April 15, 2021

Problem 1

Are the following statements tautologies or not? (1p/part)

a) $(P \vee Q) \vee (\neg P \wedge \neg Q)$.
b) $(P \rightarrow Q) \vee (Q \rightarrow P)$.
c) $((P \rightarrow Q) \wedge (Q \rightarrow R)) \rightarrow (P \rightarrow R)$.
d) $((P \wedge Q) \vee R) \leftrightarrow ((P \wedge R) \vee (Q \wedge R))$.

a) Yes. it is always true
b) yes. it is always true
c) yes. it is always true
d) no, it is not a tautology

Problem 2

Let $|A| = n$. Find a formula (in terms of n) for the number of functions $f : A \rightarrow P(A)$ such that $\forall x \in A : x \in f(x)$.

|A| = n => |P(A)| = 2^n

Problem 3

Consider the relation $\preceq$ on $\mathbb{Z}$ given by $x \preceq y$ if there exist $m \in \mathbb{N}$ and an odd integer k such that $kx = 2^m y$.

a) Prove that $\preceq$ is an order relation on $\mathbb{Z}$. (2p)
b) Draw the Hasse diagram of $\preceq$ on the set $\{0, 1, 2, \ldots, 10\}$ (1p)
c) Give an example of a linear extension of $\preceq$ on the set $\{0, 1, 2, \ldots, 10\}$. (1p)

Definition 1.47

A relation $\sim$ on A is called:

- *reflexive* if
$$\forall x \in A : x \sim x.$$
- *symmetric* if
$$\forall x, y \in A : x \sim y \leftrightarrow y \sim x.$$
- *antisymmetric* if
$$\forall x, y \in A : (x \sim y \wedge y \sim x) \to x = y.$$
- *transitive* if
$$\forall x, y, z \in A : (x \sim y \wedge y \sim z) \to x \sim z.$$

Definition 1.58 (Partial order)

A relation $\preceq$ on A is an *order relation* if it is reflexive, antisymmetric, and transitive.

Example 1.59

- $x \leq y$ on $\mathbb{R}$
- $x | y$ on $\mathbb{N}$
- $S \subseteq T$ on $P(\Omega)$.

a)

Problem 3: Relation $\preceq$ on $\mathbb{Z}$ given by $x \preceq y$ if exists $m \in \mathbb{N}$, odd integer k such that $kx = 2^m y$

a) Prove $\preceq$ is an order relation on $\mathbb{Z}$

- Reflexive: $\forall x \in \mathbb{Z}: x \sim x \Rightarrow kx = 2^m x \Rightarrow k = 2^m$

  Let $m = 0$, $k = 1 \Rightarrow 1 = 2^0 \Rightarrow$ exists m and k that satisfies the equation

  $\Rightarrow \preceq$ is reflexive
- Antisymmetric: $\forall x, y \in \mathbb{Z}\ (x \sim y \wedge y \sim x) \rightarrow x = y$

  $\Rightarrow (kx = 2^m y) \wedge (ky = 2^m x) \rightarrow x = y$

  $\Rightarrow kx - 2^m x = ky - 2^m y \Rightarrow x(k - 2^m) = y(k - 2^m)$. If $x \neq y$

  $\Rightarrow k - 2^m = 0 \Rightarrow k = 1, m = 0 \Rightarrow 1x = 2^0 y \Rightarrow x = y$ (contradiction) $\Rightarrow x = y$ (proven)
- Transitive: $\forall x, y, z \in \mathbb{Z}: (x \sim y \wedge y \sim z) \rightarrow x \sim z$

  $\Rightarrow (kx = 2^m y) \wedge (ky = 2^m z) \rightarrow (kx = 2^m z)$

  $\Rightarrow kx = 2^m((2^m z)/k) \rightarrow kx = 2^m z \Rightarrow \frac{2^m}{k} = 1 \Rightarrow 2^m = k$

  $\Rightarrow m = 0$, $k = 1 \Rightarrow$ exists m & k that satisfies the equation

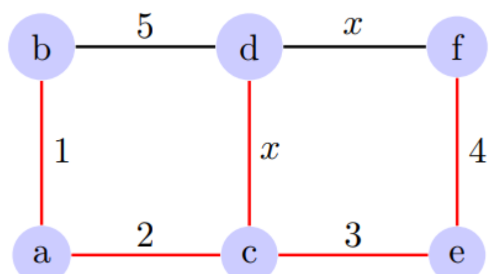
  $\Rightarrow \preceq$ is transitive

$\Rightarrow \preceq$ is an order relation on $\mathbb{Z}$

b)

PROBLEM 4

In the weighted graph below, the red edges form a minimal spanning tree. What can you say about the unknown weight $x \in \mathbb{R}$?



