CSL105: Discrete Mathematical Structures

I semester 2008-09
Major Wed 27 Nov 2008 VI 301(G123) VI401(G4) 10:30-12:30 Max Marks 60

1. Open notes exam. No borrowing of notes etc. and no text books allowed.
2. Answer in the space provided on the question paper in **ink** *(no pencils or other easily eraseable writing instruments allowed).*
3. The answer booklet you have been given is for **rough work only** and will not be collected.

Q1	Q2	Q3	Q4	Q5	Q6	TOTAL

1. **[5+5=10 marks]**

   (a) Prove that in a *directed complete* graph $G = \langle V, E\rangle$, with $|V| = n > 0$,

   $$\boxed{\sum_{v\in V} \delta^+(v)^2 = \sum_{v\in V} \delta^-(v)^2}.$$

   Solution

   In any directed graph complete graph $G = \langle V, E\rangle$ we have

   $$\sum_{v\in V} \delta^+(v) = \sum_{v\in V} \delta^-(v) \tag{1}$$

   and for every $v \in V$,

   $$\delta^+(v) + \delta^-(v) = n - 1 \tag{2}$$

   From (1) and (2) we get

   $$\sum_{v\in V} (\delta^+(v) + \delta^-(v)) = n(n-1) \tag{3}$$

   which yields

   $$\sum_{v\in V} \delta^+(v) = \frac{n(n-1)}{2} = \sum_{v\in V} \delta^-(v) \tag{4}$$

   Again from (2) we get

   $$\begin{aligned}
   & \delta^+(v) && = && (n-1) - \delta^-(v) \\
   \Rightarrow\ & \delta^+(v)^2 && = && (n-1)^2 - 2(n-1)\delta^-(v) + \delta^-(v)^2 \\
   \Rightarrow\ & \sum_{v\in V} \delta^+(v)^2 && = && \sum_{v\in V} (n-1)^2 - 2(n-1)\sum_{v\in V} \delta^-(v) + \sum_{v\in V} \delta^-(v)^2 \\
   & && = && n(n-1)^2 - 2(n-1)\frac{n(n-1)}{2} + \sum_{v\in V} \delta^-(v)^2 \\
   & && = && \sum_{v\in V} \delta^-(v)^2
   \end{aligned}$$

(b) Prove that any connected undirected graph with $2k$ vertices of odd degree may be decomposed into k *edge-disjoint* subgraphs such that each subgraph has an Euler path.

Solution

Assume G is a connected undirected (multi-)graph of n vertices and $u_1, \ldots, u_k$ and $v_1, \ldots, v_k$ are the $2k < n$ distinct vertices of odd degree in the (multi-)graph G. Let G be the subsgraph of G^* which has all the vertices and edges of G and in addition has k new edges u_i—v_i, $1 \leq i \leq k$. Clearly G^* is an Euler (multi-)graph since it is connected and every vertex is of even degree. Hence by Euler's theorem for Euler graphs, G^* has an Eulerian circuit, say

$$\epsilon = w_0\text{—}w_1\text{—}\cdots\text{—}w_{n-1}\text{—}w_0$$

in which each of the new edges u_i—v_i is also present (in addition to all the edges of G and every edge occurs exactly once in ϵ). Deleting the k new edges from ϵ yields exactly k edge-disjoint paths $\epsilon_0, \ldots, \epsilon_{k-1}$ containing only and all the edges of the original (multi-)graph G. Each of these k paths defines a subgraph of G which has an Euler path. Further all the subgraphs so defined are edge-disjoint (though they may not be vertex-disjoint).

2. **[5+5=10 marks]** Define $S(m) = \{a \mid \phi(a) = m, a > 0\}$, where $\phi(a)$ is the Euler function on positive integers. Prove that

   (a) $S(m)$ is finite.

   (b) $S(m) = \emptyset$ whenever $m > 1$ is an odd integer.

Solution

Let the unique prime factorization of any integer a be given by:

$$a = {p_1}^{k_1} {p_2}^{k_2} \dots {p_r}^{k_r} \tag{5}$$

Therefore,

$$\phi(a) = \prod_{i=1}^{i=r} (p_i^{k_i} - p_i^{k_i - 1}) \tag{6}$$

$$= \prod_{i=1}^{i=r} p_i^{k_i - 1}(p_i - 1) \tag{7}$$

(a) If $\phi(a) = m$, then surely $(p_i - 1)|m$ for all $1 \le i \le r$. Since there are only finite number of divisors of m, then our possible choices for p_i are restricted. If m has d_m different divisors, then we can choose a maximum of d_m different primes. Further, since $(p_i - 1)|m$, we have

