DISCRETE MATHEMATICS

SOLUTIONS

Solutions to Exploratory Exercises.

Problem 1. Many composed statements (in mathematics and elsewhere) can be written using the logical symbols $\wedge$ ("and"), $\vee$ ("or"), $\rightarrow$ ("if...then..."), $\neg$ ("not"), $\leftrightarrow$ ("if and only if", "is equivalent to"). Whether these composed statements are true or false depends on whether or not the *elementary* statements that they are composed of are true. For example, the composed statement "it rains and it is cold" is true precisely if the elementary statements "it rains" and "it is cold" are both true. Thus, we can *define* the truth value of the composed statement $A \wedge B$ by the following *truth table*, where T and F denote the truth values "true" and "false" respectively:

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

(a) Make sure you understand the meaning of this truth table.
(b) Write similar truth tables that define the symbols $\wedge$ ("and"), $\vee$ ("or"), $\neg$ ("not"), $\leftrightarrow$ ("if and only if", "is equivalent to").
(c) Please agree with me that the composed statement $x > 3 \rightarrow x^2 > 9$ should be true for all values of x. What is the truth value of the elementary statements $x > 3$ and $x^2 > 9$, when $x = 0$? When $x = 4$? When $x = -4$?
(d) Using your answer in (3), write down a truth table for the implication symbol $\rightarrow$.

Solution:

(a) The statement $A \wedge B$ is True if A and B are both True and False otherwise.

(b)

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

A	B	$\neg A$	$\neg B$
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

A	B	$A \leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

(c) If the statement $x > 3$ is true then the statement $x^2 > 9$ is also true. Hence the implication is true.
i) When $x = 0$, the truth value is *False* for both statements.
ii) When $x = 4$, the truth value is *True* for both statements.

ii) When $x = -4$, the truth value is *False* for the first statement and *True* for the second.

(d) Let A and B be the statements $A = \{x > 3\}$ and $B = \{x^2 > 9\}$

A	B	$A \to B$
T	T	T
F	T	T
F	F	T

Problem 2. Many mathematical statements also contain quantifiers such as $\forall$ ("for all") and $\exists$ ("there exists").

(a) Let $F(x, y)$ be the predicate "x and y are friends". Interpret the following two statements in natural language. Are they different?
- $\forall x \exists y : F(x, y)$
- $\exists y \forall x : F(x, y)$

(b) What are the negations (opposites) of the statements in the previous question?

(c) What is the negation of an "all-quantified" statement $\forall x P(x)$ (where P is an arbitrary predicate)?

(d) What is the negation of an "exists-quantified" statement $\exists x P(x)$?

Solution:

(a)
- Everyone has atleast one friend.
- There exist someone who is friends with everyone.

No, they are not same.

(b)
- There is someone who doesn't have a friend
- There is no one who is friends with everyone.

(c) $\exists x \neg P(x)$

(d) $\forall x \neg P(x)$

Problem 3. A set is nothing more than a collection of things (*elements*). Examples of sets include the set $\mathbb{R}$ of all real numbers, the set of all blue cars, the set of subsets of $\mathbb{R}$, etcetera. The language of sets contains the symbols $\in$ ("is a member of") and $\subseteq$ ("is contained in").

(a) What does it mean that two sets are equal? Formulate this as a logical statement using the logical symbols $\forall$, $\leftrightarrow$, and the set theory symbol $\in$.

(b) Draw a Venn diagram that describes the statement

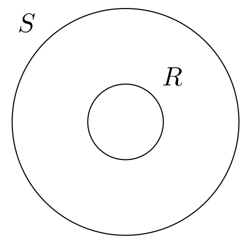
$$\forall x : x \in R \to x \in S,$$

where R and S are sets. Can you formulate this statement purely in the language of set theory?

Solution:

(a) Let A and B be two set, $A = B \leftrightarrow \forall x \in A, x \in B$ and $\forall y \in B, y \in A$

(b) $R \subset S$



Problem 4. The *power set* $P(S)$ consists of all subsets of the set S. The *cartesian product* $S \times T$ of two sets is the set $\{(s,t) : s \in S, t \in T\}$.

(a) Let $S = \{a, b, c\}$, $T = \{1, 2\}$. Write down $S \times T$, $P(S)$ and $P(T)$.
(b) Let S be a finite set with $|S| = n$ elements and let T be a finite set with $|T| = m$ elements. How many elements does $S \times T$ have?
(c) How many elements does $P(S)$ have, if S has n elements?

Solution:

(a) $S \times T = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$,
$P(T) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
$P(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$
(b) $|S \times T| = m \times n$
(c) $|P(T)| = 2^n$

<u>Solutions to Additional Exercises.</u>

Exercise 1

(i) Come up with three sentences (that can be true or false), and denote them by p, q and r. Formulate the following eight composed sentences in natural language, and convince yourself that they "should be" pairwise equivalent, accord- ing to your intuition.

p : It is sunny
q: Places are warm
r: John is happy

(a) $p \to q$: If it is sunny then places are warm. $\neg q \to \neg p$: If places are not warm, then it is not sunny. The others follows in similar manner.(If not clear,I could detail all the other phrases).

(b) $p \leftrightarrow q$: It is Sunny if and only if places are warm. and $(p \wedge q) \vee (\neg p \wedge \neg q)$: It is sunny and places are warm or it is not sunny and places are not warm. The others follows in similar manner.

(ii) Prove using truth tables that they are indeed equivalent.

(a) $p \to q$ and $\neg q \to \neg p$

p	q	$\neg q$	$\neg p$	$\neg q \to \neg p$	$p \to q$
1	1	0	0	1	1
1	0	1	0	0	0
0	1	0	1	1	1
0	0	1	1	1	1

(b) $p \leftrightarrow q$ and $(p \wedge q) \vee (\neg p \wedge \neg q)$

p	q	$\neg q$	$\neg p$	$p \wedge q$	$\neg p \wedge \neg q$	$p \leftrightarrow q$	$(p \wedge q) \vee (\neg p \wedge \neg q)$
1	1	0	0	1	0	1	1
1	0	1	0	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	1	1	1	1

(c) $p \leftrightarrow q$ and $(p \to q) \wedge (q \to p)$

p	q	$p \to q$	$q \to p$	$(p \to q) \wedge q \to p)$	$p \leftrightarrow q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	1	0	0	0
0	0	1	1	1	1

(d) $(p \to r) \vee (q \to r)$ and $(p \wedge q) \to r$

p	q	r	$p \to r$	$q \to r$	$p \wedge q$	$(p \wedge q) \to r$	$(p \to r) \vee (q \to r)$
1	1	1	1	1	1	1	1
1	1	0	0	0	1	0	0
1	0	1	1	1	0	1	1
1	0	0	0	1	0	1	1
0	1	1	1	1	0	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	0	1	1
0	0	0	1	1	0	1	1

Exercise 2

Are the following sentences true or false?

(a) $0 \in \{0\}$. True
(b) $\{0\} \in 0$. False
(c) $0 \in Z$. True
(d) $0 \subset Z$. False
(e) $\{0\} \subset Z$. True
(f)) $0 \in \{0, \{0\}, \{0, \{0, \{0\}\}\}\}$. True
(g) $0 \in \emptyset$ False
(h) $\emptyset \in \{0\}$ False
(i) $\emptyset \subset \{0\}$ True
(j) $\emptyset = \{0\}$ False

Exercise 3

Show that if A and B are sets such that $A \times B = B \times A$, then either $A = B$ or $A = \emptyset$ or $B = \emptyset$.

Suppose A and B are non-empty sets. Let $a \in A$, hence $\exists b \in B$, s.t $(a, b) \in A \times B = B \times A$(by hypothesis) $\Longrightarrow (a, b) \in B \times A \Longrightarrow a \in B \Longrightarrow A \subset B$. Following same argument we have that $B \subset A$. Hence $A = B$.

Exercise 4

Show that if $A \subseteq B$ and $C \subseteq D$, then $A \times C \subseteq B \times D$.

Let $(x, y) \in A \times C$ with $x \in A$ and $y \in C \Longrightarrow x \in B$ and $y \in D$ Hence $(x, y) \in B \times D$. Therefore, $A \times C \subseteq B \times D$.

Exercise 5

Write down the truth table of the composed statement $(p \vee q) \to (p \wedge \neg r)$.

p	q	r	$\neg r$	$p \vee q$	$p \wedge \neg r$	$(p \vee q) \to (p \wedge \neg r)$
1	1	1	0	1	1	1
1	1	0	1	0	1	0
1	0	1	0	1	0	1
1	0	0	1	1	0	1
0	1	1	0	1	0	1
0	1	0	1	0	0	1
0	0	1	0	1	0	1
0	0	0	1	1	0	1

Exercise 6

Let $L(x, y)$ be the sentence "x loves y". Write the following sentences using connectives, quantors, equality signs, and the elementary sentence L. Let r =Raymond.

a) Everybody loves Raymond. $\forall x, L(x, r)$
b) Everybody loves somebody. $\forall x, \exists y; L(x, y)$
c) There exists somebody who everybody loves. $\exists y, \forall x, L(x, y)$
d) Nobody loves everybody. $\forall y \exists x; \neg L(x, y)$
e) There is some person, whom Raymond does not love. $\exists x, \neg L(x, r)$.
f) There is some person, whom nobody loves. $\exists y, \forall x, \neg L(x, y)$
g) There is exactly one person, whom everybody loves.

$$\exists y \forall x (L(x, y) \wedge \forall z (L(x, z) \to z = y))$$

(I could detail this in 2 cases if not clear)

h) Raymond loves exactly two persons.

$$\exists x, y(x \neq y \wedge L(r, x,) \wedge L(r, y) \wedge \forall z(x \neq x \wedge y \neq z \to \neg L(r, z)))$$

(I could detail this into two cases if not clear)

i) Everybody loves themselves. $\forall x, L(x, x)$.
j) There is somebody, who only loves themself. $\exists y(L(y, y) \wedge \forall x(L(y, x) \to x = y))$.

Discrete Mathematics

Solutions For Exercise 2

March 5, 2022

Exploratory Exercises

Problem 1

Give an example of a function $f : \mathbf{Z} \to \mathbf{Z}$ that is

a) Injective but not surjective $f(x) = 2x$

$\star$ Injective: Suppose $\forall x, y \in \mathbb{Z} : f(x) = f(y) \implies 2x = 2y \implies x = y$ hence f is injective.

$\star$ Surjective: Let $y \in \mathbb{Z}$ and $f(x) = y \implies 2x = y \impliedby x = \frac{y}{2} \notin \mathbb{Z}$. Hence, f is not surjective.

b) Surjective but not injective. $f(x) = \lfloor \frac{x}{2} \rfloor$

$\star$ Injective: $f(0) = f(1) = 0$ but $0 \neq 1$ hence, f is not injective.

$\star$ Surjective: $f(2x) = x \forall x \in \mathbb{Z}$. Hence, f is surjective.

c) Both injective and surjective. $f(x) = x$. This is clear.

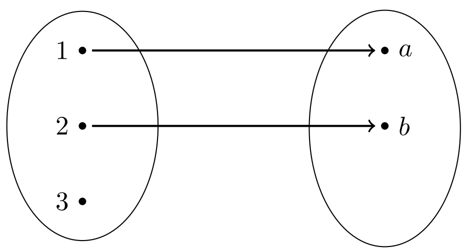
d) Neither injective nor surjective. $f(x) = x^2$

$\star$ Injective: $f(1) = f(-1)$ but $-1 \neq 1$ hence, f is not injective.

$\star$ Surjective: Let $y \in \mathbb{Z}$ and $f(x) = y \implies x = \sqrt{y} \notin \mathbb{Z}$ if y is not a square number. Hence, f is not surjective.

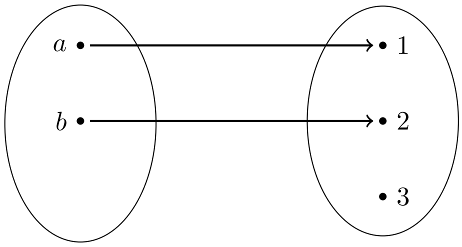
Problem 2

a) No there exist no injective map for the number of elements in the domain exceeds those of the codomain.



(b) No there exixs no surjective map.

