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.)

> *Solution* Consider the first $m+1$ terms $a_0, a_1, \ldots, a_m$ in the sequence. Since all these terms are elements of $\mathbb{Z}_m$ (which has size m), by the pigeon-hole principle, there exists a repetition among these values, i.e., $a_i = a_j$ for some i, j with $0 \leqslant i < j \leqslant m$. But then $a_{i+1} = (a_i^2+1) = (a_j^2+1) = a_{j+1} \pmod{m}$, and so $a_{i+2} = (a_{i+1}^2+1) = (a_{j+1}^2+1) = a_{j+2} \pmod{m}$, and so on. Call $t = j - i$. We then have $a_k = a_{t+k}$ for all $k \geqslant i$, i.e., the sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$ is eventually periodic.

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 $\pi_{n+1} \neq i$.)

> *Solution* First note that there are n possible values of i with $\pi_i = n+1$. Let $\pi_{n+1} = j$. If $j = i$, then $i, n+1$ form a cycle (a transposition) and π (*without* this transposition) produces a derangement of the remaining $n-1$ elements $1, 2, \ldots, i-1, i+1, \ldots, n$. On the other hand, if $j \neq i$, then $n+1$ belongs to a bigger cycle $(i, n+1, j, \ldots)$. Removing $n+1$ from this cycle produces a derangement of $1, 2, \ldots, n$.

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

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

> *Solution* The characteristic equation for this recurrence is $x^2 = \frac{1}{2}(3x-1)$, i.e., $x^2 - \frac{3}{2}x + \frac{1}{2} = 0$, i.e., $(x-1)(x-\frac{1}{2}) = 0$. This has two simple roots $x = 1, \frac{1}{2}$. Thus, $a_n = b_n + c_n$, where the homogeneous solution b_n is of the form $b_n = u + v\left(\frac{1}{2}\right)^n$ and the particular solution c_n is of the form $c_n = wn$. We first determine w from $2c_n = 3c_{n-1} - c_{n-2} + 1$, i.e., $2wn = 3w(n-1) - w(n-2) + 1$, i.e., $w = 1$, i.e., $c_n = n$. Thus, $a_n = u + v\left(\frac{1}{2}\right)^n + n$. Now, $a_0 = 1 = u + v$ and $a_1 = 3 = u + (v/2) + 1$. Solving this system yields $u = 3$, $v = -2$. Therefore, $a_n = n + 3 - \frac{1}{2^{n-1}}$ for all $n \in \mathbb{N}$.

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)**

Solution [Closure] For any $A, B \subseteq S$, we clearly have $A \,\Delta\, B \subseteq S$.

[Associative] Let $A, B, C \subseteq S$. Then, using Venn diagrams or manipulation of set identities, one can show that both $(A \,\Delta\, B) \,\Delta\, C$ and $A \,\Delta\, (B \,\Delta\, C)$ comprise only those elements of $A \cup B \cup C$, that belong to exactly one or all of the sets A, B, C.

[Identity] The null set $\emptyset$ is the identity of $\mathcal{P}(S)$.

[Inverse] For every $A \subseteq S$, we have $A \,\Delta\, A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset$, i.e., A itself is the inverse of A.

[Commutative] Evident.

(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)**

Solution Let $S = \{a_1, a_2, \ldots, a_n\}$. For a subset $A \subseteq S$ and for $a \in S$, define $\chi_a(A) = \begin{cases} 0 & \text{if } a \notin A, \\ 1 & \text{if } a \in A. \end{cases}$ Define a function $f : \mathcal{P}(S) \to \mathbb{Z}_2^n$ as $f(A) = (\chi_{a_1}(A), \chi_{a_2}(A), \ldots, \chi_{a_n}(A))$. Let $A, B \subseteq S$. Then $A \,\Delta\, B$ consists precisely of those elements that are in exactly one of the sets A, B, i.e., those elements a for which ($\chi_a(A) = 1$ and $\chi_a(B) = 0$) or ($\chi_a(A) = 0$ and $\chi_a(B) = 1$). Now, let $r, s \in \mathbb{Z}_2$. If ($r = 1, s = 0$) or ($r = 0, s = 1$), then $r + s = 1$ in $\mathbb{Z}_2$. On the other hand, if ($r = s = 0$) or ($r = s = 1$), then $r + s = 0$ in $\mathbb{Z}_2$. It, therefore, follows that $f(A \,\Delta\, B) = f(A) + f(B)$, i.e., f is indeed a homomorphism of groups. It remains to establish that f is bijective. Since two different subsets A, B of S differ with respect to the inclusion of at least one element, $f(A) \neq f(B)$, i.e., f is injective. Furthermore, given an n-tuple $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, we construct the subset A of S as $a_i \in A$ if and only if $x_i = 1$. We clearly have $f(A) = (x_1, x_2, \ldots, x_n)$, i.e., f is surjective too.

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)**

Solution Let e denote the identity element of G. Since H is closed under $*$, we have $H * H \subseteq H$. On the other hand, $e \in H$, and so $H = \{e\} * H \subseteq H * H$.

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

Solution Let $G = \mathbb{Z}$ and $*$ be integer addition. Take $H = \mathbb{N}$. Although $\mathbb{N} + \mathbb{N} = \mathbb{N}$, $\mathbb{N}$ is not a subgroup of $\mathbb{Z}$, since inverses of elements (other than 0) do not reside in $\mathbb{N}$.

