CS21001 Discrete Structures, Autumn 2007

End-semester examination

Total marks: 100   November 2007   **Duration:** 3 hours

[*Answer all questions. Be brief and precise. Show all important steps.*]

1 Let $m \in \mathbb{N}$, $m \geqslant 2$, be a fixed modulus. Choose an arbitrary element $a_0 \in \mathbb{Z}_m$. For $n \geqslant 1$, define $a_n = a_{n-1}^2 + 1 \pmod m$. Prove that the sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$ must be eventually periodic. **(10)**

(**Remark:** This sequence $a_0, a_1, a_2, \ldots$ is used in Pollard's rho algorithm for factoring integers.)

2 Recall that a *derangement* of $1, 2, 3, \ldots, n$ is a permutation $\pi_1, \pi_2, \pi_3, \ldots, \pi_n$ of $1, 2, 3, \ldots, n$ with $\pi_i \neq i$ for all $i = 1, 2, 3, \ldots, n$. Let D_n denote the number of derangements of $1, 2, 3, \ldots, n$. Provide a combinatorial argument to establish that $D_{n+1} = n(D_n + D_{n-1})$ for all $n \geqslant 2$. **(10)**

(**Hint:** You may proceed as follows. Let $\pi_1, \pi_2, \ldots, \pi_{n+1}$ be a derangement of $1, 2, \ldots, n+1$. Look at i with $\pi_i = n+1$. Separately consider the two cases $\pi_{n+1} = i$ and $\pi_{n+1} \neq i$.)

3 Solve the following recurrence relation: **(10)**

$$\begin{aligned} a_0 &= 1, \\ a_1 &= 3, \\ 2a_n &= 3a_{n-1} - a_{n-2} + 1 \quad \text{for } n \geqslant 2. \end{aligned}$$

4 Let S be a set, and let $\mathcal{P}(S)$ denote the power set of S (i.e., the set of all subsets of S). Define an operation Δ on $\mathcal{P}(S)$ as $A \,\Delta\, B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$ (the symmetric difference of $A, B \in \mathcal{P}(S)$).

(a) Prove that $\mathcal{P}(S)$ is an Abelian (i.e., commutative) group under the operation Δ. **(10)**

(b) In this part only, suppose that S is a finite set of size $n = |S|$. Prove that $(\mathcal{P}(S), \Delta)$ is isomorphic to the additive group $\mathbb{Z}_2^n$ (the n-fold Cartesian product of $\mathbb{Z}_2$). **(10)**

5 Let $(G, *)$ be a group. For subsets A, B of G, define $A * B = \{a * b \mid a \in A, b \in B\}$. Let H be a non-empty subset of G. Prove the following assertions.

(a) If H is a subgroup of G, then $H * H = H$. **(5)**

(b) If $H * H = H$, then H need not be a subgroup of G. **(5)**

(c) If H is finite and $H * H = H$, then H is a subgroup of G. **(5)**

6 Prove that every subgroup of $(\mathbb{Z}, +)$ is cyclic. **(10)**

7 Let A denote the set of all functions $\mathbb{Z} \to \mathbb{Z}$. Define addition and multiplication of $f, g \in A$ as $(f+g)(n) = f(n) + g(n)$ and $(fg)(n) = f(n)g(n)$ for all $n \in \mathbb{Z}$. Prove that under these operations A is a commutative ring with identity. What are the units in A? **(10)**

8 Let R be an integral domain and $A = R \times (R \setminus \{0\})$. Define a relation $\sim$ on A as $(a, b) \sim (c, d)$ if and only if $ad = bc$.

(a) Prove that $\sim$ is an equivalence relation on A. **(5)**

Denote the equivalence class of $(a, b) \in A$ as a/b. Also let K denote the set of all equivalence classes of $\sim$. Define addition and multiplication in K as $(a/b) + (c/d) = (ad + bc)/(bd)$ and $(a/b)(c/d) = (ac)/(bd)$.

(b) Prove that these operations are well-defined. **(5)**

(c) Prove that K is a field under these operations. **(5)**

Dr. Abhijit Das, Dept. of Computer Science & Engineering, IIT Kharagpur, India