$$p_i^{k_i - 1} \le m, \ 1 \le i \le r. \tag{8}$$

$$\text{or } k_i \le 1 + \frac{\log m}{\log p_i} \tag{9}$$

$$\le 1 + \frac{\log m}{\log 2} \tag{10}$$

Hence, we have a finite upper bound on the possible prime factors and also their exponents. Therefore, the number of a's such that $\phi(a) = m$, is finite. In fact,

$$|S(m)| \le d_m \left(1 + \frac{\log m}{\log 2}\right) \tag{11}$$

(b) We know $\phi(2) = 1$. For any $a = 2^n$, $n > 1$, we have $\phi(a) = 2^{n-1}$ which is always even. If a is not a power of 2, then it must be of the form $a = p^k.q$ where p is an odd prime and p is not a divisor of q. By the multiplicative nature of ϕ, we get $\phi(a) = (p-1)p^{k-1}.\phi(q)$. But since $p - 1$ is even , $\phi(a)$ is also even. Hence for all odd $m > 1$, $S(m) = \emptyset$.

3. **[10 marks]** Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function expressed only using the operations of addition, subtraction and multiplication on integers. Let $n = \prod_{i=1}^{k} n_i$, where $gcd(n_i, n_j) = 1$ for all $1 \leq i < j \leq k$. Prove that the number of roots of the equation $f(x) =_n 0$ equals the product of the number of roots of each of the equations $f(x) =_{n_i} 0$, $1 \leq i \leq k$.

Solution

Let $f(x) =_{n_i} 0$ have r_i roots. Let α_i, $1 \leq i \leq k$ be some arbitrarily chosen roots of the equations $f(x) =_{n_i} 0$, $1 \leq i \leq k$ respectively. Then the system of equations

$$y =_{n_1} \alpha_1, \qquad \cdots, y =_{n_k} \alpha_k$$

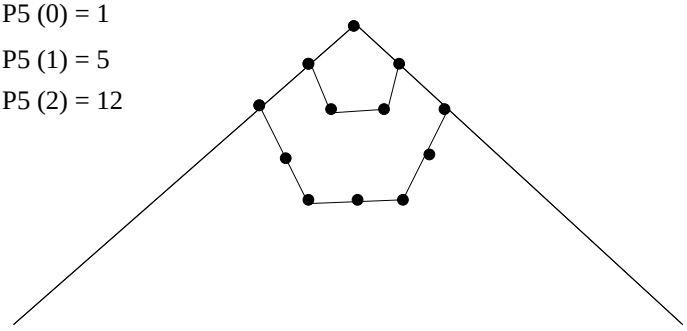
has a unique solution α modulo $n = \prod_{i=1}^{k} n_i$. Since f is made up of only the operations of addition, subtraction and multiplication on integers, it follows that $f(\alpha) =_{n_i} 0$, for each i, $1 \leq i \leq k$, which implies that α is a solution of the equation $f(x) =_n 0$. Since each α_i can be picked in r_i ways, the number of different tuples of solutions $(\alpha_1, \ldots, \alpha_k)$ (which yield a solution to $f(x) =_n 0$ that is unique modulo n) is $\prod_{i=1}^{k} r_i$.

4. **[1+3+7=10]**

P5 (0) = 1

P5 (1) = 5

P5 (2) = 12



The concept of triangular numbers ($P_3(k) = (k+1)(k+2)/2$) may be generalized to "polygonal" numbers, $P_n(k)$ where n is the number of sides of a regular polygon and k is its position in the sequence. Assume for all $n \geq 3$, $P_n(0) = 1$ and $P_n(1) = n$. The figure above shows an example of how the sequence of "pentagonal" numbers $P_5(0), P_5(1), P_5(2)$ may be constructed. By this construction, $P_n(k)$ is the number of dots inside and on a n-sided polygon with sides of length k. Notice also that the sequence P_4 by a similar construction is simply the sequence of perfect squares where $P_4(k) = (k+1)^2$.

(a) Just to make sure you understand the construction, give the values of $P_5(4)$ and $P_6(3)$.

(b) Write a recurrence relation for $P_n(k)$ for $k > 1$, where n is fixed.

(c) Assuming n is a constant of the equation, solve the recurrence equation by any method (an inductive "guess" would have to be justified by an inductive proof that your guess is indeed the correct solution of the equation).

Solution

(a) $P_5(4) = 35$ and $P_6(3) = 28$.

