The second exam will be on Friday, October 24, 2008. The syllabus will be RSA cryptography from section 1.6 plus sections 2.1, 2.2, 2.3, 4.1, and 4.2. Of course, the material is cumulative, and the listed sections depend on earlier sections, which it is assumed that you still know.

Following are some of the concepts and results you should know:

- Know how to encipher and decipher using the RSA scheme.
- Know the algebra of set combinations (Theorem 2.1.1).
- Know the definition of function and the basic properties of functions: surjective, injective, bijective, composition of functions, inverse of a function, criterion for when \( f : X \to Y \) has an inverse \( f^{-1} \).
- The cardinality of \( X \), denoted \(|X|\), is the number of elements of \( X \). Some formulas for the cardinality of combinations of sets \( X \) and \( Y \):
  1. \(|X \cup Y| = |X| + |Y| - |X \cap Y|\).
  2. \(|X \times Y| = |X||Y|\).
  3. \(|\mathcal{P}(X)| = 2^{|X|}\) where \( \mathcal{P}(X) \) denotes the power set of \( X \), that is, \( \mathcal{P}(X) \) is the set of all subsets of \( X \).
  4. \(|\{\text{all functions } f : X \to Y\}| = |Y|^{|X|}\).
- Know how to check if a relation is a partial order (reflexive, weakly antisymmetric, and transitive) or an equivalence relation (reflexive, symmetric, and transitive).
- Know the relationship between equivalence relations and partitions. Know what the equivalence classes \([a]_R\) of an equivalence relation are?
- \( S(n) \) denotes the set of all permutations of the set \( \{1, \ldots, n\} \) of integers from 1 to \( n \). The cardinality of \( S(n) \) is \(|S(n)| = n!\).
- Know how to represent permutations in the two rowed notation, and how to multiply permutations using this notation.
- Know what a cycle of length \( r \) is. A cycle of length 2 is a transposition.
- Know what is means to say that a permutation \( \pi \in S(n) \) moves an integer \( k \) and what it means to say that \( \pi \) fixes \( k \).
- Know what it means to say that two permutations \( \pi \) and \( \sigma \) are disjoint.
- (Theorem 4.1.2) Disjoint permutations commute.
- Know how to compute the cycle decomposition of permutations in \( S(n) \).
- Know how to go back and forth between two rowed notation for permutations and cycle decompositions. Know how to multiply permutations given in either format and express the result in either two rowed or cycle notation.
- Know the rules of exponents for a permutation (Theorem 4.2.1).
- Know what is meant by the order of a permutation: \( \text{ord}(\pi) \) is the smallest positive integer \( k \) such that \( \pi^k = \text{id} \).
The order of an \( r \)-cycle is \( r \) (Theorem 4.2.4).

(Lemma 4.2.5) If \( \pi \) and \( \sigma \) are disjoint permutations, then \( \text{ord}(\pi \sigma) = \text{lcm}(\text{ord}(\pi), \text{ord}(\sigma)) \).

Know how to compute the order of a permutation from the cycle structure. (Theorem 4.2.6): If \( \pi = \tau_1 \tau_2 \cdots \tau_k \) is a product of disjoint cycles, then the order of \( \pi \) is the least common multiple of the lengths of the cycles \( \tau_1, \ldots, \tau_k \).

A transposition is a cycle of length 2. Every permutation is a product of transpositions. The number of transpositions in such a product for a permutation \( \sigma \) is always even or always odd. \( \sigma \) is even if it is a product of an even number of transpositions; \( \sigma \) is odd if it is a product of an odd number of transpositions.

An \( r \)-cycle \( (j_1, j_2, \ldots, j_r) \) is an even permutation if \( r \) is odd and it is odd if \( r \) is even. This follows from the factorization
\[
(j_1 j_2 \cdots j_r) = (j_1 j_r) (j_1 j_{r-1}) \cdots (j_1 j_2).
\]

What are even and odd permutations and how can the parity be computed from the cycle decomposition. (Theorems 4.2.10 and 4.2.11)

Review Exercises

Be sure that you know how to do all assigned homework exercises. The following are a few supplemental exercises similar to those already assigned as homework. These exercises are listed randomly. That is, there is no attempt to give the exercises in the order of presentation of material in the text.