(c) If there is an injection, $|A| \leq |B|$. And if the map is surjective, $|B| \leq |A|$



Problem 3

a) For the four examples above, determine if they are reflexive, transitive, and/or symmetric.

i) x and y are siblings: Obviously this is Symmetric, not Reflexive, it is transitive if we are only considering "full siblings." But if we consider half siblings, then it is not transitive(for example if A and B have the same mother but different fathers, and B and C have the same father but different mothers).

ii) x divides y.: $x = x.1 \to x|x$ so Reflexive. It is not symetric since $x|y \nRightarrow y|x$ e.g $1|2$ but $2 \nmid 1$. Lastly, it is Transitive since if $a|b \Rightarrow \exists k \in \mathbb{Z} : b = ak$ and $b|c \Rightarrow \exists l \in \mathbb{Z} : c = bl = akl = am$ where $m = kl \in \mathbb{Z}$.Therefore $a|c$

iii) $x < y$ in $\mathbb{R}$: Clearly Transitive. But not Reflexive since $1 \nless 1$ and not Symmetric since $0 < 1 \nRightarrow 1 < 0$.

iv) $x = y$ Cleary Relexive, Transitive and Symetric.

b) i) The relation $x = y$.

ii) The relation $R = \{(x, x), (y, y), (z, z), (x, y), (y, z)\}$

iii) $x \neq y$

iv) $x < y$

Additional Exercises

Problem 1

Prove that, if A, B and C are sets, then $(A \cup B) \times C = (A \times C) \cup (B \times C)$

- $(A \cup B) \times C \subseteq (A \times C) \cup (B \times C))$: Let $(x, y) \in (A \cup B) \times C \Rightarrow a \in A \cup B$ and $y \in C \Rightarrow x \in A$ and $y \in C$ or $x \in B$ and $y \in C$. Therefore $(x, y) \in A \times C$ or $(x, y) \in B \times C$. Hence $(x, y) \in (A \times C) \cup (B \times C))$.
- $(A \times C) \cup (B \times C)) \subseteq (A \cup B) \times C$: Let $(x, y) \in (A \times C) \cup (B \times C)) \Rightarrow (x, y) \in (A \times C)$ or $(x, y) \in (B \times C) \Rightarrow x \in A \cup B$ and $y \in C$.

Problem 2

Prove that $(\mathbb{Z} \times \mathbb{R}) \cap (\mathbb{R} \times \mathbb{Z}) = \mathbb{Z} \times \mathbb{Z}$

- $(\mathbb{Z}\times\mathbb{R})\cap(\mathbb{R}\times\mathbb{Z})\subseteq\mathbb{Z}\times\mathbb{Z}$: Let $(x,y)\in(\mathbb{Z}\times\mathbb{R})\cap(\mathbb{R}\times\mathbb{Z})\Rightarrow(x,y)\in(\mathbb{Z}\times\mathbb{R})$ and $(x,y)\in(\mathbb{R}\times\mathbb{Z})\Rightarrow(x,y)\in\mathbb{Z}\times\mathbb{Z}$ since x is an integer from the first product and y is an integer from the second.
- $\mathbb{Z}\times\mathbb{Z}\subseteq(\mathbb{Z}\times\mathbb{R})\cap(\mathbb{R}\times\mathbb{Z})$: Let $(x,y)\in\mathbb{Z}\times\mathbb{Z}\Rightarrow x\in\mathbb{Z}\subset\mathbb{R},\Rightarrow(x,y)\in\mathbb{R}\times\mathbb{Z}$ similarly, $y\in\mathbb{R}\Rightarrow(x,y)\in\mathbb{Z}\times\mathbb{R}$. Hence $(x,y)\in(\mathbb{Z}\times\mathbb{R})\cap(\mathbb{R}\times\mathbb{Z})$

Problem 3

$$\begin{aligned} f:&\mathbb{R}\longrightarrow\mathbb{R} & \qquad g:&\mathbb{R}\longrightarrow\mathbb{R}\\ x&\longmapsto 4x-3 & y&\longmapsto\frac{y+3}{4}\end{aligned}$$

$$\begin{cases} f(g(y))=f(\frac{y+3}{4})=4(\frac{y+3}{4})-3=y\\ \\ g(f(x))=g(4x-3)=x\end{cases}$$

Problem 4

a) Clearly $\sim$ is Reflexive sinve $x^2-x^2=0\in\mathbb{Z}$. Also it is symmetric since the negative of an integer is also an integer. Lastly it is transitive for if $x^2-y^2\in\mathbb{Z}$ and $y^2-z^2\in\mathbb{Z}$, then $x^2-z^2=(x^2-y^2)+(y^2-z^2))\in\mathbb{Z}$. Hence $\sim$ is indeed an Equivalence relation.

b) $[0]=\{a|0Ra,\forall a\in\mathbb{R}\}=\{a|-a^2\in\mathbb{Z},\forall a\in\mathbb{R}\}=\{\ldots,-\sqrt{3},-\sqrt{2},-1,0,1,\sqrt{2},\sqrt{3}\ldots\}$

c) $[\frac{1}{3}]=\{a|\frac{1}{3}Ra,\forall a\in\mathbb{R}\}=\{a|\frac{1-(3a)^2}{9}\in\mathbb{Z},\forall a\in\mathbb{R}\}=\left\{\ldots,-\frac{\sqrt{19)}}{3},-\frac{\sqrt{10}}{3},-\frac{1}{3},\frac{1}{3},\frac{\sqrt{10}}{3},\frac{\sqrt{19}}{3}\ldots\right\}$

Problem 5

Prove by induction that for every $n\in\mathbb{N}$ holds $\displaystyle\sum_{i=1}^{n}\frac{i}{(i+1)!}=1-\frac{1}{(n+1)!}$

- Base Case Verify for $n=1$: $\displaystyle\sum_{i=1}^{n}\frac{i}{(i+1)!}=\frac{1}{2}=1-\frac{1}{2!}$ so True for $n=1$.
- I.H: Assume true for $n=k$. i.e $\displaystyle\sum_{i=1}^{k}\frac{i}{(i+1)!}=1-\frac{1}{(k+1)!}$
- Verify for $n=k+1$:

  $$\sum_{i=1}^{k+1}\frac{i}{(i+1)!}=\sum_{i=1}^{k}\frac{i}{(i+1)!}+\frac{k+1}{(k+2)!}=1-\frac{1}{(k+1)!}+\frac{k+1}{(k+2)!}=1-\frac{1}{(k+2)!}$$

  Hence statement is true for all $n\in\mathbb{N}$

Problem 6

The thrid point: In particular "Clearly, these colours must be the same, as the socks $s_2 \ldots s_n$ can only have one colour" is wrong when $n = 1$ (because then the set $s_2 \ldots s_n$ is empty). This highlights the fact that already if the induction step fails for one particular value of n, the induction proof collapses.

Problem 7

The statement is not true for the base case. i.e for $n = 1$, $1 \neq \frac{9}{8}$

Problem 8

By Double induction show that the Fibonacci numbers satisfy

$$f_{m+n+1} = f_m f_n + f_{m+1} f_{n+1} \; \forall m, n \geq 0.$$

Let the statement be denoted by $P(m, n)$

- Base Case $P(0, 0) : f_1 = 1 = f_1 f_1$ since $f_0 = 0, f_1 = 1$ So statement true.
- Assume $P(m, n)$ and $P(m, n-1)$ true $\forall m, n \geq 0$. We show that $P(m, n+1)$ is also true.

$$\begin{aligned} f_{m+n+2} = f_{m+n+1} + f_{m+n} &\overset{\text{I.H}}{=} f_m f_n + f_{m+1} f_{n+1} + f_{n-1} f_m + f_n f_{m+1} \\ &= f_m f_{n+2} + f_{m+1} f_{n+2} \end{aligned}$$

- Similarly, assume $P(m, n)$ and $P(m-1, n)$ true $\forall m, n \geq 0$ Show $P(m + 1, n)$ is also true.

$$\begin{aligned} f_{m+n+2} = f_{m+n+1} + f_{m+n} &\overset{\text{I.H}}{=} f_m f_n + f_{m+1} f_{n+1} + f_n f_{m-1} + f_n f_{m+1} \\ &= f_n f_{m+2} + f_{n+1} f_{m+2} \end{aligned}$$

  This implies $P(m, n)$ is true $\forall m, n \geq 0$

HOME WORK 1
SOLUTIONS

Problem 1. (10pts) Prove that if $n \in \mathbb{Z}$, then $n^2 + 3n + 4$ is even.

Solution: Proving by Direct proof we consider the two cases:

- Case 1: Assume n is even. This implies $n = 2k, k \in \mathbb{Z}$

$$\begin{aligned} \Longrightarrow n^2 + 3n + 4 &= 4k^2 + 6k + 4 \\ &= 2(2k^2 + 3k + 2) \\ &= 2m, m = 2k^2 + 3k + 2 \in \mathbb{Z} \end{aligned}$$

- Case 2: assume n is odd i.e $n = 2k + 1, k \in \mathbb{Z}$

$$\begin{aligned} \Longrightarrow n^2 + 3n + 4 &= 4k^2 + 10k + 8 \\ &= 2(2k^2 + 5k + 4) \\ &= 2m, m = 2k^2 + 5k + 4 \in \mathbb{Z} \end{aligned}$$

Problem 2. (10pts) Prove that there exists no integers a and b for which $24a+6b = 1$.

Solution: Proving by contradiction we suppose there exist integers a and b for which $24a + 6b = 1 \Longleftrightarrow 6(4a + 1) = 1 \Longrightarrow 4a + 1 = \frac{1}{6} \notin \mathbb{Z}$ which is a contradiction since $4a + 1 \in \mathbb{Z}$

Problem 3. (10pts) Prove by induction that for all $n \in \mathbb{Z}_+ = \{1, 2, \dots\}$ we have

$$\sum_{k=1}^{n} (-1)^k k^2 = \frac{(-1)^n (n+1)n}{2}.$$

Solution:

- Base case: Verify for $n = 1$

$$\text{LHS:} \sum_{k=1}^{n} (-1)^k k^2 = -1$$

$$\text{RHS:} \frac{(-1)^n (n+1)n}{2} = -1$$

Hence statement is true for the case $n = 1$.

- Assume the statement is true for n .i.e. $\sum_{k=1}^{n} (-1)^k k^2 = \frac{(-1)^n (n+1)n}{2}$.

- Verify if statement is true $n+1$.

$$\begin{aligned}\sum_{k=1}^{n+1}(-1)^k k^2 &= \sum_{k=1}^{n}(-1)^k k^2 + (-1)^{n+1}(n+1)^2 \\ &\overset{I.H}{=} \frac{(-1)^n(n+1)n}{2} + (-1)^{n+1}(n+1)^2 \\ &= \frac{(-1)^n(n+1)n + 2(-1)^{n+1}(n+1)^2}{2} \\ &= \frac{(-1)^{n+1}(n^2+3n+2)}{2} \\ &= \frac{(-1)^{n+1}(n+1)(n+2)}{2}\end{aligned}$$

Hence statement is true for $n+1$. Therefore statement is true $\forall n \in \mathbb{N}$.

Problem 4. (10pts) Define a relation $\sim$ on $\mathbb{R}$ by $a \sim b$ if and only if $a \leq b$. Check if $\sim$ is (i) reflexive, (ii) symmetric, and/or (iii) transitive, and prove it if it does. If it does not satisfy the property you are checking, give an example to show it.

Solution:

(i) Reflexive: $a \leq a \Longrightarrow a \sim a$ hence reflexive.
(ii) Symmetry: If $a \leq b$ it's not generally true that $b \leq a$ e.g $1 \leq 2$ but $2 \not\leq 1$ hence the relation is not symmetric
(iii) Transitive: If $a \leq b$ and $b \leq c \Longrightarrow a \leq c$ hence transitive.

1 Explorative Exercises

1.1

1.1.1

Example:
$f : \mathbb{N} \to B$, $B = \mathbb{N}_{\geq 1}$, $f(x) = x + 1$
Surjective function: $f^{-1} : B \to \mathbb{N}$, $f^{-1}(x) = x - 1$
If an injection exists, then $|\mathbb{N}| \leq |B|$. This condition is sufficient for there to exist a surjection from B to $\mathbb{N}$.

