Practice Final

MAT 312

May 6, 2024

List of topics

1. GCD, LCM, Euclid algorithm. Writing $\gcd(a, b)$ as linear combination of a, b.
2. Mathematical induction
3. Primes, unique factorization. Finding all divisors of a number from its prime factorization.
4. Congruences and congruence classes. $\mathbb{Z}_n$. Solving linear congruences. Finding inverses in modular arithmetic.
5. Chinese remainder theorem. Euler's function.
6. Order of a number mod n. Fermat's little theorem and Euler's theorem.
7. Permutations. Composition of permutations, cycle decomposition. Order of a permutaiton.
8. Sign of a permutation. Even and odd permutations.
9. Groups, subgroups, group isomorphism. Examples of groups, including S_n and the dihedral group (symmetries of an n-gon).
10. Order of an element. Subgroups generated by a single element. Cyclic groups.
11. Cosets. Lagrange Theorem and its corollaries (order of an element divides the order of the group). Using Lagrange theorem to prove Little Fermat's theorem and Euler's theorem.
12. Normal subgroups and quotient groups.
13. Examples of groups of small order. Klein 4-group, cartesian product of groups.
14. Binary codes. Distance between codewords and number of errors the code can detect/correct. Linear codes and generating matrix. Hammings (7,4) code.
15. General definition of commutative ring and field. Ring of polynomials in one variable.
16. Long division of polynomials. Roots of polynomial and factorisation into linear factors.
17. Euclid algorithm for polynomials. GCD of polynomials.
18. Irreducible polynomials, unique factorization of polynomials (without proof).
19. Irreducible polynomials over $\mathbb{R}$ and $\mathbb{C}$. Fundamental theorem of algebra. Irreducible polynomials over $\mathbb{Z}_p$ (examples).
20. Polynomial congruences. Ring $F[x]/f$ of polynomial congruence classes modulo f; when this ring is a field.

Practice problems

Note that the actual exam will be shorter than this collection of problems. Please not that these problems are just a sample of what you coudl see in the exam, not the full list. To be fully prepared for the final, please make sure you know how to solve all homework problems, then go over practice midterms 1 and 2, and only after that, start on htis practice final.

1. Find all pairs of integer numbers (x, y) such that $36x + 47y = 32$.

2. Let $x, y_1, \ldots, y_n$ be integer numbers. Prove that if $\gcd(x, y_i) = 1$ for all i, then $\gcd(x, y_1 y_2 \ldots y_n) = 1$.

You can use any results from the textbook, but please carefully state what exactly you are using.

3. In this problem please find the answer using the method suggested in the problem.

Let $k = 7^{73}$

(a) Use Fermat's little theorem to find $k \mod 11$

(b) Use Fermat's little theorem to find $k \mod 19$

(c) Use Chinese remainder theorem to find $k \mod 209$ (note: $209 = 11 \cdot 19$)

4. Let the permutation $\sigma \in S_8$ be defined by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 6 & 2 & 3 & 5 & 8 & 1 \end{pmatrix}$$

(a) Find the sign of σ

(b) Write σ^{93} as product of non-intersecting cycles

Let G_{40} be the group of invertible congruence classes mod 40 with respect to multiplication.

5. (a) Find the order of element $x = [33]_{40}$ in G.

(b) Let H be the cyclic subgroup generated by x. How many H-cosets are there in G?

6. Let the coding function $f\colon \mathbf{B}^3 \to \mathbf{B}^{18}$ be defined by

$$f(a, b, c) = (a, b, c, c, a, b, b, c, a, a, b, c, c, a, b, b, c, a,)$$

(you might find it convenient to divide it into groups of 3).

How many transmission errors can this code detect? how many can it correct?

7. Let G be a group, and let $g, h \in G$.

(a) Show that the order of ghg^{-1} is equal to order of h

(b) Show that order of gh is equal to order of hg.

8. Compute greatest common divisor of polynomials $f(x) = x^4 + 1$ and $x^2 + 5x + 6$ (in $\mathbb{R}[x]$). Write this greatest common divisor in the form $f(x)u(x) + g(x)v(x)$ for some polynomials $u(x), v(x)$.

9. Let $f(x) = x^2 - 5x + 6$. Show that a polynomial congruence class $[g(x)]_f$ has an inverse modulo f if and only $g(2) \neq 0$, $g(3) \neq 0$.

10. (a) Factor the polynomial $f(x) = x^3 + 2x - 3$ into product of irreducible polynomials in $\mathbb{R}[x]$.

(b) Factor the polynomial $f(x) = x^3 + 2x - 3$ into product of irreducible polynomials in $\mathbb{Z}_5[x]$.