Problem 5

We know that

$$2^{11} = 2048$$

and that

$$2021 = 43 \cdot 47.$$

Using these facts, find a number k such that

$$27^k \equiv 2 \mod 2021.$$

Problem 5:

- we have $2^{11} = 2048$, $2021 = 43 \cdot 47$. Find k such that $27^k \equiv 2 \pmod{2021}$

  We notice that $2048 = 2021 + 27 \Rightarrow 2048 \equiv 27 \pmod{2021}$

  $\Rightarrow 27^k \equiv 2 \pmod{2021}$

  $\Rightarrow (2^{11})^k \equiv 2 \pmod{2021} \Rightarrow 2^{11k} \equiv 2 \pmod{2021}$

- Modular multiplication rule: $(A * B) \bmod C = (A \bmod C * B \bmod C) \bmod C$. We want to divide 2^{11k} into 2 parts $2 \times m$, where $m \equiv 1 \pmod{2021}$

  $\Rightarrow 2 \times 2^{11k-1} \equiv 2 \pmod{2021} \Rightarrow m = 2^{11k-1}$

  $\Rightarrow 2^{11k-1} \equiv 1 \pmod{2021}$

  We have $2021 = 43 \times 47 \Rightarrow \phi(2021) = (43-1)(47-1) = 1932$

  and $\gcd(2, 2021) = 1 \Rightarrow$ According to Euler's theorem

  $\Rightarrow 2^{\phi(2021)} \equiv 1 \pmod{2021}$ or $2^{1932} \equiv 1 \pmod{2021}$

- According to modular exponential rule: $(A^B) \bmod C = (A \bmod C)^B \bmod C$

  $\Rightarrow (2^{1932}) J = 2^{1932J} \bmod 2021 = (2^{1932} \bmod 2021)^J \bmod 2021$

  $\Rightarrow 2^{1932J} \equiv 1 \pmod{2021}$, since $1^J = 1$

  $\Rightarrow$ we need to find $J, k \in N$ such that $11k - 1 = 1932J$

  Let $J = 1 \Rightarrow k \notin N$. $J = 2 \Rightarrow k \notin N$ but $J = 3 \Rightarrow k = 527 \in N$

  $\Rightarrow$ Answer: $k = 527$, $27^{527} \bmod 2021 = 2$

Tehtävä 1:

a) Määritellään relaatio $\sim$ joukossa $\mathbb{Z}$ asettamalla $x \sim y \Leftrightarrow x$:llä ja y:llä on sama pariteetti (ts. molemmat parillisia tai molemmat parittomia). Perustele tarkasti miksi relaatio $\sim$ on ekvivalenssirelaatio ja määritä sen ekvivalenssiluokat.

b) Monelleko funktiolle $f\colon \{1,2,3,4,5,6,7,8\} \to \{0,1,2,3,4,5,6\}$ pätee $|f^{-1}(\{2\})| = 4$?

Tehtävä 2: Todista induktiolla, että

$$\sum_{k=1}^{n}(2k+3) = n^2 + 4n$$

kaikille $n \in \mathbb{Z}_+$. Muista kirjoittaa selkeästi näkyviin, mikä on käyttämäsi induktio-oletus ja missä kohtaa todistusta sitä käytät.

Tehtävä 3: Kymmenen teekkaria on juhlimassa. Saapuessaan juhlapaikalle he jättävät teekkarilakkinsa eteiseen. Lähtiessään kukin nappaa yhden lakin taas mukaansa. Kuinka monta eri tapaa lakeilla on jakautua teekkareille, kun tiedetään, että kuusi teekkaria saa oman lakkinsa, mutta neljä ei? Perustele vastauksesi!

Tehtävä 4: Osoita, että renkaan $\mathbb{Z}_n$ alkiolla a on olemassa käänteisalkio jos ja vain jos luvut n ja a ovat keskenään jaottomat (eli syt$(a,n) = 1$).

