CS21001 Discrete Structures, Autumn 2005

End-semester examination : Solutions

---

1. Solve the recurrence relation:

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

Solution The characteristic equation $\chi(x) = x^2 - 2x + 1 = (x-1)^2 = 0$ has a single root 1 of multiplicity 2. So the particular solution is of the form $T_n = an^2$ for some constant a. Plugging in this solution in the recurrence gives

$$an^2 = 2a(n-1)^2 - a(n-2)^2 + 2, \text{ i.e., } 0 = -2a + 2, \text{ i.e., } a = 1.$$

Thus a general solution for the given recurrence is of the form $T_n = 1^n(bn + c) + n^2 = n^2 + bn + c$ for some constants b, c. The initial conditions give:

$$\begin{aligned} b + c &= 2, \\ 2b + c &= 3. \end{aligned}$$

The solution of this system is $b = c = 1$. To sum up, the given recurrence has the solution

$$T_n = n^2 + n + 1 \text{ for all } n \in \mathbb{N}.$$

2. Compute the multiplicative inverse of 17 modulo 71.

Solution Let us compute the extended gcd of 17 and 71:

$$\begin{aligned} 71 &= 4 \times 17 + 3, \\ 17 &= 5 \times 3 + 2, \\ 3 &= 1 \times 2 + 1, \\ 2 &= 2 \times 1. \end{aligned}$$

It follows that $1 = 3 - 1 \times 2 = 3 - (17 - 5 \times 3) = 6 \times 3 - 17 = 6 \times (71 - 4 \times 17) - 17 = -25 \times 17 + 6 \times 71$. Therefore, $17^{-1} = -25 = 71 - 25 = 46$ modulo 71.

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

Solution $\phi(32) = \phi(2^5) = 2^4(2-1) = 2^4$, i.e., ord 19 is of the form 2^i for some $i \in \{0, 1, 2, 3, 4\}$. Now $19^1 = 19$, $19^2 = 361 = 9$, $19^4 = 81 = 17$, $19^8 = 289 = 1$ modulo 32. Thus the order of 19 in $\mathbb{Z}_{32}^*$ is 8.

4. Compute the monic gcd of the polynomials $x^4 + 3x^3 + 2x^2 + 4x + 1$ and $x^3 + 2x^2 + 5x + 3$ in $\mathbb{Z}_7[x]$.

Solution Polynomial division yields:

$$\begin{aligned} x^4 + 3x^3 + 2x^2 + 4x + 1 &= (x+1)(x^3 + 2x^2 + 5x + 3) + 2x^2 + 3x + 5, \\ x^3 + 2x^2 + 5x + 3 &= (4x + 2)(2x^2 + 3x + 5). \end{aligned}$$

The last non-zero remainder is $2x^2 + 3x + 5 = 2(x^2 + 5x + 6)$. Thus the monic gcd of the given two polynomials is $x^2 + 5x + 6$.

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.

Solution Denote by H the set of all elements of G of finite orders.

[Closure] Let $a, b \in H$, $\operatorname{ord} a = m$ and $\operatorname{ord} b = n$. But then $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e$, i.e., $\operatorname{ord}(ab) \mid mn$. In particular, $\operatorname{ord}(ab)$ is finite, i.e., $ab \in H$.

[Inverse] Let $a \in H$. Since $a^k = e$ if and only if $(a^k)^{-1} = (a^{-1})^k = e$, we have $\operatorname{ord}(a^{-1}) = \operatorname{ord} a$.

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 $2^{n-1} \pm 1$.)

Solution For $n \geqslant 3$ the elements $2^{n-1} \pm 1$ are distinct modulo 2^n and neither of them is the identity element. Also $(2^{n-1} \pm 1)^2 = 2^{2n-2} \pm 2^n + 1 = 1$ modulo 2^n, since $2n - 2 \geqslant n$ for $n \geqslant 3$. Thus $2^{n-1} - 1$ and $2^{n-1} + 1$ are distinct elements of $\mathbb{Z}_{2^n}^*$ of order 2, i.e., G has two distinct subgroups $\{1, 2^{n-1} - 1\}$ and $\{1, 2^{n-1} + 1\}$ of the same size 2. We know that a finite cyclic group of order r has a unique subgroup of order s for every divisor s of r. Therefore, $\mathbb{Z}_{2^n}^*$ cannot be cyclic.

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.

Solution [Reflexive] $a = 1 \times a$ for all $a \in R$.

[Symmetric] Let $a = ub$ for some unit u. Let $v \in R$ be the element with $uv = vu = 1$ in R. Then v is also a unit of R, and $b = va$.

[Transitive] Let $a = ub$ and $b = vc$ for some units u, v (i.e., $u^{-1}, v^{-1} \in R$). Then $a = (uv)c$. Moreover, $(v^{-1}u^{-1})(uv) = v^{-1}(u^{-1}u)v = v^{-1}v = e$, i.e., uv is also a unit in R.

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 $r \mapsto ra$.)

