LUND UNIVERSITY

Centre for Mathematical Sciences
Mathematics, Faculty of Science

Review Questions for Discrete Mathematics

1. State and prove the generalisation of the binomial theorem (the so called multinomial theorem).

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

3. 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?

4. Describe Dirichlet's box principle (the pigeonhole principle) in some non-trivial example.

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

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

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

8. 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.

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

10. 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.

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

12. 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.

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

14. What is a zero divisor? Give examples.

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

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

17. State and prove Fermat's little theorem.

18. Describe the RSA public key cryptography.

19. State and prove the Chinese remainder theorem.

20. What is meant by the characteristic of a finite field? Show that the characteristic of a finite field is a prime number. Show that the number of elements in a finite field is p^n, where $n \in \mathbf{Z}$ and p is the characteristic of the field.

21. What is meant by a polynomial ring over a finite field? State the division algorithm and the factor theorem for polynomials over a field. Show that a polynomial of degree n with coefficients in a field has at most n different zeros.

22. What is an irreducible polynomial (prime polynomial) over a field K? Define the ring $K[x]/(s(x))$, where $s(x)$ is a polynomial in $K[x]$. Show that this ring is a field if and only if $s(x)$ is irreducible.

23. Construct a field with 8 elements.

24. What is meant by the order of an element in a finite field? What is a primitive element? Show that a finite field has a primitive element.

25. Define the index (the discrete logarithm) with regard to a primitive element in a finite field. Explain how indices can be used to calculate products and quotients in the field.

26. Give two examples of binary block codes.

27. 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.

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

29. 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.

30. 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.

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

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

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

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

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

36. What is a Vandermonde matrix? Show that such a matrix is invertible.

37. What is a Reed-Solomon code? Give examples.