Problem 1:
a) Define the relation ~ on the set Z by setting x ~ y, x and y have the same parity
(i.e., both even or both odd). Justify exactly why the relation ~ is equivalence relation and determine its equivalence classes.
b) For many functions f: {1; 2; 3; 4; 5; 6; 7; 8} -> {0; 1; 2; 3; 4; 5; 6} that holds |f −1({2})| = 4?

Problem 4:
Show that for the element a of the ring Zn there exists an inverse element if and only if the numbers n and
a are indivisible (i.e. syt (a; n) = 1)

Problem 1:

a) Define relation $\sim$ on $\mathbb{Z}$ with $x \sim y$ if x and y have the same parity (both even or both odd). Justify why $\sim$ is equivalence relation

- Reflexive: $\forall x \in \mathbb{Z}: x \sim x$. This is obvious because if x is even, it will relate to any number $\in \mathbb{Z}$ that are also even, including itself. The same argument for odd x
- Symmetric: $\forall x, y \in \mathbb{Z}: x \sim y \leftrightarrow y \sim x$
  If x is even $\rightarrow$ y is even. Since y is even, it also relates to x as x is even
  $\sim$ odd $\sim$ odd $\sim$ odd $\sim$ odd
- Transitive: $\forall x, y, z \in \mathbb{Z}: (x \sim y \land y \sim z) \rightarrow x \sim z$
  If x is even $\rightarrow$ y is even. As y is even $\rightarrow$ z is also even due to parity. Finally, as x and z are both even, they relate to each other. Same argument for odd

$\Rightarrow$ There are two equivalence classes of $\sim$

Odd class: $[1] = \{\ldots, -3, -1, 1, 3, \ldots\}$

Even class: $[0] = \{\ldots -4, -2, 0, 2, 4, \ldots\}$

Number of functions from one set to another: Let X and Y are two sets having m and n elements respectively. In a function from X to Y, every element of X must be mapped to an element of Y. Therefore, each element of X has 'n' elements to be chosen from. Therefore, total number of functions will be n×n×n.. m times = n^m.

For example: X = {a, b, c} and Y = {4, 5}. A function from X to Y can be represented in Figure 1.

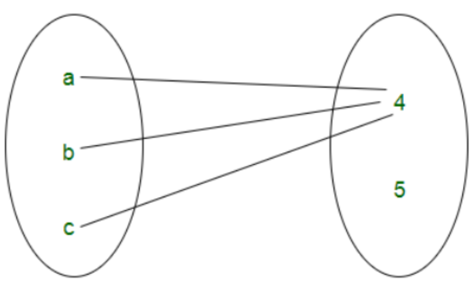


Figure 1 : Function from X to Y

Since the inverse of 2 is strictly 4, so we can drop this pair from both domain and codomain. Now, domain has 7 elements and codomain has 6 elements => There are 6^7 functions that holds true

Problem 2: prove by induction : $\sum_{k=1}^{n}(2k+3) = n^2+4n$, $n \in Z^+$

Base case: $(n = 1)$: $\sum_{k=1}^{1}(2k+3) = 2\times 1+3 = 5 \Rightarrow$ base case holds for $n = 1$

$1^2 + 4\times 1 = 5$

Induction step: Assume (IH) that $\sum_{k=1}^{m}(2k+3) = m^2+4m$

$\cancel{\sum_{k=1}^{m+1}(2k+3) = (m+1)^2+4(m+1}$

$$\begin{aligned}\sum_{k=1}^{m+1}(2k+3) &\overset{def}{=} \left(\sum_{k=1}^{m}(2k+3)\right) + 2(m+1)+3 \\ &\overset{IH}{=} m^2+4m+2m+2+3 \\ &= (m^2+2m+1)+(4m+4) \\ &= (m+1)^2+4(m+1)\end{aligned}$$

so the statement is also true for $n = m+1$ (proven)

Problem 3:

Ten tekkaris are celebrating. When they arrive at the party, they leave their tea caps in the hallway. When they leave, they grab one cap again. How many different ways caps have to divide into tekkaris when it is known that six tekkaris get their own caps, but four do not? justify your answer

Task 5:

a) Let π = (1 2 3) and ρ = (2 3 4) be the permutations of S5. Express πρ and ρπ both in matrix form and as a cyclic representation.

b) In how many different ways can the vertices of an equilateral triangle be colored if three different colors are available and the cases obtained by inverting the triangle in three-dimensional space are not distinguished?