1. Let \( p = 29 \) and \( q = 31 \) so that \( n = pq = 899 \), and let \( e = 101 \) in the RSA algorithm.
   (a) Compute \( d \) so that \( ed \equiv 1 \mod \varphi(899) \).

   \[ \text{Solution.} \] Use the Euclidean algorithm to compute that \( d = 341 \).

   (b) Using the public key \((899, 101)\), explain how to encrypt a message consisting of a single number \( M \). That is, what do you do to \( M \) to send it as an encrypted message?

   \[ \text{Solution.} \] Compute \( N = M^{101} \mod 899 \).

   (c) If the message \( N \) was received, explain how you would decrypt this message.

   \[ \text{Solution.} \] Compute \( N^{341} \mod 899 \).

2. (a) Give an example of a function \( f : \mathbb{Z} \to \mathbb{Z} \) (\( \mathbb{Z} \) is the set of integers) such that \( f \) is injective but not surjective.

   \[ \text{Solution.} \] Let \( f : \mathbb{Z} \to \mathbb{Z} \) be defined by \( f(n) = 2n \). Since \( 2n = 2m \) implies \( n = m \), \( f \) is injective and since \( 1 \neq f(n) \) for any \( n \in \mathbb{Z} \), \( f \) is not surjective.

   (b) Give an example of a function \( g : \mathbb{Z} \to \mathbb{Z} \) such that \( g \) is surjective but not injective.
Solution. Define $g : \mathbb{Z} \to \mathbb{Z}$ by the formula $g(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}$. Since $n = (2n)/2 = g(2n)$, $g$ is surjective. However, $g(1) = 0 = g(3)$ so $g$ is not injective.

(c) Give an example of a bijection $h : \mathbb{Z}^+ \to Y$ where $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ and $Y = \{2, 3, 4, \ldots\}$.

Solution. Define $h$ by $h(n) = n + 1$. The inverse function is $h^{-1}(n) = n - 1$ so $h$ is bijective.

3. How many functions are there from a set $X$ with 3 elements to a set $Y$ with 4 elements? How many of these functions are injective? How many are surjective?

Solution. To count the number of functions from $X$ to $Y$, just note that any element of $Y$ can be chosen for each $f(x)$. Since $X$ has three elements, and each can be assigned any of the 4 elements of $Y$, there are $4 \times 4 \times 4 = 4^3 = 64$ possible functions from $X$ to $Y$. To produce an injective function, the first element of $X$ can be assigned any of the 4 elements of $Y$, the second element of $X$ can be assigned any element not already used. That is there are 3 choices for the second element, after the first has already been chosen. The final element of $X$ can then be assigned either of the 2 remaining unassigned elements of $Y$. Hence there are $4 \times 3 \times 2 = 24$ injective functions from $X$ to $Y$. Since $|Y| = 4 > 3 = |X|$ there are no surjections from $X$ to $Y$. (The image of $f : X \to Y$ has size $\leq$ the size of $X$.)

4. (a) If $S$ and $T$ are finite sets, write the formula relating $|S \cup T|$, $|S|$, $|T|$, and $|S \cap T|$. It is not necessary to verify the formula, just write it down.

(b) The following is a portion of a report submitted by a marketing analysis employee:

Number of consumers interviewed: 100.
Number of consumers using brand $X$: 78.
Number of consumers using brand $Y$: 71.
Number of consumers using both brands: 48.

Explain why this report cannot be correct. (Hint: Part (a) may be useful.)

Solution. (a) $|S \cup T| = |S| + |T| - |S \cap T|$.

(b) Let

$$S = \{\text{consumers interviewed who use brand } X\} \text{ and } T = \{\text{consumers interviewed who use brand } Y\}.$$ 

Then $S \cup T$ will be the set of consumers interviewed who use at least one of brand $X$ or brand $Y$, while $S \cap T$ denotes the set of consumers interviewed who use both brand $X$ and brand $Y$. From the report, $|S| = 78$ and $|T| = 71$. Moreover, 100 consumers were interviewed so $|S \cup T| \leq 100$ (note that there is not an assumption that every consumer uses one of the two brands). From the formula of Part (a):

$$|S \cap T| = |S| + |T| - |S \cup T| \geq 78 + 71 - 100 \geq 49.$$ 

But the report says $|S \cap T| = 48$, so there must be an error in the report. Note that you do not have enough information to tell precisely where the error is.
5. Let \( A = \{1, 2, 3, 6, 9, 18\} \). (This is the set of all positive divisors of 18.) Define a relation \( R \) on \( A \) by the rule \( aRb \iff a|b \).