1.1.2

Example:
$f : \mathbb{N} \to B$, $B = \{1\}$, $f(x) = 1$
Surjective function: $g : B \to \mathbb{N}$, $g(1) = 1$
If a surjection exists, then $|\mathbb{N}| \geq |B|$. This condition is sufficient for there to exist an injection from B to $\mathbb{N}$.

1.1.3

This is true in general (Partition Principle)

1.2

1.2.1

For the first position we have n choices, $n - 1$ for the second one, $n - 2$ for the third one, and so on. The later number of choices are independent of the first choices, hence we get $n!$

1.2.2

We are given that $\binom{n}{k}$ is the number of ways to choose k elements out of a set of size n. Additionally, we know that $k!$ is the number of ways to order k people. Hence it easily follows that the number of ways to first choose k elements, then order then, and the order the remaining $n - k$ elements is $\binom{n}{k}k!(n - k)!$

1.2.3

Both the value $n!$ and $\binom{n}{k}k!(n-k)!$ count the number of ways to order n elements, although they have a different approach to it. Hence we have the equality

$$n! = \binom{n}{k}k!(n-k)!$$

Dividing this by $k!(n-k)!$, we get the final result.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

1.2.4

$$\binom{n}{0} = 1 = \binom{n}{n}$$

These formulas do make sense. There is only one way to choose nothing out n, i.e. by choosing nothing. Similarly, there is only one way to choose everything, i.e. by choosing everything.

1.3

1.3.1

$\binom{n}{k}$ is the number of ways to choose k elements from a set of n. However, we can also count this in a different way. Let us fix a special element. Then there are two ways to choose k elements from n; either you choose the special element or you don't choose it.

If you do not choose the special element, then we have $\binom{n-1}{k}$ ways to choose k elements from the group without the special element. On the other hand, if we choose to have the special element, then we have to choose the remaining $k-1$ elements from a set of size $n-1$. This can be done in $\binom{n-1}{k-1}$ ways. So the number of ways to choose k elements from a set of size n is the sum of the previous two numbers.

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

1.3.2

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{(n-k-1)!k!} + \frac{(n-1)!}{(n-k)!(k-1)!} \\ = \frac{(n-k)(n-1)!}{(n-k)!k!} + \frac{k(n-1)!}{(n-k)!k!} &= \frac{n(n-1)! - k(n-1)! + k(n-1)!}{(n-k)!k!} \\ &= \frac{n!}{k!(n-k)!} = \binom{n}{k}\end{aligned}$$

1.4

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

This sum computes the number of all possible ways to choose a team of size k, for all values of k between 0 and n, out of a group of n people. We get the same number by doing a binary choice on every person whether or not they are in the team. So we have 2 choices n times, i.e. 2^n.

2 Additional Exercises

2.1

For the number to be odd, its last digit must be odd. Hence we have five choices for the final digit. For the number to be consider a 5-digit number, the first digit has to be non-zero. So it has at most 9 choices. The other digits have no other restrictions aside from being distinct.

Let us choose these two digits first and then the middle digits in any order. There are two choices, either the first digit is odd and thus it limits the choices of the final digit, or it is even and it does not limit the last digit. These two cases contain $5*8*7*6*4$ and $4*8*7*6*5$ numbers, respectively (each multiplier corresponds to the number of choices for the digit in the corresponding position. The final answer is the sum of these two (equal) numbers, i.e. $2*4*8*7*6*5 = 13440$

2.2

Since every zero must be followed by one, the number will have eight “01” blocks. We are left with two ones that can be placed to the sequence with the “01” blocks freely. These positions can be picked in $\binom{10}{2}$ ways. Thus, there are $\binom{10}{2} = 45$ such numbers

2.3

We have to choose 3 men and 3 women to the committee. The choices of men are independent of the choices of women. Thus the number of solutions is

$$\binom{10}{3}\binom{15}{3} = 54600$$

2.4

Binomial theorem:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

From this we see that the coefficient of $x^i y^j$ in the expansion of $(x+y)^n$ is $\binom{n}{i}$

2.4.1

$\binom{5}{2} = 10$

2.4.2

$\binom{17}{8} = 24310$

2.4.3

Substituting $x' = 2x$ and $y' = 3y$, we get

$$\binom{17}{8}(x')^8(y')^9 = \binom{17}{8}2^8 3^9 x^8 y^9.$$

Thus the coefficient is $\binom{17}{8}2^8 3^9 = 122494394880$

2.5

2.5.1

For a relation on a set of size n, there are n^2 possible elements (a, b) in a relation. There are n elements of the form (a, a). For any element (a, b) we have in the relation, we also must have (a, a) and (b, b). So the number of possible additional elements, outside of the (a, a) elements, in the relation is $n^2 - n$. Thus we get

$$2^{n^2-n} = 2^{n(n-1)}$$

2.5.2

For symmetric relations we need to choose the pairs (a, b) and (b, a) to be in the relation. We have n choices for elements of the form (a, a). For the others we have for other possible elements we have $n^2 - n$ choices, but since we choose those elements in pairs, we have $(n^2 - n)/2$ choices for those. Thus the final answer is

$$2^n 2^{(n^2-n)/2} = 2^{n(n+1)/2}$$

2.5.3

Again, the number of elements of the form (a, a) is n and we have a binary choice for them. For all other pairs (a, b) and (b, a), we have three options either one of the is in the relation or neither of them is. The number of such pairs is $n(n-1)/2$ and thus our final answer is

$$2^n 3^{n(n-1)/2}$$

2.6

We want to show that among 101 integers there is a pair whose difference is divisible by 100. Let the pidgeonholes be the equivalence classes of integers modulo 100. If any two integers land in the same equivalence class, their difference must be divisible by 100. Since we have 101 integers, by the pidgeonhole principle at least two of them have to be in the same pidgeonhole, i.e. there are two integers who have the same remainder when divided by 100. The difference of these two integers is divisible by 100.

2.7

In an $n \times m$ chess-board there are $n+1$ horizontal lines and $m+1$ vertical lines. A rectangle on chess-board is nothing but a space enclosed by two vertical and two horizontal lines, that is to say that counting rectangles is equivalent to counting the ways to choose two horizontal and two vertical lines. The number of ways to do so is $\binom{n+1}{2}$ for horizontal and $\binom{m+1}{2}$ for vertical lines. Since these choices are independent, the final answer is

$$\binom{n+1}{2}\binom{m+1}{2}$$

2.8

$$\sum_{k=0}^{n} k\binom{n}{k}^2 = n\binom{2n-1}{n-1}$$

We will present a combinatorial argument for this equality. Note that

$$\sum_{k=0}^{n} k\binom{n}{k}^2 = \sum_{k=0}^{n} k\binom{n}{k}\binom{n}{n-k}.$$

Suppose we have two groups of size n, for example a group of teachers and a group students. Now suppose we have to form a team of teachers and students of size n with a team leader who is a teacher. Say we choose k teachers, then we must have $n-k$ students. We have $\binom{n}{k}$ choices for the teachers, $\binom{n}{n-k}$ choices for the students, and k choices for the team leader from the chosen teachers. So for a given k, there are $k\binom{n}{k}\binom{n}{n-k}$ way to form the team. To get the number of all possible teams, we sum over k.

On the other hand, the team formation can be done differently. If we pool the groups together, we have a total of $2n$ people. For choosing the team leader, who has to be a teacher, we have n choices. Now we have to choose $n-1$ members, who can be either teachers or students, from $2n-1$ people. Hence we get that the number of ways to do this is, $n\binom{2n-1}{n-1}$. Thus the claimed equality follows.

Problem 9. Proof that there is no bijection $\mathbb{N} \to P(\mathbb{N})$

Suppose we can list all the subsets of $\mathbb{N}$:
$\{1, 5, 13, 2, 7, ...\}$
$\{6, 5, 3, 9, 45, ...\}$
$\{45, 3, 6, 9, 5, ...\}$
etc.

Now change the i:th element in each set in any way. Now, the set consisting of all the changed elements cannot be in the original set $P(\mathbb{N})$, which creates a contradiction. Thus, $|\mathbb{N}| \neq |P(\mathbb{N})|$ and there cannot be a bijection.

EXERCISE SET 3,
MS-A0402, FOUNDATIONS OF DISCRETE MATHEMATICS

Homework solutions

Problem 1. Let P be the set of all Finland's presidents, and let G be the set of all ordered pairs $(a, b) \in P \times P$ such that the president b succeeded president a in office. Is G the graph of a function? Explain your answer.

The graph of a function $f : X \to Y$ is defined as

$$G(f) = \{(x, f(x)) : x \in X\}$$

Now let $p_{Niinistö} \in P$ be the current president of Finland. As there is no pair $(p_{Niinistö}, p) \in P \times P$, we see that G cannot be a graph of a function from P to $P \times P$. However, it is a graph of a function from $(P \setminus \{p_{Niinistö}\})$ to $P \times P$ because then all required ordered pairs exist in G. Also notice that the function only maps each president to one pair $(a, b) \in P \times P$, which is a requirement of a function.

Problem 2. Find the domain and range of the function which assigns to each non-negative integer its last digit.

Domain (where the function maps from): Non-negative integers ($\mathbb{Z}_{\geq 0}$)
Range (where the function maps to): All possible last digits of an integer i.e. $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Problem 3. Eight people are to be seated around a table; the chairs don't matter, only who is next to whom, but right and left are different. Two people, X and Y, cannot be seated next to each other. How many seating arrangements are possible?

First, we can place X to any position in the table. As the chairs do not matter, placing X to any chair is considered equivalent. Thus, there is 1 way to do so. Then, we can place Y to any of the remaining seats that is not next to X. We have 8-3=5 possibilities to do so. After that, the rest of the people can be positioned in the remaining 6 seats, giving 6! possible arrangements. Now the total number of arrangements is $5 \cdot 6! = 3600$.

Problem 4. Prove that for all $n \in \mathbb{N}$, $n \geq 9$, the following statement is true: for all $k \in \mathbb{N}$ with $0 \leq k \leq n$ we have

$$\binom{n}{k} < 2^{n-2}.$$

Proof by induction:

1. Base case ($n = 9$)

$$\binom{9}{k} \leq \max \binom{9}{k} = 126 < 128 = 2^{9-2}$$

2. Induction assumption:

Assume that the statement holds for all $k \in \mathbb{N}$ with $0 \leq k \leq n$ when $n = m - 1$ i.e.

$$\binom{m-1}{k} < 2^{m-1-2}$$

3. Proof that the statement also holds for for all $k \in \mathbb{N}$ with $0 \leq k \leq n$ when $n = m$

First, notice that

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Then, by the induction assumption

$$\binom{n-1}{k} < 2^{m-1-2} \text{ and } \binom{n-1}{k-1} < 2^{m-1-2}$$

Thus,

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} < 2 \cdot 2^{m-1-2} = 2^{m-2}$$

Ex4

Perttu Saarela

March 2021

1 Explorative exercises

1.1

There exists m^n functions from $\{1, \ldots, n\}$ to $\{1, \ldots, m\}$ because for each of the n elements we have m choices of where it can be mapped.

1.1.1

For an injective function to exist, we must have that $n \leq m$. When we construct the function, we have m choices for the first element, $m - 1$ for the second, and so on until for the final element we have $m - n + 1$ choices. Hence the number of injective functions is $\frac{m!}{(m-n)!}$.

1.1.2

For a function to be non-surjective, it has to "miss" some element of $\{1, 2\}$. Since there are only two elements, we have only two such functions, one where everything is mapped to 1, and another where everything is mapped to 2.

1.1.3

The number of functions where the function "misses" $i \in \{1, 2, 3\}$ is 2^n for each i. Summing these up we get $3 \cdot 2^n$. However, this sum double counts all of the functions that map all elements to one element. Hence the final answer is $3 \cdot (2^n - 1)$.

1.2

We can consider the original set to be an increasing ordering and the map (the permutation) as giving the set a new total order by the value they are assigned to.

1.3

1.3.1

The permutation $(\sigma(1), \ldots, \sigma(9)) = (2, 7, 5, 6, 9, 3, 8, 4, 1)$ gives the cycle of length 9:

$$1 \to 2 \to 7 \to 8 \to 4 \to 6 \to 3 \to 5 \to 9 \to 1$$

1.3.2

Yes, bijectivity ensures this. Cycles of length one are also cycles.