Solution Let R be a finite integral domain. Take any non-zero $a \in R$. I have to show that a has an inverse in R. Consider the function $\varphi : R \to R$ that maps $r \mapsto ra$. Since R is an integral domain and $a \neq 0$, $ra = sa$ implies $r = s$, i.e., φ is injective. Moreover, R is a finite set. So φ is indeed a bijection. Thus there exists an element $r \in R$ such that $\varphi(r) = ra = 1$.

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.)

Solution $\mathbb{Z}$ is a PID. Let $\mathfrak{a}_n = \langle a_n \rangle$ with $a_n > 0$ for all $n \in \mathbb{N}$. Since $a_n \in \langle a_n \rangle \subseteq \langle a_{n+1} \rangle$, it follows that a_n is an integral multiple of a_{n+1}. In particular, $a_1 \geqslant a_2 \geqslant a_3 \geqslant \cdots \geqslant a_n \cdots$. But we cannot have a strictly decreasing infinite sequence of positive integers. So there exists $n \in \mathbb{N}$ such that $a_n = a_{n+1} = a_{n+2} = \cdots$, which in turn implies that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots$.

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

Solution Let $F = \{a_1, a_2, \ldots, a_n\}$, where n is the size of F. The polynomial

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) + 1$$

evaluates to 1 when x is substituted by any element of F, i.e., $f(x)$ has no root in F.

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.)

Solution I will prove the contrapositive of the given statement, i.e., I will assume that G is not cyclic and determine an $n \in \mathbb{N}$ for which $x^n = e$ has more than n solutions in G.

Let $m = |G| = p_1^{e_1} \cdots p_r^{e_r}$ with pairwise distinct primes $p_1, \ldots, p_r$, and with $r, e_i \in \mathbb{N}$. Suppose that for each $i \in \{1, \ldots, r\}$ there exists an element $a_i \in G$ with the property that $p_i^{e_i} \mid \operatorname{ord} a_i$. Call $m_i = \operatorname{ord} a_i$. Define the element $b_i = a_i^{m_i/p_i^{e_i}}$. Then $\operatorname{ord} b_i = p_i^{e_i}$. Since G is Abelian, the element $b_1 \cdots b_r$ has order $p_1^{e_1} \cdots p_r^{e_r} = m$, i.e., G is cyclic, a contradiction. Thus there exists at least one i for which $p_i^{e_i}$ does not divide $\operatorname{ord} a$ for all $a \in G$. Then $n = \operatorname{lcm}(\operatorname{ord} a \mid a \in G)$ is also not divisible by $p_i^{e_i}$ for this particular i. Moreover, $\operatorname{ord} a \mid m$ for all $a \in G$, i.e., n is a *proper* divisor of m. In particular, $m > n$. Finally note that $x^n = e$ is satisfied by all of the m elements of G.

(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.)

Solution Since F is a field, the polynomial $x^n - 1$ can have at most n roots in F and hence in any subset of F. The result then follows immediately from Part (a).

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.)

Solution [if] Let $a_1^{k_1} = a_2^{k_2} = \cdots = a_n^{k_n} = 0$ for some positive integers $k_1, k_2, \ldots, k_n$. Also let $a_0 b_0 = 1$. Take $k = n \times \max(k_1, k_2, \ldots, k_n)$. Let $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x$, i.e., $f(x) = a_0 + g(x)$. We have $g(x)^k = 0$, since every term in the expansion of $g(x)^k$ has a coefficient involving $a_i^{l_i}$ with $l_i \geqslant k_i$ for at least one $i \in \{1, 2, \ldots, n\}$. But then

$$f(x) b_0^k \left[a_0^{k-1} - a_0^{k-2} g(x) + a_0^{k-2} g(x)^2 - \cdots + (-1)^{k-1} g(x)^{k-1} \right] = (a_0 b_0)^k + b_0^k (-1)^{k-1} g(x)^k = 1 \,,$$

i.e., $f(x)$ has an inverse in $R[x]$.

[only if] Let $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in R[x]$ be the inverse of $f(x)$ in $R[x]$. Since $f(x)g(x) = 1$, equating coefficients of $x^0, x^1, \ldots, x^{m+n-1}, x^{m+n}$ from the two sides yields:

$$\begin{aligned}
a_0 b_0 &= 1, \\
a_0 b_1 + a_1 b_0 &= 0, \\
a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0, \\
&\cdots \\
a_{n-1} b_m + a_n b_{m-1} &= 0, \\
a_n b_m &= 0.
\end{aligned}$$

The first equation shows that a_0 and b_0 are units. Multiplying the second last equation by a_n yields $a_n^2 b_{m-1} = 0$, the third last equation by a_n^2 yields $a_n^3 b_{m-2} = 0$, and so on. Finally, we get $a_n^{m+1} b_0 = 0$. Since b_0 is a unit, it follows that $a_n^{m+1} = 0$, i.e., a_n is nilpotent.

It is easy to check that the sum of a nilpotent element and a unit is again a unit. (For example, look at the proof of the [if] part.) In particular, $f(x) + (-a_n x^n)$ is a unit. But then using the above argument we can conclude that a_{n-1} is nilpotent.

Proceeding in this fashion proves that $a_{n-2}, a_{n-3}, \ldots, a_1$ are all nilpotent.