CS21001 Discrete Structures, Autumn 2005

End-semester examination

Total marks: 50 November 21, 2005 **Duration:** 3 hours

Answer any <u>three</u> questions from Part I, any <u>five</u> questions from Part II, and any <u>one</u> question from Part III. Do not use facts not proved in the lectures.

Part I
Answer any <u>three</u> questions

1. Solve the recurrence relation: **(5)**

$$\begin{aligned} T_1 &= 3, \\ T_2 &= 7, \\ T_n &= 2T_{n-1} - T_{n-2} + 2 \quad \text{for } n \geqslant 3. \end{aligned}$$

2. Compute the multiplicative inverse of 17 modulo 71. **(5)**

3. Compute the order of 19 in the multiplicative group $\mathbb{Z}_{32}^*$. **(5)**

4. Compute the <u>monic</u> gcd of the polynomials $x^4 + 3x^3 + 2x^2 + 4x + 1$ and $x^3 + 2x^2 + 5x + 3$ in $\mathbb{Z}_7[x]$. **(5)**

Part II
Answer any <u>five</u> questions

5. Let G be an Abelian group. An element $a \in G$ is called a *torsion element* of G if $\operatorname{ord} a$ is finite. Prove that the set of all torsion elements of G is a subgroup of G. **(5)**

6. Prove that for any integer $n \geqslant 3$ the multiplicative group $\mathbb{Z}_{2^n}^*$ is *not* cyclic. (Hint: You may look at the elements $2^{n-1} \pm 1$.) **(5)**

7. Let R be a ring. Two elements $a, b \in R$ are called *associates*, denoted $a \sim b$, if $a = ub$ for some unit u of R. Prove that $\sim$ is an equivalence relation on R. **(5)**

8. Prove that every finite integral domain is a field. (Hint: For a non-zero element a in a finite integral domain R, look at the function $R \to R$ that maps $r \mapsto ra$.) **(5)**

9. Let $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ be non-zero ideals of $\mathbb{Z}$ satisfying the condition:

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots .$$

Prove that there exists $n \in \mathbb{N}$ such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots$, that is, there cannot exist an infinite strictly increasing chain of ideals of $\mathbb{Z}$. (Hint: $\mathbb{Z}$ is a PID.) **(5)**

10. Let F be a finite field. Prove that there exists a polynomial $f(x) \in F[x]$ having no roots in F. (Do <u>not</u> use the fact that $F[x]$ contains an irreducible polynomial of every degree $n \in \mathbb{N}$.) **(5)**

Part III
Answer any one question

11. **(a)** Let G be a finite Abelian group (with identity e) in which the number of elements x satisfying $x^n = e$ is at most n for every $n \in \mathbb{N}$. Prove that G is cyclic. (Do not use the structure theorem for finite Abelian groups.) **(8)**

(b) Prove that any finite subgroup of the multiplicative group $F^* = F \setminus \{0\}$ of any field F (possibly infinite) is cyclic. (In particular, the multiplicative group of any finite field is cyclic.) **(2)**

12. Let R be a commutative ring and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$. Prove that $f(x)$ is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent elements of R. (Recall that an element a in a ring A is called nilpotent if $a^k = 0$ for some positive integer k.) **(10)**