2 Additional exercises

2.1

There are 26! permutations for the 26 letters. To find the number of permutations which do not contain the words "cats", "snow" or "walk", let us first find the number of permutations which do contain them and then substract that number from 26!.

First, count the number of permutations containing one of the words. We can consider that word to be a solid block and represent it with a new symbol, say π. If the set of letters is Σ, then we now have to count the permutations of $(\Sigma \setminus \{"c","a","t","s"\}) \cup \pi$. That number is 23!.

Let A_1, A_2, A_3 be the sets of permutations containing all permutations which have the word "cats", "snow" and "walk", respectively. Since all words are of length four, we have that $|A_i| = 23!$

For $A_1 \cap A_2$, we only have to consider the block "catsnow". And thus by the previous arguments $|A_1 \cap A_2| = 20!$. The same also holds for $A_2 \cap A_3$, where we consider the block "snowalk", so $|A_2 \cap A_3| = 20!$. The words "cats" and "walk" both contain the letter 'a' in the middle of the word and thus cannot occur at the same time. Hence $|A_1 \cap A_3| = |A_1 \cap A_2 \cap A_3| = \emptyset$. Let Σ^* be the set of all permutations of Σ. By the inclusion-exclusion principle, we get
$|\Sigma^*| - |A_1 \cup A_2 \cup A_3| = |\Sigma^*| - (|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3|) = 26! - 3 \cdot 23! + 2 \cdot 20!$

2.2

2.2.1

Let's say we first had the pairs $(ab), (cd), (ef)$. Now let's re-assign the pairs, starting with choosing a pair for a. There are 4 choices for a. If a was to be paired with c, then b couldn't be paired with d, since that would leave the pair (ef) untouched. Hence there are 2 choices for b. After this choice there is only one pair left. Thus the answer is $4 \cdot 2 = 8$.

2.2.2

Let us take it as a given that the number of ways to divide a group of $2n$ people into pairs is $f(2n) = \frac{(2n)!}{n!2^n}$. (This can be shown easily).

Now let $A = \{a_1, a_2, \ldots, a_n\}$ be the original set of pairs and let A_i be the set of pairs where the pair a_i is kept the same. It follows that $|A_i| = f(2n-2)$. To get the number of ways to form new pairs without anyone having the same partner, we substract $|A_1 \cup A_2 \cup \cdots \cup A_n|$ from the total number of pairs $f(2n)$.

By the inclusion-exclusion principle

$$|A_1 \cup \cdots \cup A_n| = \sum_{i=0}^{n} |A_i| - \sum_{i \neq j} |A_i \cap A_j| + \cdots - |A_1 \cap A_2 \cap \cdots \cap A_n|$$

The number $|A_i \cap A_j|$ represent the number of pairings where there are the pairs a_i ja a_j. So we find that $|A_i \cap A_j| = f(2n-4)$. The sum over all of these terms is equal to $\binom{n}{2} f(2n-4)$. Same argument can be repeated for k fixed pairs, i.e. $\binom{n}{k} f(2n-2k)$ is the number of pairings where some k pairs are fixed. The final answer becomes

$$f(2n) - |A_1 \cup \cdots \cup A_n| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(2n-2k)$$

2.3

2.3.1

Product of disjoint cycles:

$$(1362)(2564)(2345) = (13)(5)(264)$$

2.3.2

Two line notation:

$$(1362)(2564)(2345) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 2 & 5 & 4 \end{pmatrix}$$

2.3.3

Product of transpositions:

$$(1362)(2564)(2345) = (13)(24)(26)$$

2.4

Let $\rho = (123)$ and $\pi = (12)$ in S_3

2.4.1

We see that π^2 is clearly the identity. For ρ^3 we have

$$(123)^3 = (123)(123)^2 = (123)(132) = \iota$$

2.4.2

$S_3 = \{\iota, (12), (13), (23), (123), (132)\}$. We find that

π	(12)
ρ	(123)
ρ^2	(132)
$\pi\rho$	(23)
$\pi\rho^2$	(13)

2.5

2.5.1

$\rho = (abdc)(efhg), \ \ \sigma = (acge)(bdhf), \ \ \tau = (abfe)(cdhg)$

2.5.2

$\rho\sigma = (bce)(dgf), \ \ \sigma\tau = (che)(dfa), \ \ \tau\rho = (fga)(hcb)$

2.5.3. These permutations that can be written as products of ρ, σ, τ preserve the orientation of the cube (i.e. which sides are next to each other). The number of them is equal to the number of ways in which a cube can be rotated. To count them, let's enumerate the six faces of the cube with numbers $1-6$. To select the face that points upwards, we have 6 choices. Then, we have 4 choices for the face that points forward. The rest of the faces are forced to preserve the orientation of the cube. Thus, there are $6 \cdot 4 = 24$ ways to rotate a cube. All of these rotations can be written as products of ρ, σ, τ

2.5.4. Now, we only need to preserve the distances between the corners. To see how many options we have now, let's enumerate the eight corners. For the first corner (e.g. front-up-left), we have 8 choices. Then for the next (e.g. front-up-right), we have 3 choices (all of the corners next to the first one). Then, for the third corner (e.g. front-down-left), we have 2 choices (all of the corners next to the first one still left). The rest of the corners are forced. Thus, we have in total $8 \cdot 3 \cdot 2 = 48$ symmetries. Half of these cannot be written as products of ρ, σ, τ. These flip the cube inside out. One example is the permutation $(gc)(hd)(fb)(ea)$

2.6

Let $|A \cap B| = |A \cap C| = |B \cap C| = m$. Note that $A \cap B \cap C = \emptyset \ \Rightarrow \ |A \cap B \cap C| = 0$. From the inclusion-exclusion principle it follows that

$$\begin{aligned}
|A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\
2n &= 3n - 3m \\
n &= 3m
\end{aligned}$$

Thus these condition can only be true when n is divisible by 3.

2.7

2.7.1

See Figure 1 for the set up. Let's start by pairing a. It has three choices. If a is paired with c or e, it leads to only one possible pairing. Since if a chooses c, the only valid choice for b is e. Same holds, if a chooses e. So that's two possible pairings. If a is paired with d, then b has two choices. Thus the number of pairings is 4.

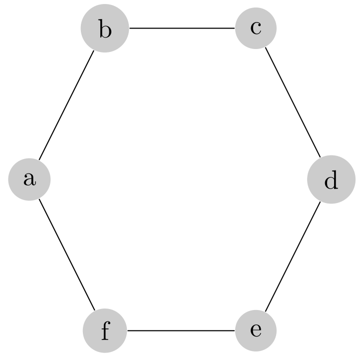


Figure 1: Visualisation of the problem

2.7.2

The answer is

$$\sum_{k=0}^{n}(-1)^k P(n,k)(2n-2k-1)!!,$$

where $P(n,k) = \binom{2n-k}{k} + \binom{2n-k-1}{k-1}$ and $(2n-2k-1)!! = 1 \cdot 3 \cdot 5 \cdots (2n-2k-1)$. The equation comes from the inclusion-exclusion principle. Here $P(n,k)$ is the number of ways to choose k pairs of adjacent people in the circle. The multiplier $(2n-2k-1)!!$ is the number of ways to pair up the rest of the people.

2.7.3

Overlapping pairs make this problem more difficult and the coefficient more complicated.

2.8

For any element $a \in A$ or any element $b \in B$, let us consider the chain

$$\cdots \to f^{-1}(g^{-1}(a)) \to g^{-1}(a) \to a \to f(a) \to g(f(a)) \to \cdots$$

This chain may terminate to the left if the inverse function does not exist. By injectivity of both f and g, every element has exactly one such chain. Therefore, if an element occurs in the the chain, the chains for these two elements are the same. Thus we have a partition for the set $A \cup B$. Hence it suffices to construct separate bijections for these partitions. If a sequence stops at an element in A, then f is a bijection for it. Similarly, if a sequence stops at an element of B, then g is the bijection. Finally, if the sequence never stops, either one of f or g will work as a bijection.

This is known as the Schröder-Bernstein Theorem.

EXERCISE SET 4,
MS-A0402, FOUNDATIONS OF DISCRETE MATHEMATICS

Homework solutions

Problem 1. How many integers from 1 to 60 are multiples of 2 or 3 but not both?

There are $\lfloor \frac{60}{2} \rfloor = 30$ numbers that are divisible by two.
There are $\lfloor \frac{60}{3} \rfloor = 20$ numbers that are divisible by three.
There are $\lfloor \frac{60}{2\cdot 3} \rfloor = \lfloor \frac{60}{6} \rfloor = 10$ numbers that are divisible by both two and three.
As the numbers divisible by six are also divisible by both two and three, the total number of integers between 1 to 60 that are multiples of 2 or 3 but not both is $30 - 10 + 20 - 10 = 30$

Problem 2. Consider the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 7 & 3 & 6 & 4 & 2 & 1 & 5 & 8 \end{pmatrix}$$

a) Write it as a product of disjoint cycles.

The first cycle can be obtained from: $\pi(1) = 9$, $\pi(9) = 8$, $\pi(8) = 5$, $\pi(5) = 4$, $\pi(4) = 6$, $\pi(6) = 2$, $\pi(2) = 7$, $\pi(7) = 1$. It is (1985462). The only other cycle is (3) because $\pi(3) = 3$. Thus, $\pi = (1985462)(3)$.

b) Write it as a product of transpositions.

Transpositions are cycles of length 2 (e.g. (ab)). Transpositions can be obtained in many ways, for example using $(a_1a_2...a_k) = (a_1a_k)(a_1a_{k-1})...(a_1a_2)$. Thus, one example is $\pi = (12)(16)(14)(15)(18)(19)$

Problem 3. In how many ways can we rearrange the letters in the word "knackered"

a) with no restrictions?

There are nine letters that can be arranged in 9! ways. However, as there are two k:s and two e:s, we need to eliminate the duplicates. As there are 2! ways to order the k:s and 2! ways to order the e:s, we get $\frac{9!}{2!2!} = 90720$ unique rearrangements.

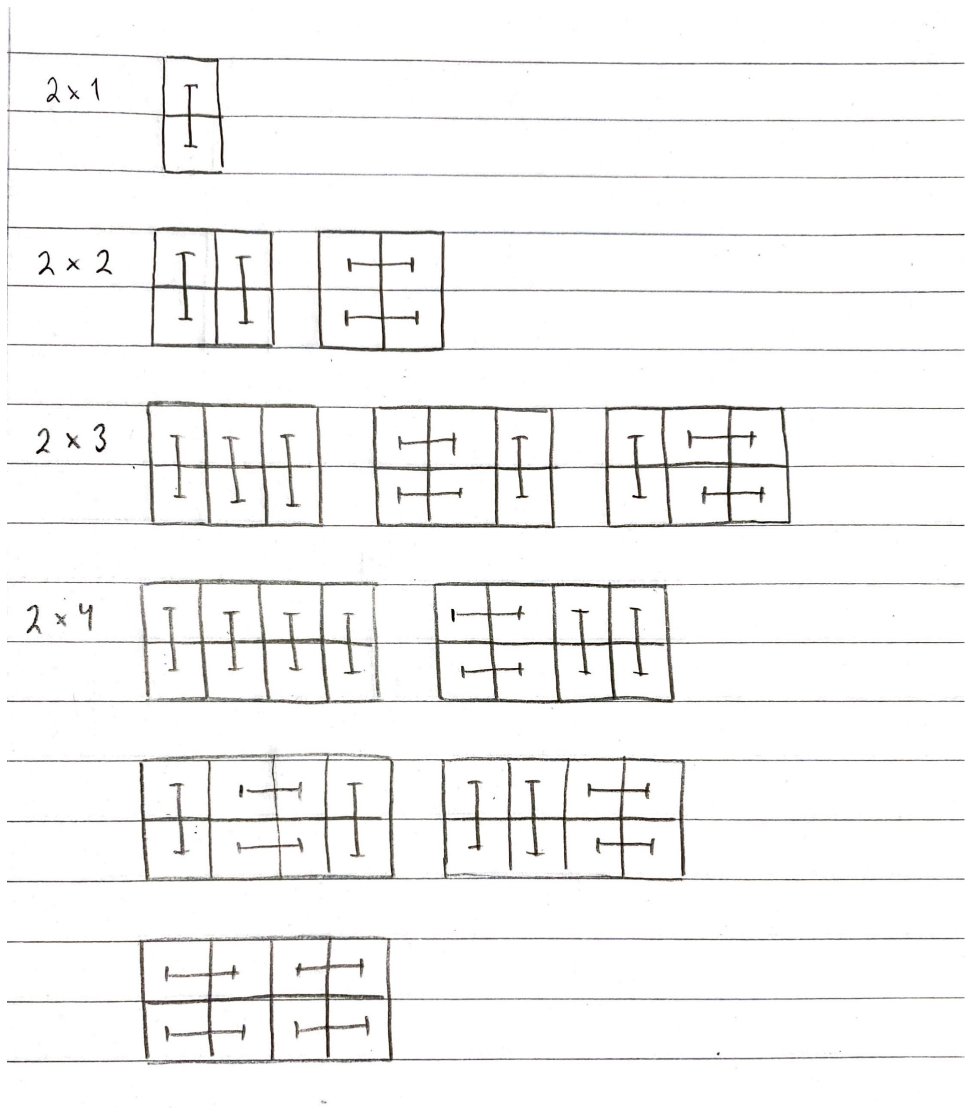
Another way to approach this problem is to first choose two positions for k:s, which can be done in $\binom{9}{2}$ ways. Then choosing two positions for e:s, which can be done in $\binom{7}{2}$ ways. Last, the rest of the digits can be rearranged in 5! ways. This gives the same result as above $\binom{9}{2}\binom{7}{2}5! = 90720$

b) if the first and last letter must be vowels?