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

Solution Take any $h \in H$. Since $H * H = H$, the elements $h, h * h, h * h * h, \ldots$ all belong to H. H being finite, these elements cannot be all distinct, i.e., $h * h * \cdots * h$ (i times) $=$ $h * h * \cdots * h$ (j times) for some i, j with $0 \leqslant i < j$. Call $t = j - i$. By cancellation (in G), $h * h * \cdots * h$ (t times) $= e$, i.e., $e \in H$. Let $h' = h * h * \cdots * h$ ($t - 1$ times). Then $h' * h = h * h' = e$, i.e., $h' = h^{-1} \in H$. Finally, $H * H = H$ implies closure of H under $*$.

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

Solution Let H be a subgroup of $\mathbb{Z}$. If $H = \{0\}$, then H is generated by 0. So assume that H contains a non-zero integer a. Since H is closed under taking inverses, $-a \in H$, i.e., without loss of generality we may assume that H contains a positive integer. Let h be the smallest positive integer in H. For any integer $a \in H$, we write $a = qh + r$, where q and r are the quotient and the remainder of Euclidean division of a by h with $0 \leqslant r < h$. Also $r = a - qh \in H$, since $a, h \in H$ and H is a subgroup of $\mathbb{Z}$. The construction of h (its minimality) then implies that $r = 0$, i.e., $a = qh$. Therefore, $H \subseteq \langle h \rangle$. On the other hand, since $h \in H$ and H is a subgroup, $\langle h \rangle \subseteq H$.

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)**

Solution Let $f, g, h \in A$.

[Closure of $+$] Evident.

[Associativity of $+$] $((f+g)+h)(n) = (f+g)(n) + h(n) = (f(n)+g(n)) + h(n) = f(n) + (g(n)+h(n)) = f(n) + (g+h)(n) = (f+(g+h))(n)$ for all $n \in \mathbb{Z}$, so $(f+g)+h = f+(g+h)$.

[Identity of $+$] The zero function 0 that takes every $n \in \mathbb{Z}$ to 0.

[Inverse of $+$] $(-f)(n) = -f(n)$ for all $n \in \mathbb{Z}$.

[Commutativity of $+$] $(f+g)(n) = f(n)+g(n) = g(n)+f(n) = (g+f)(n)$ for all $n \in \mathbb{Z}$, so $f+g = g+f$.

[Closure of $\cdot$] Evident.

[Associativity of $\cdot$] $((fg)h)(n) = (fg)(n)h(n) = (f(n)g(n))h(n) = f(n)(g(n)h(n)) = f(n)(gh)(n) = (f(gh))(n)$ for all $n \in \mathbb{Z}$, so $(fg)h = f(gh)$.

[Identity of $\cdot$] The constant function 1 that maps every $n \in \mathbb{Z}$ to 1.

[Commutativity of $\cdot$] $(fg)(n) = f(n)g(n) = g(n)f(n) = (gf)(n)$ for all $n \in \mathbb{Z}$, so $fg = gf$.

[Distributivity of $\cdot$ over $+$] For every $n \in \mathbb{Z}$, we have $(f(g+h))(n) = f(n)(g+h)(n) = f(n)(g(n)+h(n)) = f(n)g(n) + f(n)h(n) = (fg)(n) + (fh)(n) = (fg+fh)(n)$, i.e., $f(g+h) = fg+fh$. Similarly, $(f+g)h = fh+gh$.

Units of A: Let $f \in A$ be (multiplicatively) invertible, i.e., there exists $g \in A$ such that $fg = gf = 1$, i.e., $f(n)g(n) = g(n)f(n) = 1$ for all $n \in \mathbb{Z}$. This means that each $f(n) \in \{1, -1\}$. Conversely, given $f \in A$ with the property that $\operatorname{Im} f \subseteq \{1, -1\}$, we have $f(n)f(n) = 1$ for all $n \in \mathbb{Z}$, i.e., f is invertible.

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)**

Solution Let $a, c, e \in R$ and $b, d, f \in R \setminus \{0\}$. Since $ab = ba$, we have $(a,b) \sim (a,b)$, i.e., $\sim$ is reflexive. If $(a,b) \sim (c,d)$, then $ad = bc$, i.e., $bc = ad$, i.e., $cb = da$, i.e., $(c,d) \sim (a,b)$, i.e., $\sim$ is symmetric. Finally, let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$, i.e., $ad = bc$ and $cf = de$, i.e., $adf = bcf = bde$, i.e., $adf = bde$, i.e., $af = be$ (since $d \neq 0$), i.e., $(a,b) \sim (e,f)$, i.e., $\sim$ is transitive.

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)**

Solution Let $a/b = a'/b'$ and $c/d = c'/d'$, i.e., $ab' = a'b$ and $cd' = c'd$. But then $(ad+bc)(b'd') = ab'dd' + bb'cd' = a'bdd' + bb'c'd = bd(a'd'+b'c')$, i.e., $(ad+bc)/(bd) = (a'd'+b'c')/(b'd')$. Similarly, $(ac)(b'd') = (ad')(b'c) = (a'd)(bc') = (bd)(a'c')$, i.e., $(ac)/(bd) = (a'c')/(b'd')$.

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

Solution One can check (do it!) that K is a commutative ring. The additive identity is $0/1$ and the multiplicative identity is $1/1$. Moreover, every non-zero a/b (with both $a, b \in \mathbb{Z} \setminus \{0\}$) has the inverse b/a. Thus K is a field.