(a) Which of the properties: reflexive, symmetric, antisymmetric, transitive, are valid for this relation? (No justification is required for this part.)

(b) Is the relation a partial order? an equivalence relation?

(c) Write the relation matrix \( M_R \) for \( R \).

\[ M_R = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix} \]

6. Let \( A \) be the set of integers defined by

\[ A = \{n \in \mathbb{Z} : -8 \leq n < 10\} . \]

Define an equivalence relation on \( A \) by the rule \( nRm \iff 4|(n - m) \). You do not need to verify that this is an equivalence relation. List all of the equivalence classes for \( R \).

\[ [0]_R = \{-8, -4, 0, 4, 8\} \]
\[ [1]_R = \{-7, -3, 1, 5, 9\} \]
\[ [2]_R = \{-6, -2, 2, 6\} \]
\[ [3]_R = \{-5, -1, 3, 7\} \]

7. Assume that \( \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \) and \( \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \) are permutations in \( S_4 \). Compute each of the following elements of \( S_4 \):

(a) \( \sigma \tau \)  
(b) \( \tau \sigma \)  
(c) \( \sigma^2 \)  
(d) \( \tau^2 \)  
(e) \( \tau^3 \)  
(f) \( \tau^4 \)  
(g) \( \sigma^{-1} \)  
(h) \( \tau^{-1} \)

\[ \sigma \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \quad \tau \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \tau^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \quad \tau^4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \]
8. Write each of the following permutations as a single cycle or a product of disjoint cycles.

(a) \( \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 5 & 3 & 2 \end{pmatrix} \)  
(b) \( (1 \ 4) \ (1 \ 5) \ (1 \ 2) \ (3 \ 5) \)  
(c) \( (1 \ 2 \ 3)^{-1} (2 \ 3) (1 \ 2 \ 3) \)  
(d) \( (2 \ 4 \ 5) (1 \ 3 \ 5 \ 4) (1 \ 2 \ 3) \)

\begin{solution}
(a) \( (2 \ 6) (3 \ 4 \ 5) \)  
(b) \( (1 \ 2 \ 5 \ 3 \ 4) \)  
(c) \( (1 \ 2) \)  
(d) \( (1 \ 4) \)
\end{solution}

9. Let \( \alpha \) be a fixed element of \( S(n) \) and define a function \( \phi_\alpha : S(n) \to S(n) \) by the rule \( \phi_\alpha(\sigma) = \alpha \sigma \alpha^{-1} \) for all \( \sigma \in S(n) \).

(a) Show that \( \phi_\alpha \) is a bijective function.

\begin{solution}
Suppose \( \phi_\alpha(\sigma) = \phi_\alpha(\tau) \). Then \( \alpha \sigma \alpha^{-1} = \alpha \tau \alpha^{-1} \). Multiplying by \( \alpha^{-1} \) on the left and \( \alpha \) on the right gives \( \sigma = \tau \). Hence \( \phi_\alpha \) is injective. To show that \( \phi_\alpha \) is surjective, let \( \sigma \in S(n) \) be arbitrary. Define \( \tau \in S(n) \) by \( \tau = \alpha^{-1} \sigma \alpha \). Then
\[
\phi_\alpha(\tau) = \alpha \tau \alpha^{-1} = \alpha (\alpha^{-1} \sigma \alpha^{-1}) \alpha^{-1} = \sigma.
\]
Thus \( \phi_\alpha \) is surjective, and hence bijective.
\end{solution}

(b) In \( S(3) \), let \( \alpha = (1 \ 2) \) and compute the function \( \phi_\alpha \), that is, find \( \phi_\alpha(\sigma) \) for all \( \sigma \in S(3) \).

\begin{solution}
The function \( \phi_{(1,2)} : S(3) \to S(3) \) is given by the following table:

<table>
<thead>
<tr>
<th>( \sigma )</th>
<th>( (\cdot) )</th>
<th>( (1, \ 2) )</th>
<th>( (1, \ 3) )</th>
<th>( (2, \ 3) )</th>
<th>( (1, \ 2, \ 3) )</th>
<th>( (1, \ 3, \ 2) )</th>
<th>( (1, \ 2, \ 3) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \phi_{(1,2)}(\sigma) )</td>
<td>( (\cdot) )</td>
<td>( (1, \ 2) )</td>
<td>( (2, \ 3) )</td>
<td>( (1, \ 3) )</td>
<td>( (1, \ 3, \ 2) )</td>
<td>( (1, \ 2, \ 3) )</td>
<td>( (1, \ 2, \ 3) )</td>
</tr>
</tbody>
</table>
\end{solution}

10. How many elements of \( S(10) \) are products \((abcd)(efghi)\) of two disjoint cycles, one of length 4 and the other of length 5?

\begin{solution}
\[
\frac{1}{4} \cdot 10 \cdot 9 \cdot 8 \cdot 7 \times \frac{1}{5} \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 181,440
\]
\end{solution}

11. In \( S(10) \), let \( \alpha = (1, \ 3, \ 5, \ 7, \ 9), \ \beta = (1, \ 2, \ 6), \ \gamma = (1, \ 2, \ 5, \ 3) \), and let \( \sigma = \alpha \beta \gamma \). Write \( \sigma \) as a product of disjoint cycles, and use this to find its order and its inverse. Is \( \sigma \) even or odd?

\begin{solution}
\( \sigma = (1, \ 6, \ 3, \ 2, \ 7, \ 9) \). Thus \( \sigma \) is a 6-cycle so the order of \( \sigma \) is 6, \( \sigma \) is odd, and \( \sigma^{-1} = (1, \ 9, \ 7, \ 2, \ 3, \ 6) \).
\end{solution}

12. Show that \( S(10) \) has elements of order 10, 12, and 14, but not 11 or 13.
Solution. If $\alpha = (1, 2)(3, 4, 5, 6, 7), \beta = (1, 2, 3)(4, 5, 6, 7), \gamma = (1, 2)(3, 4, 5, 6, 7, 8, 9), \gamma = (1, 2)(3, 4, 5, 6, 7, 8, 9)$, then the order of $\alpha$ is 10, the order of $\beta$ is 12 and the order of $\gamma$ is 14 (see Theorem 4.2.6). Since 11 is prime, any permutation of order 11 must be an 11-cycle or a product of disjoint 11-cycles. In $S(10)$ there are no cycles of length 11. Hence there can be no elements of $S(10)$ of order 11. The same argument applies to 13 since 13 is also a prime bigger than 10.

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

(a) $(1, 2, 3)(1, 4, 5) \quad (1, 4, 5, 2, 3)$

(b) $(1, 2, 3, 4)(1, 5, 6, 7) \quad (1, 5, 6, 7, 2, 3, 4)$

(c) $(1, 2, 3, 4, 5)(1, 6, 7, 8, 9) \quad (1, 6, 7, 8, 9, 2, 3, 4, 5)$

(d) $(1, 4)(2, 4)(3, 4)(1, 2)(2, 4)(2, 3) \quad (1)(2)(3)(4) = ()$

14. Let $\alpha = (1, 3)(1, 5)(1, 6)(2, 1)(2, 4)(2, 6)$ and $\beta = (1, 2, 5)(3, 2, 6)(1, 4)$. Find the disjoint cycle factorizations of $\alpha$, $\alpha^{-1}$, $\beta$, and $\beta^{99}$ and give the order of each of these four permutations.

Solution. $\alpha = (1, 2, 5, 3)(4, 6), \alpha^{-1} = (1, 3, 5, 2)(4, 6)$, and $\beta = (1, 4, 2, 6, 3, 5)$. Since $\beta$ is a 6-cycle, it has order 6. Since $99 = 6 \cdot 16 + 3$, $\beta^{99} = \beta^3 = (1, 6)(2, 5)(4, 3)$. The order of $\alpha$ and $\alpha^{-1}$ is $\text{lcm}\{4, 2\} = 4$. Since $\beta^{99}$ is a product of disjoint 2-cycles, the order is 2.