First, there are three possibilities for the first letter. Then there are two possibilities for the last letter. The rest of the letters can be arranged freely in 7! ways. To eliminate the duplicates, we must again divide the possible number of arrangements by 2!2!. This gives a total of $\frac{3 \cdot 2 \cdot 7!}{2!2!} = 7560$ rearrangements.

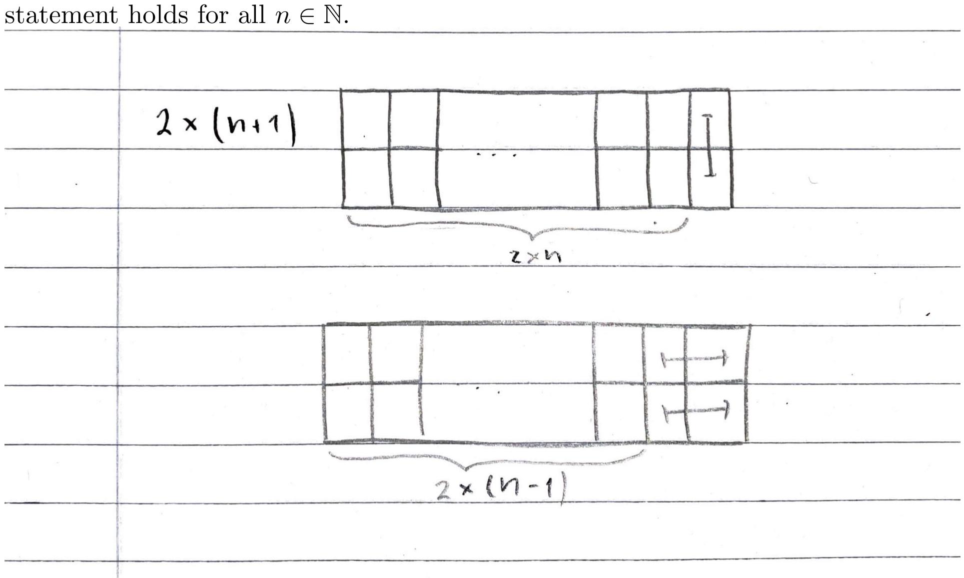
Problem 4. How many ways are there to tile dominos (with size 2×1) on a grid of size $2 \times n$?

Experimenting with small values of n:



Denoting the number of tilings on a $2 \times n$ grid by $T(n)$. We notice that it looks like $T(n) = T(n-1) + T(n-2)$ (also known as Fibonacci sequence). This relationship can be proven by induction.

(1) Base case shown above
(2) Assume that the statement holds for arbitrary $n = k$
(3) We see that tiling of $2 \times (n+1)$ grid can be obtained in two ways; either by adding a vertical domino to any tiling of size $2 \times n$ grid or by adding two horizontal dominos to any tiling of size $2 \times (n-1)$ grid. It follows that the statement holds for all $n \in \mathbb{N}$.



Using this formula we get 10946 tilings on a 2×20 grid.

Discrete Mathematics

Exercise sheet 5

Jouni Tammenmaa

March 2021

Explorative exercises

Problem 1.

A graph G = (V, E) is a set of nodes V together with a set of edges E. Therefore we can represent the given graphs G and H as the following.

$G = (V_G, E_G) = (\{u1, u2, u3, u4), \{(u1, u2), (u1, u3), (u3, u4), (u2, u4)\})$

$H = (V_H, E_H) = (\{v1, v2, v3, v4),\{(v1, v4), (v1, v3), (v3, v2), (v4, v2)\})$

These two graphs are isomorphic given there exists a bijection $\phi : V_G \rightarrow V_H$ such that there is an edge between u_i and u_j if and only if there is an edge between $\phi(u_i)$ and $\phi(u_j)$.

Now it can be intuitively seen that the given graphs are the same, with v_4 corresponding to u_2 and v_2 corresponding to u_4, hence let us construct a the bijection: $\phi = \{(u_1, v_1), (u_2, v_4), (u_3, v_3), (u_4, v_2)\}$.

Now lets write H in terms of this bijection.

$H = (V_H, E_H) = (\{\phi (u1), \phi(u4), \phi (u3), \phi(u2)\},\{(\phi (u1), \phi (u2)), (\phi(u1), \phi(u3)), (\phi(u3), \phi(u4)), (\phi(u2), \phi(u4))\})$

Now it can clearly be seen that there is an edge between u_i and u_j if and only if there is an edge between $\phi(u_i)$ and $\phi(u_j)$, and hence the graphs are isomorphic.

Problem 2.

All the graphs have 6 vertices, and 9 edges, with each vertice being associated with 3 edges, and hence we can not use those details to dismiss the possibility of isomorphism, but let us consider the shape of the graphs, or rather the cycles in the graphs.

The graph a) has cycles of length 3, for example (1, 2, 3) and (4, 5, 6). So too does graph c), for example (1, 2, 3) and (6, 4, 5). However no cycle of size 3 can be found in b), hence it is clear that b) is not isomorphic to a) and c).

A = ({1, 2, 3, 4, 5, 6}, {(1, 2), (1, 4), (1, 3), (2, 3), (2, 5), (3, 6), (4, 5), (4, 6), (5, 6)}

C = ({C1, C2, C3, C4, C5, C6}, {(C1, C2), (C1, C3), (C1, C6), (C2, C3), (C2, C5), (C3, C4), (C4, C5), (C4, C6), (C5, C6)}

Now let us have a bijection $\phi = \{(1, C1), (2, C2), (3, C3), (4, C6), (5, C5), (6, C4)\}$

Then C can be written as

$C = (\{\phi(1), \phi(2), \phi(3), \phi(6), \phi(5), \phi(4)\}, \{(\phi(1), \phi(2)), (\phi(1), \phi(3)), (\phi(1), \phi(4)), (\phi(2), \phi(3)), (\phi(2), \phi(5)), (\phi(3), \phi(6)), (\phi(6), \phi(5)), (\phi(6), \phi(4)), (\phi(5), \phi(4))\}$

From which it can be seen that **a) and c) are isomorphic.**

Problem 3

a)

if n = 1 clearly there are 0 edges.

If n = 2 clearly there is 1 edge.

Since it is true for some n lets assume it true for n, that is lets assume a tree with n vertices has n-1 edges.

Now lets prove it for n + 1:

Let there be a tree A of n vertices (and hence n – 1 edges). Let there also be another tree B with 1 vertices (and hence 0 edges). Now let there be drawn an edge between any one vertice in A and the sole vertice in B. The graph created is now connected and acyclic, since A and B are acyclic, and there is only one path from A to B, and hence no cycle is possible. Hence the new graph is a tree, and the number of vertices is $|A| + |B| = n + 1$, and the number of edges is the sum of the edges in A and B and the single edge we created. Hence it is

$n-1 + 0 + 1 = n = (n + 1) - 1$

One can not add another edge from a vertice of A to the sole vertice of B without creating a

cycle, since if another one were to be added then there would be 2 distinct paths to the vertice of B and since A is a tree there must be a path from the vertices which connect to B to each other, and hence a cycle would exist.

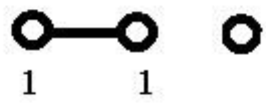
And hence by induction a tree of n vertices has exactly n – 1 edges.

b)

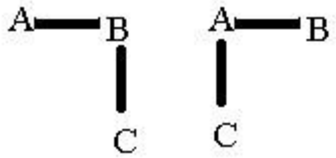
Let the degree of a vertice be the number of edges associated with the vertice. Now any configuration of a tree is isomorphic to another, if:

For each vertice of degree n in A with the neighbors of degrees $\{m1, ..., m_n\}$ there is a vertice of degree n in B with neighbors of degrees $\{m1, ..., m_n\}$

since by mapping the vertices of the same degree with the same neighbors to each other we can create a bijection such that there is an edge between u_i and u_j if and only if there is an edge between $\phi(u_i)$ and $\phi(u_j)$. Now let there be a tree of 2 vertices. Clearly any such tree only has vertices of degree 1



Now we have 2 choices, and regardless of which one of the 2 vertices we connect the third vertice to, we get a tree with 1 vertice of degree 2, and 2 of degree 1.



The first graph can be represented

A = ({A, B, C}, {(A, B), (C, B)} And the second

B = ({A, B, C}, {(C, A), (B, A)}

Now let ϕ = {(B, A), (A, C), (C, B)}

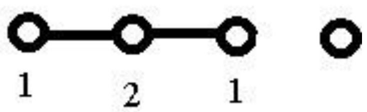
Now the edges of B can be represented as

{(ϕ(A), ϕ(B)), (ϕ(C), ϕ(B))}

And hence it is clear that the trees are isomorphic, and that all trees of 3 vertices are isomorphic.

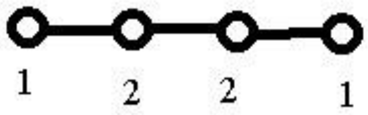
c)

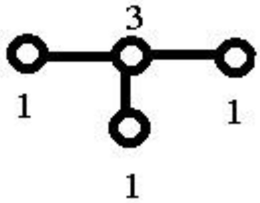
Let there be a tree of 3 vertices. There is only 1 such tree as all trees of 3 vertices are isomorphic as shown in part b)



Now we have 3 choices of where to connect the fourth vertice.

If we were to connect the fourth vertice to either of the vertices of degree 1, we would get a tree with 2 vertices of degree one, and 2 of degree 2, with each vertice of degree 1 having a neighbor of degree 2, and each vertice of degree 2 having a neighbor of degree 1 and 2, and hence choosing either of them would result in a tree that is isomorphic to the tree produced by the other choice. If however we connect it to the vertice of degree 2 we get a tree that has 3 vertices of degree 1, and 1 vertice of degree 3. Hence there are only 2 non-isomorphic trees of 4 vertices.

