Review Questions for Discrete Mathematics

1. State and prove the binomial theorem. Use the multinomial theorem to compute the coefficent of ab^3c^3 in $(a+2b+c)^7$.

2. Determine the number of integer solutions to $x_1 + x_2 + \cdots x_n = r, x_i \geq 0$.

3. From a bag containing n distinct balls in how many ways can you pick k (a) if you put back a ball in the bag after picking it up? (b) if you remove a ball after picking it up? (We do not care about in which order the balls are picked up.)

4. Let A be a set with m elements and B a set with n elements. How many functions are there from A to B? How many of these functions are one-to-one? How many are onto?

5. Describe the Dirichlet's box principle (the pigeon hole principle) in some non-trivial example.

6. State and prove the principle of inclusion and exclusion.

7. Define the Euler ϕ-function, and derive an expression for this function.

8. Show that the number of derangements of n objects is approximately $e^{-1}n!$ when n is large.

9. Give a (combinatorial) definition of Stirling numbers of the second kind. State a recurrence relations for them.

10. Explain why the coefficient for x^r in the expansion of

$$(1+x^2+x^4+x^6)^2(x^3+x^4+x^5)^3$$

is equal to the number of ways to distribute r indistinguishable objects into five distinguishable containers with 0, 2, 4, or 6 objects in the first two containers and 3, 4 or 5 objects in the other three containers.

11. Define the binomial coefficient $\binom{n}{r}$, where $n \in \mathbb{R}$ and $r \in \mathbb{N}$. Determine $\binom{-n}{r}$, where $n \in \mathbb{Z}^+$.

12. Show that the coefficient for $x^r/r!$ in the expansion of

$$\left(\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}+\cdots\right)\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots\right)^2$$

equals the number of ways to distribute r distinguishable objects into three distinguishable containers with at least two objects in the first container. Show that it also equals the number of words of length r, which can be composed of the letters A, B and C, if the letter A occurs at least twice.

13. Derive a formula for the sum $1^2 + 2^2 + \cdots + n^2$ by means of generating functions.

14. Show that the general solution to the recurrence equation $a_n + ba_{n-1} + ca_{n-2} = 0$ can be written $a_n = Ar_1^n + Br_2^n$ if the roots r_1 and r_2 of the characteristic equation are unequal. Also account for the case where the roots are equal.

15. Explain the difference between an (undirected) graph, a multigraph and a directed graph.

16. Explain the concepts a) simple path, b) the length of a path, c) the degree of a vertex, d) the complement of a graph.

17. Why does the complete graph K_n have exactly $\binom{n}{2}$ edges?

18. What is meant by a) Euler circuit, b) Hamilton cycle?

19. Let $G = (V, E)$ be a connected, undirected graph or a multigraph. Define the degree of a vertex in G. Show that G has an Euler circuit if and only if each vertex has an even degree.

20. State necessary conditions for a graph to have a Hamilton cycle.

21. State sufficient conditions for a graph to have a Hamilton cycle.

22. What is meant by a ring? Give examples of both commutative and non-commutative rings. What is a field?

23. What is a zero divisor? Give examples.

24. Define the ring $\mathbb{Z}_n$. Check that addition and multiplication are well-defined. Show that $\mathbb{Z}_n$ is a field if and only if n is a prime number.

25. Define the notion of isomorphic rings. Give examples.

26. State and prove Fermat's little theorem.

27. Describe the RSA public key cryptography.

28. State and prove the Chinese remainder theorem.

29. Define the Hamming distance in K^n and the separation of a code. Formulate sufficient conditions on a code for detection or correction of up to k errors and motivate your statement.

30. How many words does the sphere $S(x, r) \subseteq K^n$ contain? What is a perfect code?

31. What is a linear $[n, m]$-code? Define the weight of a linear code, and show that the weight is equal to the separation of the code.

32. What is a generator matrix for a linear code? What is the definition of two codes being equivalent? Show that each linear code is equivalent to a code, which has a generator matrix of standard form.

33. What is the dual code to a linear code? What is a control matrix for a linear code? Show how a control matrix can be constructed from a generator matrix in standard form.

34. Let H be a control matrix for a linear code. What is meant by a syndrome of a word? What is a coset leader belonging to a syndrome? Account for decoding by means of syndromes and coset leaders.

35. How can the separation of a linear code be determined by means of a control matrix?

36. What is meant by a linear $[n, m]$ Hamming code over $\mathbb{Z}_2$? What are the possible values of n and m?

37. Construct a binary $[32, 6]$-code with separation 16.