Math 342, Spring Term 2009
Pre-Midterm Sheet

February 8, 2009

Material

The material for the exam consists of the material covered in the lectures up to and including Friday, Feb 6^{th}, as well as Problem Sets 1 through 5. Here are some headings for the topics we covered:

- Arithmetic in $\mathbb{F}_2$ (the field with two elements); vectors and linear equations over $\mathbb{F}_2$. Application: the one-time pad.
- Proof by induction.
- Foundations of the natural numbers: Peano's axioms; proving the laws of arithmetic, order, and divisibility; well-ordering.
- Foundations of the integers: divisibility and division with remainder, ideals, principal ideals.
- The integers: GCD and LCM, Euclid's Algorithm and Bezout's Theorem, Unique factorization. Application: irrational numbers.
- Congruences and modular arithemtic: definition of congruence and congruence classes; arithmetic modulu m; invertibility and inverses using Euclid's algorithm; solving congruences. Application: tests for divisibility by 3, 9 and 11. Application: Luhn's algorithm.
- $\mathbb{Z}/m\mathbb{Z}$: the set of congruence classes; systems of representatives; the laws of arithmetic in $\mathbb{Z}/m\mathbb{Z}$; invertibility; zero-divisors.

Structure

The exam will consist of several problems. Problems can be calculational (only the steps of the calculation are required), theoretical (prove that something holds) or factual (state a Definition, Theorem, etc). The intention is to check that the basic tools are at your fingertips.

Sample paper

1. (Unique factorization)
   (a) [calculational] Write 148 as a product of prime numbers.
   (b) [factual] State the Theorem on unique factorization of natural numbers.
   (c) [theoretical] Prove that every natural number can be written as a product of irreducibles.

2. Solve the following system of equations in $\mathbb{Z}/5\mathbb{Z}$:

$$\begin{cases} x + y + z & = [4]_5 \\ [2]_5 x + y - z & = [2]_5 \\ [3]_5 x + z & = [1]_5 \end{cases}$$

3. Prove by induction that $a_n = \frac{n(n+1)}{2}$ is an integer for all $n \geq 0$.

4. (modular arithmetic)
   (a) State the definition of a zero-divisor modulu m.
   (b) What are the zero-divisors in $\mathbb{Z}/15\mathbb{Z}$?
   (c) How many non-zero-divisors are there in $\mathbb{Z}/15\mathbb{Z}$?

Solutions

1. (Unique factorization0

   (a) $148 = 2 \cdot 74 = 2 \cdot 2 \cdot 37$.

   (b) "Every natural number $n \geq 1$ can be written as a (possibly empty) product $n = \prod_{i=1}^{d} p_i$ of prime numbers, uniquely up to the order of the factors." or "For every natural number $n \neq 0$ there exist unique natural numbers $\{e_p\}_{p \text{ prime}}$, all but finitely many of which are zero, such that $n = \prod_p p^{e_p}$".

   (c) Let S be the set of natural numbers which are non-zero and which cannot be written as a (possibly empty) product of irrreducible numbers. If S is non-empty then by the well-ordering principle it has a least element $n \in S$. If n were irreducible, it would be equal to a product of irreducibles of length 1 (itself), so n must be reducible, that is of the form $n = ab$ with $1 < a, b < n$. But then $a, b \notin S$ (since n was minimal). It follows that both a and b are products of irreducibles, say $a = \prod_{i=1}^{d} p_i$ and $b = \prod_{j=1}^{e} q_j$. In that case, $n = \prod_{i=1}^{d} p_i \cdot \prod_{j=1}^{e} q_j$ displays n as a product of irreducibles, a contradiction. It follows that S is empty, that is that every non-zero integer is a product of irreducibles.

2. Let (x, y, z) be a solution to the system. Adding the first two equations we see that $[5]_5 x + y = [3]_5$. Since $5 \equiv 0\,(5)$ this reads $y = [3]_5$. Subtracting the first equation from the third gives: $[2]_5 x - y = [-3]_5$, that is $[2]_5 x = y - [3]_5 = [0]_5$. Since 2 is invertible modulu 5, we find $x = [0]_5$. Finally, from the last equation we read $z = [1]_5$. Thus, the only possible solution is $x = [0]_5$, $y = [3]_5$, $z = [1]_5$. We now check that this is, indeed a solution: $0 + 3 + 1 = 4 \equiv 4\,(5)$, $2 \cdot 0 + 3 - 1 = 2 \equiv 2\,(5)$ and $3 \cdot 0 + 1 = 1 \equiv 1\,(5)$ as required.

3. When $n = 0$ we have $a_n = 0$ which is an integer. Continuing by induction, we note that $a_{n+1} - a_n = \frac{(n+1)(n+2)}{2} - \frac{n(n+1)}{2} = \frac{(n+1)}{2} \cdot ((n+2) - n) = \frac{n+1}{2} \cdot 2 = n + 1$. Asusming, by induction, that a_n is an integer then shows that $a_{n+1} = a_n + (n + 1)$ is an integer as well.

4. (zero-divisors)

   (a) "A number a is a *zero-divisor* modulu m if there exists b, $b \not\equiv 0\,(m)$, so that $ab \equiv 0\,(m)$" or "a residue class $x \in \mathbb{Z}/m\mathbb{Z}$ is a *zero-divisor* if there exists $y \in \mathbb{Z}/m\mathbb{Z}$, $y \neq [0]_m$, so that $xy = [0]_m$".

   (b) The zero-divisors are $[0]_{15}, [3]_{15}, [5]_{15}, [6]_{15}, [9]_{15}, [10]_{15}, [12]_{15}$.

   (c) There are 7 zer0-divisors hence $8 = 15 - 7$ non-zero-divisors.