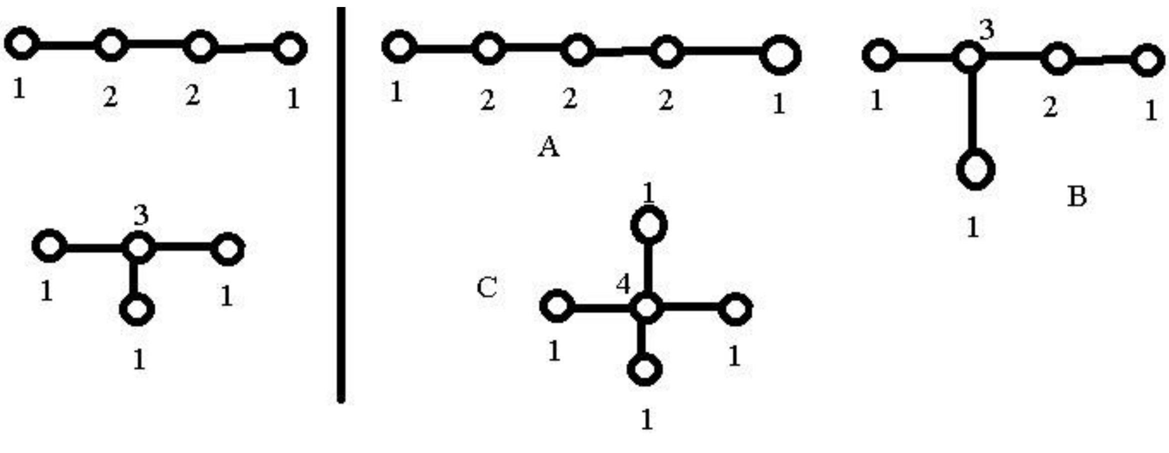




d)

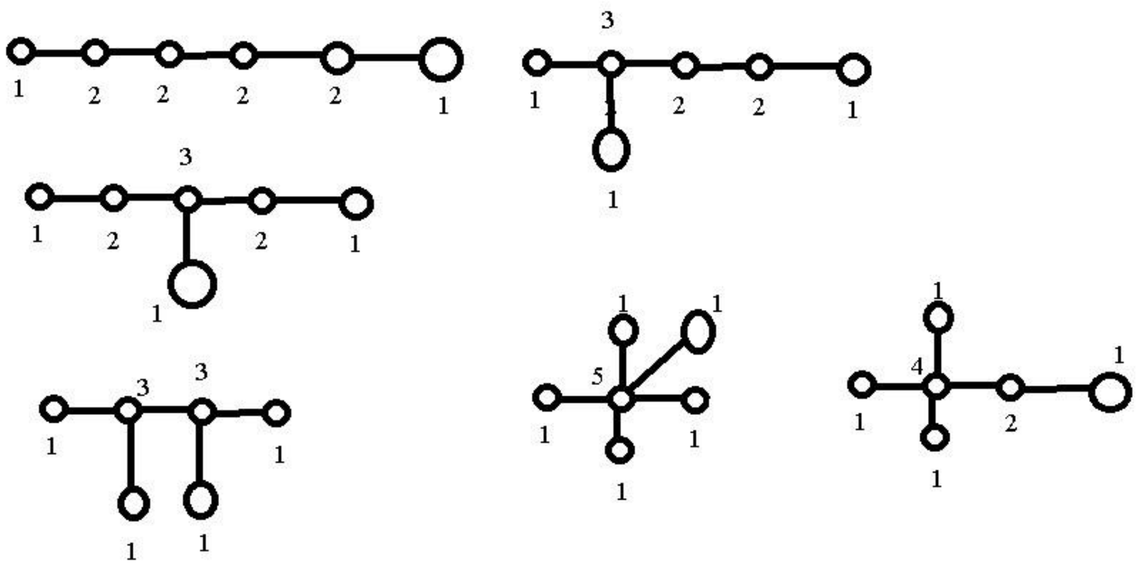
Given the 2 possible non-isomorphic trees of 4 vertices we get the following choices of where to attach the 5th vertice: Either we pick the first non-isomorphic tree of 4 vertices in which case we can either attach it to a vertice of degree 1 resulting in A below, or of degree 2, resulting in B. The choice of which vertice of degree 2 or 1 we attach it to does not matter due to symmetry.

Or we pick the second 4 vertice non-isomorphic tree, and get 2 choices, either attach to the vertice of degree 3, giving us C, or attach to one of the vertices of degree 1, giving us a tree with 1 vertice of degree 3 with neighbors of degrees {1, 1, 2}, 1 of degree 2 with neighbors of degrees {3, 1}, and 3 of degree 1, 2 of which have a neighbor of degree 3, and 1 which has a neighbor of degree 2, which would be isomorphic to B. Hence A, B and C are the only nonisomorphic trees of degree 5.



e)

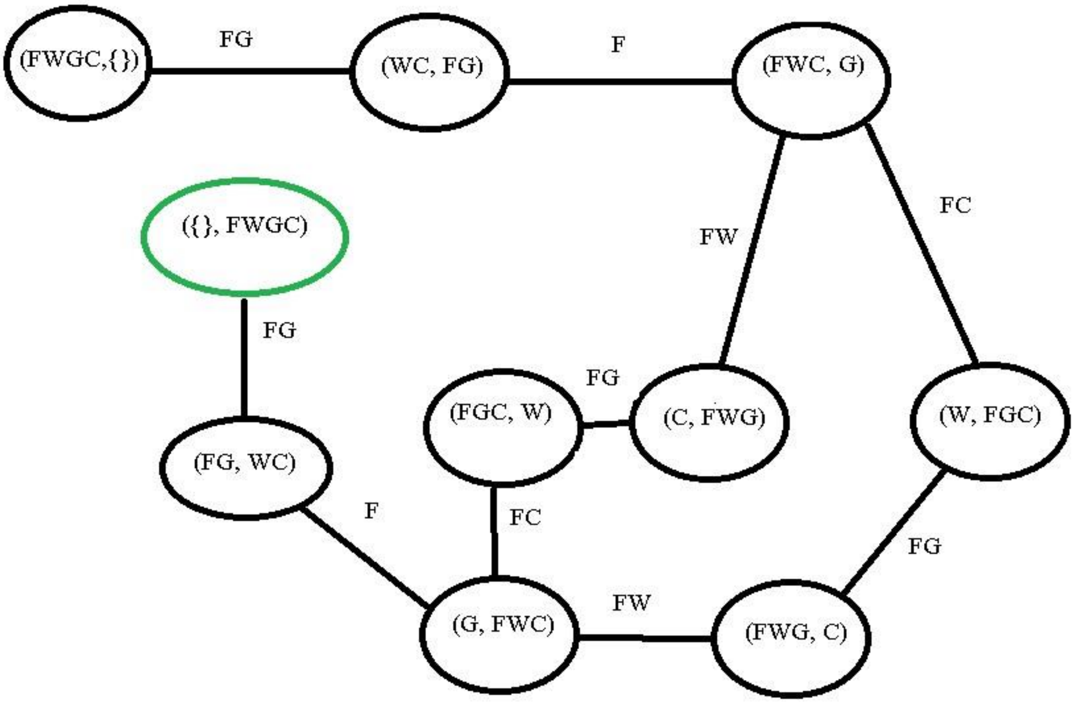
Following the same principles as in the previous parts the only possible non-isomorphic trees of degree 6 are the following:



Additional exercises

Problem 1

a) and b)



c)

The edges of the graph correspond to possible moves, and hence if we can find a path from the start to the goal we can extract from the edges on the path the steps to solve the puzzle.

d)

FG -> F -> FW -> FG -> FC -> F -> FG

And

FG -> F -> FC -> FG -> FW -> F -> FG

Problem 2

We can construct all such permutations by first choosing which corner 1 map to which gives us 4 choices, and then choosing which corner 2 will map to, which gives us 2 choices since 2 must be a neighbor of 1, after which 4 and 3 are locked in place, as 4 must be the remaining neighbor of 1, and 3 must then take the last available corner.

Hence there are 4 * 2 * 1 * 1 = 8 possible permutations in

D_4. **b)**

Let us prove it by writing out all the possible permutations as products of ρ and π.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = p^4 = p^0 = I = \begin{matrix} 4 & 3 \\ 1 & 2 \end{matrix} = \pi^2$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = p = \begin{matrix} 3 & 2 \\ 4 & 1 \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = p^2 = \begin{matrix} 2 & 1 \\ 3 & 4 \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = p^3 = \begin{matrix} 1 & 4 \\ 2 & 3 \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \pi = \begin{matrix} 4 & 1 \\ 3 & 2 \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = p\pi = \begin{matrix} 1 & 2 \\ 4 & 3 \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = p^2\pi = \begin{matrix} 2 & 3 \\ 1 & 4 \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = p^3\pi = \begin{matrix} 3 & 4 \\ 2 & 1 \end{matrix}$$

Problem 3

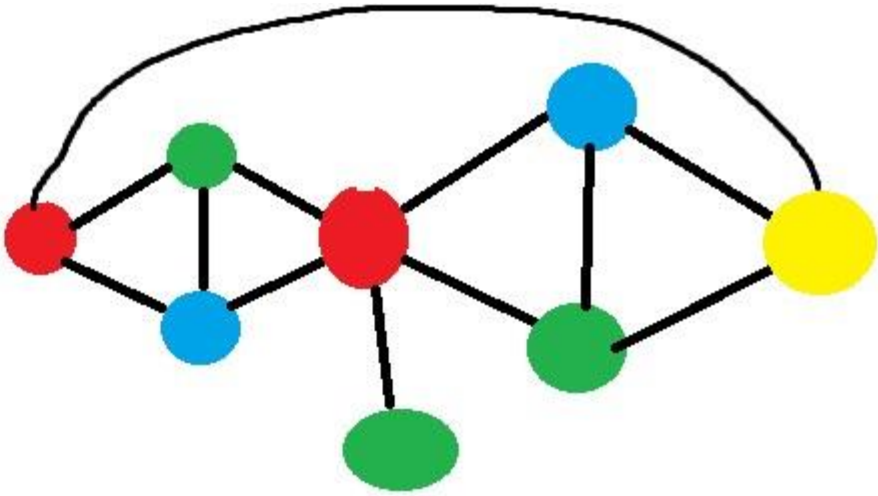
The shortest path from a to z is the following sequence:

a -> c -> d -> e -> g -> z

Problem 4

Chromatic number is the least amount of distinct colours required to color a graph so that no adjacent vertices have the same color.

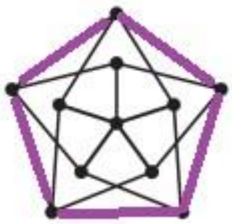
A clique is a complete subgraph of a graph, that is a subgraph where each vertice has an edge to each other vertice.



Here the chromatic number is 4, the largest clique is 3 and the largest degree is 5. 3 < 4 < 5.

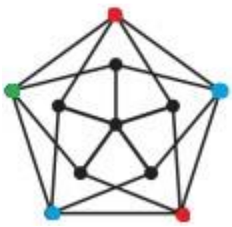
Problem 5

Let χ denote the chromatic number of the graph.

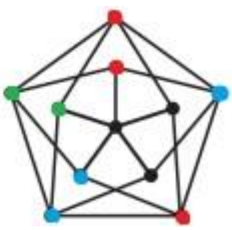


Clearly there is an odd length cycle in the graph, and hence χ ≥ 3 since colors in a cycle must alternate, but alternating colors in an odd length cycle will result in the first and last vertice to be colored to have the same color despite being adjacent, and hence coloring any odd length cycle requires atleast 3 colors.

Let us color the outlined cycle with the minimum 3 colors.



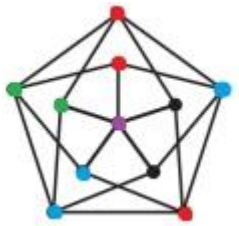
Now observer that using 3 colors this fixes the colors of the following vertices.



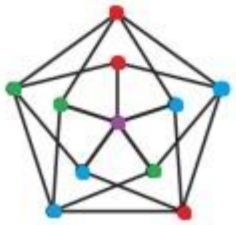
The red one must be red since it is adjacent to a blue and a green vertice, and similarly the green one must be green and the blue one must be blue.

Due to symmetry regardless of how we color the outside cycle 3 of the vertices in the middle will be fixed to different colors.

Now observe that the purple vertice can not be one of the three colors chosen, as it will always be adjacent to each of those colors. Hence $\chi \geq 4$.



Here is a coloring of the graph with 4 colors.



Since such a coloring is possible $4 \geq \chi$ and hence $4 \geq \chi \geq 4$

Hence the chromatic number is 4.

Problem 6

Since there are 5 total couples there are 10 total people. Since each person does not shake his own hand, nor their spouses, each person shakes from 0 to 8 hands. Since all 9 answers were different the answers must be 0, 1, ..., 8. It must be that the person who shook 0 hands is married to the person who shook 8 hands, since the person who shook 8 hands shook hands with everyone but themselves and their spouse, since there were 10 people total, and hence none of the other people could be the one who shook no hands, since everyone else has at least shook the hand of the person who shook 8 hands. Hence he shook hands with the people who answered 1, 2, 3, 4, 5, 6 and 7 and Mr X.