Task 6:

Define precisely the concepts in the course, chromatic number and minimum spanning tree and give an example of both as well. Then introduce something for each concept application where it could be exploited

- Chromatic number: The chromatic number of a graph is the smallest number of colors needed to color the vertices of so that no two adjacent vertices share the same color
- Minimum spanning tree: A minimum spanning tree (MST) or minimum weight spanning tree is a subset of the edges of a connected, edge-weighted undirected graph that connects all the vertices together, without any cycles and with the minimum possible total edge weight.
- application of chromatic number: Scheduling Vertex coloring models to a number of scheduling problems [8]. In the cleanest form, a given set of jobs need to be assigned to time slots, each job requires one such slot. Jobs can be scheduled in any order, but pairs of jobs may be in conflict in the sense that they may not be assigned to the same time slot, for example because they both rely on a shared resource. The corresponding graph contains a vertex for every job

and an edge for every conflicting pair of jobs. The chromatic number of the graph is exactly the minimum makespan, the optimal time to finish all jobs without conflicts.
- Application of minimum spanning tree: Minimum spanning trees are used for network designs (i.e. telephone or cable networks). They are also used to find approximate solutions for complex mathematical problems like the Traveling Salesman Problem

Tehtävä 1: Osoita, että kaikilla $n \in \mathbb{Z}_+$ pätee

$$(1+2+3+\ldots+n)^2 = 1^3+2^3+3^3+\ldots n^3.$$

Tehtävä 2: Osoita, että joukot $\mathbb{Z}$ ja $\{2n \ : n \in \mathbb{N}\}$ ovat yhtä mahtavia.

Tehtävä 3: Tarkastellaan tavallista 52 kortin korttipakkaa (neljä maata, kutakin 13 korttia, numeroarvot 2-13 ja ässä).

a) Kuinka monta erilaista viiden kortin kättä (eli järjestämätöntä joukkoa) on olemassa?

b) Pokerissa viiden kortin kättä, jossa kaikki kortit ovat samaa maata, kutsutaan väriksi. Montako viiden kortin väriä on olemassa?

c) Viiden kortin kättä, jossa korteilla on peräkkäiset numeroarvot, kutsutaan suoraksi. Ässää voi käyttää numeroarvoina 1 ja 14, eli suora saa alkaa ässällä tai päättyä siihen, mutta ässä ei saa olla keskellä suoraa. Montako suoraa on olemassa?

d) Montako sellaista viiden kortin suoraa on olemassa, jotka eivät ole värejä?

Perustele vastauksesi.
Vastauksia ei tarvitse laskea auki, niihin saa jäädä esim. kertomerkkejä, potensseja, summia, binomikertoimia, multinomikertoimia ja kertomia.

Tehtävä 4: a) Etsi jäännösluokkarenkaan $\mathbb{Z}_9$ kääntyvät alkiot ja niiden käänteisalkiot.

b) Ratkaise x, kun

$$5x \equiv 3 \mod 9$$

tai perustele, miksi ratkaisua ei ole.

Tehtävä 5: Tarkastellaan permutaation $g = (123)(45)$ generoimaa ryhmää $G = \langle g \rangle$, joka toimii joukossa $M = \{1, 2, 3, 4, 5\}$.

a) Mitkä kaikki permutaatiot kuuluvat ryhmään G?

b) Etsi kunkin ryhmän G permutaation sykli-indeksi.

c) Mikä on ryhmän G sykli-indeksi?

Tehtävä 6: Tarkastellaan suuntaamatonta verkkoa $G = (V, E)$, jossa $V = \{a, b, c, d, e, f, g\}$ ja $E = \{\{a, c\}, \{a, d\}, \{d, c\}, \{c, b\}, \{b, e\}, \{e, c\}, \{f, b\}, \{f, g\}, \{g, e\}\}$.

a) Piirrä verkon kuva.

b) Onko verkossa Hamiltonin kävelyä, eli kävelyä, johon kuuluvat kaikki verkon solmut?

c) Onko verkossa Hamiltonin sykliä?

Kohdissa b) ja c) joko anna kävely/sykli tai perustele, miksi sitä ei ole.