Math 312/ AMS 351 (Fall '17)

Sample Questions for Final

Part A - Midterm 2 (Number Theory) (about 30%). Key concepts: congruence classes, division with remainder, Euclid's Algorithm, gcd as linear combination, Euler/Fermat Theorems, Chinese Remainder Theorem, congruence equations. Practice: Sample Midterm 1, Midterm 1.

1. Solve the system of equations

$$\begin{aligned} 2x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 7 \\ x &\equiv 7 \mod 8 \end{aligned}$$

2. Can we write 12 as a linear combination of 24 and 114. If yes, find a and b such that $12 = 24a + 114b$.

3.
   - Compute $6^{76} \mod 13$
   - Suppose $a \equiv 4 \mod 10$. What are the possible last 2 digits of a^n.

Part B - Midterm 2 (groups, rings, fields) (about 30%). Key concepts: notion of group, examples of groups (permutation, cyclic, dihedral groups), orders, Lagrange's Theorem, isomorphism, groups of small order, other algebraic structures (esp. rings, fields). Practice: Sample Midterm 2, Midterm 2.

4. We define the quaternion group Q to be the group with 8 elements $\{\pm 1, \pm i, \pm j, \pm k\}$ such that $i^2 = j^2 = k^2 = -1$, and $ij = k$, $jk = i$, and $ki = j$. Show that Q is not isomorphic to
   - $\mathbb{Z}_8$
   - $\mathbb{Z}_4 \times \mathbb{Z}_2$
   - Σ_4
   - $D(4)$

5. Give an example of
   - a field with finitely many elements
   - two different examples of integral domains, which are not fields
   - a ring (commutative and with unit) which is not an integral domain
   - a ring which doesn't have a unit
   - a ring which is not commutative

   Part C - Polynomials (about 40%). Key concepts: division with remainder, Euclid's Algorithm, gcd, irreducible polynomials, factorization into irreducible factors, congruence classes modulo polynomials

6. Find the decomposition into irreducible factors for
   i) $x^3 - 3x^2 + 3x - 2$ over $\mathbb{Z}_7$
   ii) $x^4 - x^2 - 6$ over $\mathbb{R}$
   iii) same as (ii), but over $\mathbb{C}$

7. Find the gcd and lcm of the following polynomials x^4+x+1 and x^3+x+1 over $\mathbb{Z}_3$. Use both methods: factorization and Euclid's Algorithm.

8. Find all irreducible cubic polynomials over $\mathbb{Z}_2$.

9. Let $f = x^2 + x + 2$ over $\mathbb{Z}_3$
   i) Show that f is irreducible.
   ii) Write down the 9 representatives for the congruence classes mod f.
   iii) Compute $(x + 1)^3$ mod f.
   iv) Find the inverse of $[x + 1]_f$.

10. Give example of a field with 9 elements.