorem, the number of different color wheels is $N = (243 + 4 \cdot 3)/5 = 51$.

15. Let X be the set of all 6 bead bracelets, where each bead is either red, white, or blue. Then, $|X| = 3^6 = 729$. The relevant group of symmetries is the dihedral group D_6, the group of symmetries of the regular hexagon, consisting of rotations by multiples of 60 degrees (counterclockwise), and six reflections.

    The identity element fixes all of X, and as noted above, $|X| = 3^6$.

    Rotation by 60° fixes only those bracelets which are made of the same color, there are 3 such bracelets. The same holds for rotation by 300°. Rotation by 120° fixes bracelets with 3 beads one color, and 3 another (possibly the same) color, there are 3^2 such bracelets. The same holds for rotation by 240°. Rotation by 180°. fixes bracelets with 2 beads one color, 2 beads another color, and 2 beads yet another color (there may be coincidences among these colors), there are 3^3 such bracelets.

    A reflection in D_6 either fixes a pair of beads (vertices) or fixes no beads, and there are three of each type. If a reflection fixes a pair of beads, these beads can be any color, while beads in the other two pairs must be the same color, there are 3^4 such bracelets. If a reflection fixes no pair of beads, beads in the three pairs must be the same color, there are 3^3 such bracelets.

    Using these observations and the Burnside Theorem, the number of bracelets is
    $N = (3^6 + 2 \cdot 3 + 2 \cdot 3^2 + 3^3 + 3 \cdot 3^3 + 3 \cdot 3^4)/12 = 92$.

16. Since X is the set of 6-digit binary words, $|X| = 2^6 = 64$. The relevant group of symmetries is the cyclic group G generated by the cyclic permutation $\sigma = (123456)$. The elements of G are the identity $e = \sigma^0$, σ, $\sigma^2 = (135)(246)$, $\sigma^3 = (14)(25)(36)$, $\sigma^4 = (153)(264)$, $\sigma^5 = (165432)$.

    Check that $|X_e| = 2^6$, $|X_\sigma| = |X_{\sigma^5}| = 2$, $|X_{\sigma^2}| = |X_{\sigma^4}| = 2^2$, and $|X_{\sigma^3}| = 2^3$. Then, the number of non-equivalent words is the number N of orbits of G on X, which by the Burnside Theorem is
    $N = (2^6 + 2 \cdot 2 + 2 \cdot 2^2 + 2^3)/6 = 14$.