The second exam will be on Wednesday, March 24, 2004. The syllabus will be sections 1.6, 2.1, 2.3, 2.4, 4.1, and 4.2, together with the RSA supplement. 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 what it means for an integer \( a \) to have finite multiplicative order modulo \( n \) (Page 51):
  \[ a_k^n \equiv 1 \pmod{n} \]
  for some positive integer \( k \).

- Know the criterion for \( a \) to have finite multiplicative order modulo \( n \) (Theorem 1.6.1):
  \( a \) is relatively prime to \( n \).

- Know the definition of order of \( a \) modulo \( n \) (Page 52):
  \[ \text{ord}_n(a) = k \] if \( k \) is the smallest positive integer such that \( a^k \equiv 1 \pmod{n} \).

- (Theorem 1.6.2) If \( a \) has order \( k \) modulo \( n \) then \( a^r \equiv a^s \pmod{n} \) if and only if \( r \equiv s \pmod{k} \).

- Know Fermat’s theorem: if \( p \) is prime and \( p \) does not divide \( a \) then \( a^{p-1} \equiv 1 \pmod{p} \). (Theorem 1.6.3, Page 54).

- If \( p \) is prime and \( a \) is an integer not divisible by \( p \), then the order of \( a \) mod \( p \) divides \( p - 1 \).

- The Euler phi-function is defined by \( \varphi(n) = |\mathbb{Z}_n^*| \). (Page 56).

- Know how to use Theorems 1.6.5 and 1.6.6 to compute \( \varphi(n) \) from the prime factorization of \( n \): If \( n = p_1^{k_1} \cdots p_r^{k_r} \), then
  \[ \varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_1^{k_r} - p_1^{k_r-1}) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \]

- Know Euler’s Theorem: If \( n \geq 2 \) and \( a \) is relatively prime to \( n \), then
  \[ a^{\varphi(n)} \equiv 1 \pmod{n} \]

- Corollary to Euler’s Theorem: If \( a \) is relatively prime to \( n \), then the order of \( a \) mod \( n \) divides \( \varphi(n) \).

- Know how to use the RSA encryption and decryption algorithm.

- 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 what a relation on a set $X$ is and the various properties of $R$ contained in the definition on Page 94: reflexive, symmetric, weakly antisymmetric, antisymmetric, and transitive.

• Know how to represent relations on finite sets by means of the directed graph of $R$ ($\Gamma(R)$) (Page 95) and the adjacency matrix $M(R)$ (Page 97).

• Know the two special types of relations: partial order (that is, $R$ is reflexive, weakly antisymmetric, and transitive), and equivalence relation (that is, $R$ is reflexive, symmetric, and transitive).

• Know how to represent a partial order on a finite set by means of the Hasse diagram (Page 100).

• Know the fundamental fact about an equivalence relation. Namely, an equivalence relation on set $X$ determines a partition of $X$ into disjoint sets called equivalence classes. (Theorem 2.3.1).

• $S(n)$ 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
\[
(j_1 j_2 \ldots j_r) = (j_1 j_r)(j_1 j_{r-1}) \cdots (j_1 j_2).
\]
• 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. (a) Compute \(5^{97} \mod 127\).
   (b) Compute \(4^{126} \mod 127\).
   (c) Compute \(4^{63} \mod 127\).

2. Compute the Euler phi function \(\varphi(n)\) for each of the following natural numbers \(n\).
   (a) \(n = 221\)
   (b) \(n = 6125\)
   (c) \(n = 341\)
   (d) \(n = 6860\)

3. Let \(p = 29\) and \(q = 31\) so that \(n = pq = 899\), and let \(e = 101\) in the RSA algorithm.
   (a) Compute \(d\) so that \(ed \equiv 1 \mod \varphi(899)\).
   (b) If \(M = 555\), compute \(N = M^e \mod 899\) and compute \(N^d \mod 899\).

4. Using the RSA enciphering key \((e, n) = (11, 2867)\), encrypt the message: SEAFOOD. (Note that 2867 = 47 \times 61.)

5. Let \(R\) be the relation on \(\mathbb{P}\) defined by \(aRb\) if and only if \(a\mid b\). Is \(R\) reflexive?, symmetric?, weakly antisymmetric?, antisymmetric?, transitive? Is \(R\) a partial order? Is \(R\) an equivalence relation?

6. (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.
   (b) Give an example of a function \(g : \mathbb{Z} \to \mathbb{Z}\) such that \(g\) is surjective but not injective.
   (c) Give an example of a bijection \(h : \mathbb{Z}^+ \to Y\) where \(\mathbb{Z}^+ = \{1, 2, 3, \ldots\}\) and \(Y = \{2, 3, 4, \ldots\}\).

7. 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?

8. Let \(R\) be the relation on the integers \(\mathbb{Z}\) defined by \(aRb\) if and only if \(a^2 = b^2\). Verify that \(R\) is an equivalence relation on \(\mathbb{Z}\). If \(a \in \mathbb{Z}\), find the equivalence class \([a]_R\) of \(a\).
9. Let $R$ be the relation on the set $A = \{1, 2, 3, 4, 5, 6\}$ defined by

$$R = \{(1,1), (1,3), (1,5), (2,2), (2,6), (3,1), (3,3), (3,5), (4,4), (5,1), (5,3), (5,5), (6,2), (6,6)\}.$$ 

(a) Write the relation matrix $M(R)$.
(b) Write the relation digraph $\Gamma(R)$.
(c) Assuming that $R$ is an equivalence relation, list all of the equivalence classes of $R$.

10. Let $A = \{1, 2, 3\}$. Give an example of a relation on $A$ for each of the following sets of properties:

(a) Reflexive and symmetric, but not transitive.
(b) Reflexive and transitive, but not symmetric.
(c) Symmetric and transitive, but not reflexive.
(d) Reflexive, but not symmetric or transitive.

11. 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) $\tau^{-1}$

12. 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) $(1 \ 4 \ 5 \ 1 \ 2 \ 3)$
(c) $(1 \ 2 \ 3)^{-1} (2 \ 3 \ 1 \ 2 \ 3)$
(d) $(2 \ 4 \ 5 \ 1 \ 3 \ 5 \ 4 \ 1 \ 2 \ 3)$

13. 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.
(b) In $S_3$, let $\alpha = (1 \ 2)$ and compute the function $\phi_\alpha$, that is, find $\phi_\alpha(\sigma)$ for all $\sigma \in S(3)$.

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

15. 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?

16. Show that $S(10)$ has elements of order 10, 12, and 14, but not 11 or 13.

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

(a) $(1 \ 2 \ 3)(1 \ 4 \ 5)$
(b) $(1 \ 2 \ 3 \ 4)(1 \ 5 \ 6 \ 7)$
(c) $(1 \ 2 \ 3 \ 4 \ 5)(1 \ 6 \ 7 \ 8 \ 9)$
(d) $(1 \ 4)(2 \ 4)(3 \ 4)(1 \ 2)(2 \ 4)(2 \ 3)$

18. 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.