If we then consider the people who shook 1 to 7 hands we observe the person who shook 1 hand must have shook the hand of the person who shook 8 hands, and hence did not shake the hand of the person who shook 7 hands. Now since the person who shook 7 hands shook the hand of the person who shook 8 hands there are 6 handshakes unaccounted for. He cant have shook the people who shook 0 or 1 hands, and hence he must have shook the hands of the people who shook 2, 3, 4, 5, and 6 hands. That leaves 1 unaccounted handshake, which means he must have shook hands with Mr X. It also follows 1 must be 7s spouse, since otherwise 7 would not be able to shake all the other hands, as the alternative is one of those is 7s spouse.

Similarly it must be that 2 is 6's spouse and that 6 also shook Mr. X's hand. And that 3 is 5's spouse and 5 too shook Mr. X's hand. The only person left without a spouse is 4, which means 4 must be professor X, since only professor X's spouse is not in the group of people who answered, since Mr X was the one asking. Since nobody shakes their spouses hand it follows that Mr X shook 4 hands in total, those being the hands of 8, 7, 6, and 5.

Therefore the answer is Mr X shook 4 hands.

Problem 7

a)

Lets assume the converse is true for some party, that no 2 people know the same number of guests.

Then each of the **n** guests must know a distinct number of guests between 0 and **n - 1**. (or 1 to n if we assume each person to know themselves)

Since there are n guests and n distinct numbers to choose from, it must be that for each x $\in[0, \text{n-1}]$ there must be a guest that knows exactly x guests. However the guest that knows n-1 guests must know every single other guest at the party, and hence they must also know the person who knows 0 guests, and since we are assuming the knowing relation to be symmetric it must be then that the person who knows 0 must also know the person who knows n-1, but this leads to a contradiction since the person who knows 0 people cant know anyone.

Hence it must be that at least 2 people know the same number of guests, and the statement is true.

b)

Then each of the **n** guests must know a distinct number of guests between 0 and **n - 1**. (or 1 to n if we assume each person to know themselves)

Now it is possible to ennumerate each guest with a distinct number of known guests, since there are n guests and n distinct numbers of guests that each guest can know.

For example let there be a party with the guests {a, b, c}. Since the knowing relation is not symmetric we can then define it as the following:

R = {(a, b), (a, c), (b, c)}

Now 2 knows 2 people: b and c, b knows 1 person: c and c knows 0 people. Hence there exists a party where no 2 people know the same number of guests, and hence the statement is false.

EXERCISE SET 5 SOLUTIONS,
MS-A0402, FOUNDATIONS OF DISCRETE MATHEMATICS

Homework

The written solutions to the homework problems should be handed in on MyCourses by Monday 4.4., 12:00. You are allowed and encouraged to discuss the exercises with your fellow students, but everyone should write down their own solutions.

Problem 1. (10pts) Consider the permutations

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \text{ and } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}.$$

Are they conjugates? If so, find a permutation τ such that $\tau\rho\tau^{-1} = \sigma$.

Solution 1. We note that $\rho = (132)(45)$ and $\sigma = (1)(2543)$. The permutation ρ is composed of a 3-cycle and a 2-cycle and the permutation σ is composed of a 1-cycle and a 4-cycle. For two conjugate permutations, the permutations must have the same amount of cycles and for each cycle of a certain length in one of the permutations there should exist a cycle of an equal length in the other permutation. This is clearly not the case for the two given permutations and hence they are not conjugates.

Problem 2. (10pts) The **perfect riffle shuffle** (or "*Faro shuffle*") of a deck consisting of $2n$ cards (for a fixed $n \in \mathbb{N}$) is a permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 2n-1 & 2n \\ 1 & n+1 & 2 & n+2 & \dots & n & 2n \end{pmatrix} \in S_{2n}$$

that splits a deck of $2n$ cards into two piles and interleaves them (i.e. card in position 1 goes to position 1, card in position 2 goes to position $n+1$, card in position 3 goes to position 3, card in position 4 goes to position $n+2$, etc.). This is also called an out-shuffle, because it leaves the top card at the top and bottom card at the bottom. Thus we can write a formula:

$$\sigma(k) = \begin{cases} \frac{k+1}{2}, & k \text{ is odd} \\ n + \frac{k}{2}, & k \text{ is even} \end{cases}$$

Let $n = 3$, that is, we have a deck of 6 cards. Find the number of perfect riffle shuffles needed to return the deck to its original state. In order words, find some $N \in \mathbb{N}$ such that

$$\sigma^N = \underbrace{\sigma\sigma\sigma\dots\sigma\sigma}_{N \text{ times}} = e,$$

where $e \in S_{2n}$ is the identity permutation $e(i) = i$ for all $i \in \{1, 2, \dots, 2n\}$.

Hint: for a deck of 52 cards, that is, when $n = 26$, *this can be done with* 8 *shuffles, that is,* $\sigma^8 = e$ *(proof:* `https://www.youtube.com/watch?v=7lNk7bfkFq8` *), so it probably is less than* 8 *here with just 6 cards.*

Solution 2. When $n = 3$, $\sigma \in S_6$. Using the given formula we get $\sigma(1) = 1$, $\sigma(2) = 4$, $\sigma(3) = 2$, $\sigma(4) = 5$, $\sigma(5) = 3$, $\sigma(6) = 6$. Hence in cycle notation we have $\sigma = (2453)$. We then look for the order (N such that $\sigma^N = e$) of this σ. For any cycle, the order corresponds to the length of the cycle. Hence $N = 4$.

Problem 3. (10pts) The following figure shows two graphs with eleven vertices. The graph on the left has $V = \{0, 1, 2, \ldots, 10\}$, whereas the one on the right has nodes $V' = \{a, b, \ldots, k\}$. Are they isomorphic?

Solution 3. Let us consider the degrees of the vertices in each graph. The (vertex, degree) pairs of V are:

$$V \times D_V = \{(0,5),(1,4),(2,4),(3,4),(4,4),(5,4),(6,5),(7,5),(8,5),(9,5),(10,5)\}$$

And for V' these pairs are:

$$V' \times D_{V'} = \{(a,5),(b,5),(c,5),(d,5),(e,5),(f,5),(g,4),(h,4),(i,4),(j,4),(k,4)\}$$

Assume then there exists a bijection $\phi : \{0, ..., 10\} \to \{a, ..., k\}$. By noting the listed degrees of each vertex we have the following:

- Elements from $\{1, 2, 3, 4, 5\}$ map to $\{g, h, i, j, k\}$.
- Elements from $\{0, 6, 7, 8, 9, 10\}$ map to $\{a, b, c, d, e, f\}$.

We then note that in the first graph the vertex 0 is connected to 5 edges each with degree of 4. Hence in the other graph each neighbour of $\phi(0)$, that is any of $\phi(1), \phi(2), \phi(3), \phi(4), \phi(5)$, must have a degree of 4 as well for bijectivity to hold. However in the set $\{a, b, c, d, e, f\}$ (to which $\phi(0)$ must map to) there is:

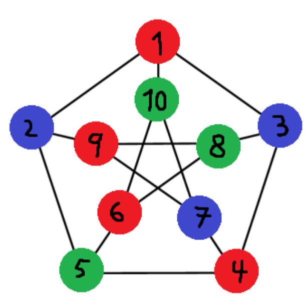
- One element such that all the neighbours have a degree of 5.
- Five elements such that two of the neighbours have degree of 4 and three of the neighbours have a degree of 5.

Hence there is no $\phi(0)$ (no matter how this element is chosen) such that all the neighbours of $\phi(0)$ have degree of 4. This is a contradiction, giving that the assumption of bijective ϕ is false. Hence the two graphs are not isomorphic.

Problem 4. (10pts) Colour the following graph with the greedy algorithm.

Can you find an ordering of the vertices such that the greedy algorithm colours the graph with 3 colors?

Solution 4. Label the colors 1,2,3 by Red, Green, Blue. Then by the greedy algorithm we get (for example) the following coloring.



Discrete Mathematics
Exercise sheet 6
Solutions for exploratory & additional exercises
April 2021

Exploratory problems:

Problem 1.

A number n ∈Z is divisible by m∈Z if there exists k∈Z such that:

$$mk = n$$

If such a k exists, then we say that "m divides n" and denote this m|n

a)

For all a∈Z: a*1 = a

Hence for all a∈Z a|a

b)

For all a∈Z: 1*a = a

Hence for all a∈Z 1|a

c)

False.

For example there is no k ∈Z such that

2*k = 1

And hence the statement does not hold for all a∈Z.

Infact it only holds for a = -1 and a = 1.

d)

False.

For example there is no k ∈Z such that

0*k = 1

And hence the statement does not hold for all a∈Z.

Under the definition of divisibility we are using it only holds for a = 0.

e)

For all a∈Z: a*0 = 0

Hence for all a∈Z a|0

f)

False.

For example let a = 1 and b = 5. Now

a*5 = b and hence a|b

but there is no k ∈Z such that

5*k = 1

And hence the statement does not hold for all a, b∈Z.

Infact it only holds for a and b such that |a| = |b|.

g)

If a|b and a|c then

a*n = b and a*m = c therefore

a*n + a*m = b + c = a*(n + m) and hence a k exists such that

ak = b + c and hence

a|b+c

h)

If a|b and b|c then

a*n = b and b*m = c and hence

(a*n)*m = c and hence a k exists such that

a*k = c

and therefore

a|c

i)

if a|b and b|a then

$$an = b \wedge bm = a \leftrightarrow bmn = b \leftrightarrow mn = 1 \leftrightarrow n = m = 1 \vee n = m = -1 \rightarrow a = b \vee a = -b$$

Problem 2.

The divisors of 98 are 1, 2, 7, 14 and 98.

The divisors of 105 are 1, 3, 5, 7, 15, 21, 35 and 105

The gcd is 7.

Problem 3.

a)

Let $c \in Z$ be such that c|a and c|b and therefore there exists some $k, m \in Z$ such that ck = a and cm=b. Then

$$b - na = cm - nck = c(m - nk)$$

And hence c|b-na for all common divisors of b and a.

b)

It should be obvious that the greatest common divisor of 2 numbers depends only upon the numbers, and therefore gcd(2331, 2037) = gcd(2037, 2331).

Now using part a we know that every common divisor of 2331 and 2037 is also a divisor of 2331-2037, and hence the greatest common divisor of 2331 and 2037 is also a divisor of 2331-2037, and hence also the greatest common divisor of 2037 and 2331-2037

Therefore gcd(2331,2037) = gcd(2037,2331-2037) = gcd(2037,294)

c)

gcd(2331, 2037) = gcd(2037, 294) = gcd(294, 2037-6*294) = gcd(273, 294) =

gcd(273, 21) = gcd(21, 273 – 13*21) = gcd(21, 0)

d)

By the result in problem 1 part a) we know that every integer divides itself, and hence it should be clear that the greatest divisor of any non-zero integer is itself, since if b > a and a is not 0 there can be no integer n such that bn = a.

By the result in problem 1 part e) we know that every integer divides 0.

And hence all divisors of any integer a are common divisors of a and 0.

Hence the greatest common divisor of a > 0 and 0 must be the greatest divisor of a, which is a. In otherwords gcd(a, 0) = a

e)

By part c we know gcd(2331,2037) = gcd(21, 0)

And by part d we know gcd(21,0) = 21

Problem 4

a)

If we add 2 to the value of x we have the following function

3*3 -2y = 1 in which case y clearly needs to be 4 since 9 – 8 = 1, and hence if we were to add 2 to x we must add 3 to y.

This should be obvious considering that the coefficient of x is 3 and the coefficient of y is -2.

b)

All the integer solutions are of the form

$x = 2n + 1$, $y = 3n + 1$, $n \in Z$

$3*(2n + 1) – 2*(3n + 1) = 6n + 3 – 6n - 2 = 1$ for all $n \in Z$

Additional problems:

Problem 1.