(b) Let us consider the construction in the figure for the general case of constructing $P_n(k)$ from $P_n(k-1)$. Note that each edge of length k units has $k+1$ dots on it. Given that $P_n(k-1)$ already exists, the construction of $P_n(k)$ in a counter-clockwise fashion starting from the left arm of the diagram proceeds as follows:

- One new dot appears on the left arm, completing the first side of the polygon
- Each of the next $(n-2)$ sides (which are not already in in $P_n(k-1)$) is constructed by measuring out k dots for each side. The last dot in this process appears on the right arm of the diagram, completing the polygon $P_n(k)$.

This yields the recurrence

$$\boxed{P_n(k) = P_n(k-1) + (n-2)k + 1}$$

(c) For $k > 0$ we have the sequence of identities

$$\begin{array}{lcl} P_n(k) - P_n(k-1) & = & (n-2)k + 1 \\ P_n(k-1) - P_n(k-2) & = & (n-2)(k-1) + 1 \\ \vdots & \vdots & \vdots \\ P_n(1) - P_n(0) & = & (n-2).1 + 1 \end{array}$$

Summing both sides of the above sequence we get

$$\begin{array}{rcl} P_n(k) - P_n(0) & = & (n-2).\sum_{i=1}^{k} i + \sum_{i=1}^{k} 1 \\ P_n(k) - 1 & = & (n-1).\frac{k(k+1)}{2} + k \\ \Rightarrow \quad P_n(k) & = & \frac{(k+1)}{2}.[(n-2).k + 2] \end{array}$$

5. **[10 marks]** Prove that the ring of integers modulo 2 (i.e. $\mathbb{Z}/=_2$) is a boolean ring, by

   (a) clearly identifying the sum and product operations, and

   (b) proving that it satisfies all the properties of a boolean ring.

Solution

The intuition behind this is that it is possible to define a homomorphic mapping from the ring of integers to the 2-element boolean ring, using the property

$$\mathsf{odd} : \mathbb{Z} \to \{0, 1\}$$

where

$$\mathsf{odd}(m) = \begin{cases} 1 & \text{if } m \text{ is odd} \\ 0 & \text{if } m \text{ is even} \end{cases}$$

Note that the value of $\mathsf{odd}(m) = m \bmod 2$. Further,

- the sum of two odd integes is even
- the sum of two even integers is also even, but
- the sum of an odd integer and an even integer is odd
- the product of two odd integes is odd
- the product of two even integers is even, and
- the product of an odd integer and an even integer is even

Hence when sums and products are taken modulo 2 we get 1 or 0 accordingly

(a) **sum.** $a \oplus b = (a + b) \bmod 2$
product. $a.b = (a.b) \bmod 2$

(b) It is easy to verify the following properties of the boolean ring.
associativity of product and sum $a.(b.c) = (a.b).c$ and $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
commutativity of product and sum $a.b = b.a$ and $a \oplus b = b \oplus a$
distributivity of product over sum $a.(b \oplus c) = (a.b) \oplus (a.c)$
identity for product and sum 1 and 0 respectively
annihilator for product and sum 0 and 1 respectively
idempotence of product $a.a = a$
self-cancellation $a \oplus a = 0$.

6. **[5+5=10 marks]**

   (a) Prove that if $(A, \leq)$ is a well-ordered set (not necessarily finite, and not necessarily countable) and $f : A \to B$ is an order-preserving isomorphism from A to a subset $B \subseteq A$, then for all $x \in A$, $x \leq f(x)$.

   (b) Let $(A, \leq_A)$ and $(B, \leq_B)$ be equipollent well-ordered sets. Then prove that there is exactly one order-preserving isomorphism from A to B.

Solution

(a) Let $C = \{x \in A \mid x \not\leq f(x)\} = \{x \in A \mid f(x) < x\} \subseteq A$. If $C \neq \emptyset$, since $C \subseteq A$ and A is well-ordered, C must have a least element x_0 and $f(x_0) < x_0$. Let $x_1 = f(x_0) < x_0$ and since f is order-preserving we have $f(x_1) < f(x_0) = x_1$, which implies $x_1 \in C$ and x_0 is not the least element of C, contradicting our assumption.

(b) Let $f, g : A \to B$ both be order-preserving isomorphisms from A to B and let $h = g; f^{-1} = f^{-1} \circ g$. Clearly h is also an order-preserving isomorphism from A to B. Further from (6a) we get that for each $x \in A$, $x \leq h(x)$ which implies that for each $x \in A$, $f(x) \leq f(h(x)) = f(f^{-1}(g(x))) = g(x)$.

By a similar reasoning, it follows that $i = f; g^{-1} = g^{-1} \circ f$ is also an order-preserving isomorphism and yields for each $x \in A$, $g(x) \leq f(x)$. From the two inequalities we get $f = g$ and hence there is exactly one order-preserving isomorphism from A to B.