Base case:

$13^0 – 6^0 = 1 – 1 = 0 = 7*0$

$13^1 – 6^1 = 13 – 6 = 7 = 7*1$

Since it is true for some n lets assume it true for n and show that it holds for n + 1

$13^n – 6^n = 7*m$

$13^{n+1} – 6^{n+1} = 13*13^n – 6*6^n = (6 + 7)*13^n – 6*6^n = 7*13^n + 6*13^n – 6*6^n$

$= 7*13^n + 6*(13^n – 6^n) = 7*13^n + 6*7*m = 7*(13^n + 6*m)$

Since a $k = (13^n + 6*m)$ exists such that $7*k = 13^{n+1} – 6^{n+1}$ we conclude $7|13^{n+1} – 6^{n+1}$

And therefore by induction $7|13^n – 6^n$ for all $n \in Z$

Problem 2.

a)

$$3^3 \equiv 27 \equiv 1 \, mod \, 13$$

$$3^{19} \equiv 3 * (3^3)^6 \equiv 3 * 1^6 \equiv 3 \, mod \, 13$$

b)

$$4^3 \equiv 64 \equiv 10 \, mod \, 27$$

$$(10)^3 \equiv 1000 \equiv 1 \, mod \, 27$$

$$4^{12} \equiv (10)^3 * 10 \equiv 10 \, mod \, 27$$

c)

$$12 \equiv -3 \, mod \, 15$$

$$12^{27} \equiv (((-3)^3)^3)^3 \equiv ((-27)^3)^3 \equiv ((3)^3)^3 \equiv (27)^3 \equiv (12)^3 \equiv (-3)^3 \equiv -27 \equiv 3 \, mod \, 15$$

d)

$146^2 \equiv 1$ mod 21

Problem 3.

a)

If $n|a-b$ then we say $a \equiv b \mod n$

Since $a \equiv b \mod n$ by definition $n|a – b$ and hence $nk = a – b$ for some $k\in Z$ and therefore

$a^2 – b^2 = (a – b)(a + b) = nk(a + b)$ from which we see that n is a factor of $a^2 – b^2$, and hence $n|\ a^2 – b^2$ and hence $a^2\equiv b^2 \mod n$.

b)

9 mod 7 = 2 and 16 mod 7 = 2 therefore $9 \equiv 16 \mod 7$

However 3 mod 7 = 3 and 4 mod 7 = 4.

Therefore this is proven false by counterexample.

Problem 4.

$$n^8 - 2n^6 + n^4 = n^4(n^4 - 2n^2 + 1) = n^4(n^2 - 1)^2 = n^4((n + 1)(n - 1))^2$$
$$= n^2(n(n + 1)(n - 1))^2$$

Lets denote $n^8 - 2n^6 + n^4$ = k

Now we observe that 3 consecutive numbers are factors of (n(n+1)(n-1)) and given 3 consecutive numbers 1 is always divisible by 3, and hence (n(n+1)(n-1)) is divisible by 3. Hence $(n(n+1)(n-1))^2$ is divisible by $3^2 = 9$ and since it is a factor of k , k too is divisible by 9.

Further we observe that n^4 is a factor k, and since any even number is divisible by 2 if n were to be even it would be divisible by 2, and hence n^4 would be divisible by $2^4 = 16$ and since it is a factor of k, k too would be divisible by 16. If n were odd however we observe that n + 1 and n – 1 would both be even, and hence their product would be divisible by 4, and hence $((n + 1)(n – 1))^2$ would be divisible by 16, and since it is a factor of k, k too would be divisible by 16.

Therefore regardless of how n is chosen k has 9 and 16 as its factors, and hence has their product as its factor, and 9*16 = 144.

Therefore regardless of how n is chosen k is divisible by 144.

Problem 5.

First break the number into its prime factors, and then observe that if p is a prime then 1/p of all numbers are divisible by it, and then if p is a divisor of x then 1/p of the numbers less than x are also divisible by p and hence not relatively prime to x. And therefore if x can be factorized by primes $p_1 \ldots p_n$ then the number of numbers less than x that are relatively prime to it can be calculated by removing all the numbers that have the same prime factors in the following manner:

$\varphi(x) = x*(1- 1/p_1)*\ldots*(1-1/p_n)$

a)

$\varphi(200) = \varphi(5^2\ 2^3) = 200*(1-1/2)*(1-1/5) = 200*0.5*0.8 = 80$

b)

φ(121) = 110

c)

φ(635) = 504

d)

φ(1010) = 400

e)

φ(2021) = 1932

Problem 6.

Let there be a sequence of 5 numbers a, a+1, a+2, a+3, a+4 where a is an odd prime number.

This means a+1 and a+3 must be even, while a+2 and a+4 are odd.

Every third number is divisible by 3. Since a is prime a is either 3, or not divisible by 3.

If a is 3, then a + 2 = 5, and 2 + 4 = 7 which is a triplet prime.

If a is not 3, and since a is an odd prime number it is therefore also not divisible by 3, then either a + 1 is divisible by 3, in which case a + 4 = a + 1 + 3 is also divisible by 3, which means a+4 is not a prime and hence we do not have a triplet prime, or a + 2 is divisible by 3 in which case we also do not have a triplet prime.

Therefore unless a is 3 a triplet prime is not possible, and hence the only triplet prime is 3, 5 and 7.

Problem 7.

a)

Each fibonacci number is the sum of the two previous fibonacci numbers. Let f_n and f_{n-1} be fibonacci numbers then $f_n = f_{n-1} + f_{n-2}$

Recall that gcd(a+b, b) = gcd(a, b) and observe that since $f_n = f_{n-1} + f_{n-2}$ it must be that:

$\gcd(f_n, f_{n-1}) = \gcd(f_{n-1} + f_{n-2}, f_{n-1}) = \gcd(f_{n-1}, f_{n-2})$ and since $f_{n-1} = f_{n-2} + f_{n-3}$ we can repeat this n-2 times until we reach $\gcd(f_2, f_1) = \gcd(1, 1) = 1$ and hence the gcd of any 2 consecutive fibonacci numbers is 1.

b)

As shown in part a) it takes n – 2 steps.

c)

Let us prove by induction that F_n and F_{n-1} are the smallest numbers for which euclids algorithm takes n-2 steps.

base case:

Let n = 3 then $f_n = 2$ and $f_{n-1} = 1$ and a = b = 1, and it takes euclid 1 step to compute for f_n and f_{n-1} while it takes 0 steps to compute for a = b.

Step:

Let us assume that for some n F_n and F_{n-1} are the smallest numbers a > b for which euclids algorithm takes n-2 steps.

Now let us consider n + 1. Let c > d be integers for which euclids algorithm takes n – 1 steps. Then when we take the first step of the algorithm we have gcd(c, d) = gcd(d, c-d) and we know that gcd(d, c-d) takes n-2 steps, and furthermore we know d and c-d must be the smallest integers taking n-2 steps, since c and d were the smallest integers taking n-1 steps. But since we also know F_n and F_{n-1} are the smallest numbers a > b for which euclids algorithm takes n-2 steps we conclude that $F_n = d$ and $F_{n-1} = c-d$ and:

$$F_{n+1} = F_n + F_{n-1} = d + c - d = c$$

And therefore the smallest integers requiring n-1 steps are F_{n+1} and F_n and hence we have proven by induction that for all n the smallest integers for which euclids algorithm requires n-2 steps is F_n and F_{n-1}

Therefore also for any integest a, b such that $b \leq a < F_n$ euclids algorithm takes more steps to compute $\gcd(F_n, F_{n-1})$ than gcd(a, b).

HOMEWORK 6 SOLUTIONS,
MS-A0402, FOUNDATIONS OF DISCRETE MATHEMATICS

TEEMU TASANEN

Homework

The written solutions to the homework problems should be handed in on MyCourses by Monday 11.4., 12:00. You are allowed and encouraged to discuss the exercises with your fellow students, but everyone should write down their own solutions.

Problem 1. (10pts) Does the following Diophantine equation

$$20x + 10y = 65.$$

have solutions $x, y \in \mathbb{N}$? If yes, find all the solutions. If not, justify your answer.

Solution 1. We compute

$$\gcd(20, 10) = \gcd(20 - 10, 10) = \gcd(10, 10) = \gcd(10 - 10, 10) = \gcd(0, 10) = 10$$

by the Euclidean algorithm. As 10 does not divide 65, the equation has no integer solutions.

Problem 2. (10pts) Does the following Diophantine equation

$$20x + 16y = 500.$$

have solutions $x, y \in \mathbb{N}$? If yes, find all the solutions. If not, justify your answer.

Solution 2. We compute $\gcd(20, 16)$ using the Euclidean algorithm.

$$\gcd(20, 16) = \gcd(20 - 1 \cdot 16, 16) = \gcd(4, 16) = \gcd(4, 16 - 4 \cdot 4) = \gcd(4, 0) = 4$$

Clearly 4 divides 500 so we expect the equation to have integer solutions. We can use the steps of the algorithm to write $500 = 125 \cdot 4$ as a linear combination of 20 and 16.

$$500 = 125 \cdot 4 = 125 \cdot (20 - 1 \cdot 16) = 20 \cdot 125 + 16 \cdot (-125)$$

So a particular solution is $x_0 = 125$ and $y_0 = -125$. Let $u = x - x_0$ and $v = y - y_0$ (x and y are some solution of the original equation). Then we must have the following.

$$20u + 16v = 0$$

This is a homogeneous Diophantine equation with solutions of the form $u = \frac{16}{4}k = 4k$ and $v = -\frac{20}{4}k = -5k$ with $k \in \mathbf{Z}$. We hence get that $x = u + x_0 = 4k + 125$ and $y = v + y_0 = -5k - 125$. Finally, we want only solutions such that $x, y \in \mathbb{N}$ so we get restrictions for k from $4k + 125 \geq 0$ and $-5k - 125 \geq 0$. Getting bounds for k from each inequality and combining these gives $-31.25 \leq k - 25$, meaning $-31 \leq k \leq -25$ as $k \in \mathbb{Z}$. The set of possible solution pairs (x, y) is hence

$$\{(4k + 125, -5k - 125) : k \in \mathbb{Z},\ -31 \leq k \leq -25\}.$$

Problem 3. (10pts) How many integers less than 22220 are relatively prime to 22220?

Solution 3. We note that $22220 = 10 \cdot 2222 = 2 \cdot 5 \cdot 2 \cdot 1111 = 2^2 \cdot 5 \cdot 11 \cdot 101$. As these are prime numbers and the prime factorization is always unique we can use Euler's totient function, which gives as the amount of relative primes

$$\phi(22220) = 22220 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{101}\right) = 8000.$$

Problem 4. (10pts) Compute the last two digits of 2022^{2022}.

Solution 4. Evaluating the last two digits corresponds to calculating $2022^{2022} \mod 100$. We first note that $2022 \equiv 22 \mod 100$ and hence $2022^{2022} \equiv 22^{2022} \mod 100$. Our goal is to apply Euler's theorem to simplify the large power. We have $\phi(100) = 40$ and hence write

$$\begin{aligned} 2022^{2022} &\equiv 22^{2022} = 2^{2022} 11^{2022} = 2^{101 \cdot 20 + 2} \cdot (11^{40})^{50} \cdot 11^{22} \mod 100 \\ &= (2^{101 \cdot 20 + 2} \mod 100) \cdot ((11^{40})^{50} \mod 100) \cdot (11^{22} \mod 100) \end{aligned}$$

The problem hence reduces to evaluating the three factors of the above product in mod 100.

(1) The leftmost part reduces to $2^2 = 4$ as powers of two repeat in a cycle in mod 100. The pattern can be found from a table and shown by induction, which is omitted here.
(2) The middle part is equal to 1, which follows from Euler's theorem by remembering that $\phi(100) = 40$ and noting that 11 and 100 are coprime i.e. $\gcd(11, 100) = 1$.
(3) The right part $11^{22} = (11^2)^{11} \equiv 21^{11} \mod 100$ is something we can calculate by writing the exponent as a sum of powers of 2 (in binary) i.e. $11 = 2^0 + 2^1 + 2^3 = 1 + 2 + 8$. We then have the following.

$$21^2 \equiv 441 \equiv 41 \mod 100$$
$$21^4 \equiv 41 \cdot 41 = 1681 \equiv 81 \mod 100$$
$$21^8 \equiv 81 \cdot 81 = 6561 \equiv 61 \mod 100$$

This gives $11^{22} \equiv 21^{11} = 21^1 \cdot 21^2 \cdot 21^8 = 21 \cdot 41 \cdot 61 = 52521 \equiv 21 \mod 100$.

Combining these results finally gives $2022^{2022} \equiv= 4 \cdot 1 \cdot 21 = 84 \mod 100$. The last two digits are hence 8 and 4.