Discrete Mathematics (104.697)

Alttest Collection

With Solutions

Repository

Contents

1 2024-11-08 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_Exam_2024-11-08

1.1

Is $\mathbb{Z}_5[x]/(x^4+x^2+1)$ a field? List all members of it.

Is $x+2$ a unit in it? If so, find its multiplicative inverse

✨ Solution for 1.1 by arch user ✨

a) Is it a field? List all member of it.
$p(x) = x^4+x^2+1, \mathbb{Z}_5$ is a field $\Rightarrow \mathbb{Z}_5/(p(x))$ is a field $\Leftrightarrow p(x)$ is irreducible

$$p(x) = x^4+x^2+1 = (x^2-x+1)(x^2+x+1)$$

therefore it is **reducible** $\Rightarrow \mathbb{Z}_5/(p(x))$ is **not** a field (only a quotient ring)
Elements in this quotient ring:

$$\deg(p(x)) = 4$$
$$Q(x) = k(x)\cdot p(x) + r(x)$$
$$\text{with } \deg(r(x)) < \deg(p(x)) = 4$$
$$\Longrightarrow r(x) = ax^3+bx^2+cx+d \quad \text{with} \quad a,b,c,d \in \mathbb{Z}_5$$

b) is $x+2$ a unit in $\mathbb{Z}_5/(p(x))$?

✨ Solution for 1.1 by $m\cdot\sum_{i=0}^{\infty}\frac{1}{k!}$ ✨

1. **Is $\mathbb{Z}_5[x]/(x^4+x^2+1)$ a field? List all members of it.**

   $R[x]/P(x)$ is field $\Leftrightarrow R$ is a field $\wedge$ $P(x)$ is irreducible.

   - $\mathbb{Z}_5$ is Field ✓
   - $$P(x) = x^4+x^2+1 = (x^2+ax+1)(x^2+bx+1)$$
     $$= (x^4+ax^3+x^2+bx^3+abx^2+bx+x^2+ax+1)$$

     $$1 = 2+ab$$
     $$0 = a+b$$
     $$\Rightarrow a = 1$$
     $$b = -1$$
     $$\Rightarrow P(x) = x^4+x^2+1 = (x^2+x+1)(x^2-x+1)$$

     ✗ reducible

     $$\mathbb{Z}_5/(x^4+x^2+1) = \left\{\overline{(ax^3+bx^2+cx+d)} \mid a,b,c,d \in \mathbb{Z}_5\right\}$$

   $\Longrightarrow$ **No Field**, just a factorring
2. **Is $x+2$ a unit in it? If so, find its multiplicative inverse**

   $$(x+2)(x+2)^{-1} \equiv 1 \bmod x^4+x^2+1$$

$$x^4 + x^2 + 1 = (x+2)(x^3 - 2x^2) + 1$$

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

$$\implies (x+2)^{-1} = (4x^3 + 2x^2)$$

1.2

Determine the number of spanning trees for a given graph (consisting of two connected components and 8 total vertices) using the matrix-tree-theorem.

The *Matrix-Tree-Theorem (Kirchhoff)* cannot be used without having the adjacency matrix A and the degree matrix D. Further calculating the det of a 7×7 matrix would be way too hard.

1.3

Let φ be a ring homomorphism and R, S two rings. Let I be the ideal of S. Prove that $\varphi^{-1} = \{x \in R \mid \varphi(x) \in I\}$ is an ideal as well.

✨ Solution for 1.3 by arch user ✨

💻 Theory

Ideal Properties:
1. closed under $+$
2. absorbing under $\cdot$

ad 1)
Let $J = \varphi^{-1}(I)$

$$\begin{aligned} a + b &= \varphi^{-1}(\varphi(a+b)) \\ &= \varphi^{-1}(\varphi(a) + \varphi(b)) \quad \text{with} \quad \varphi(a) \in I \wedge \varphi(b) \in I \\ &= \varphi^{-1}(\varphi(c)) \quad \text{with} \quad \varphi(c) \in I \\ &= c \in J \end{aligned}$$

ad 2)

$$\begin{aligned} a \cdot b \in J, a \in R, b \in J& \\ a \cdot b &= \varphi^{-1}(\varphi(a \cdot b)) \\ &= \varphi^{-1}(\varphi(a) \cdot \varphi(b)) \\ &= \varphi^{-1}(c) \in J \end{aligned}$$

✨ Solution for 1.3 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

$$\varphi^{-1} = \{x \in R \mid \varphi(x) \in I\}$$

$$\begin{aligned} \varphi^{-1} - \varphi^{-1} &= \{x - y |\ x, y \in R \wedge \varphi(x) \in I \wedge \varphi(y) \in I\} \\ &= \{x - y \in R \mid \varphi(x-y) \in I\} \subseteq \varphi^{-1} \checkmark \end{aligned}$$

$$\begin{aligned} a\varphi^{-1} &= \{ax \mid x \in R \wedge \varphi(x) \in I\} \qquad a \in R \\ &= \{ax \in R \mid \varphi(ax) \in I\} \subseteq \varphi^{-1} \checkmark \end{aligned}$$

$$\begin{aligned} \varphi^{-1}a &= \{xa \mid x \in R \wedge \varphi(x) \in I\} \qquad a \in R \\ &= \{xa \in R \mid \varphi(xa) \in I\} \subseteq \varphi^{-1} \checkmark \end{aligned}$$

✨ Solution for 1.3 by BlauBarschBube ✨

Let $J = \varphi^{-1}(I)$
What we want to show:
1. closed under $+$

2. Neutral element of $R \in J$
3. J commutative
4. J associative
5. J contains inverses of all its elements
6. absorbing under $\cdot$

ad 1)
Let $a, b \in J$:

$$\begin{aligned} a + b &\in \varphi^{-1}(\varphi(a+b)) \\ &\in \varphi^{-1}(\varphi(a) + \varphi(b)) \quad \text{by homomorphism with } \varphi(a), \varphi(b) \in I \\ &\in \varphi^{-1}(\varphi(c)) \quad \text{by I being closed under addition with } \varphi(c) \in I \\ &\Rightarrow a + b \in J \end{aligned}$$

ad 2)
Let $e_R \in R$ be the neutral element of R
Let $a \in R$

$$\begin{aligned} a &= a + e_R \\ \varphi(a) &= \varphi(a + e_R) \\ \varphi(a) &= \varphi(a) + \varphi(e_R) \quad \text{by homomorphism with } \varphi(a), \varphi(e_R) \in S \\ \varphi(a) - \varphi(a) &= \varphi(a) + \varphi(e_R) - \varphi(a) \quad \text{inverse elements exist in S} \\ e_S &= e_S + \varphi(e_R) \quad \text{reordering okay because of commutativity} \\ e_S &= \varphi(e_R) \\ e_S &\in I \quad \text{by I being an ideal} \\ &\Rightarrow e_r \in J \end{aligned}$$

ad 3)
Fulfilled by R being a Ring

ad 4)
Fulfilled by R being a Ring

ad 5)
Let $a \in J$ and $-a \in R$

$$\begin{aligned} a + (-a) &= e_R \\ \varphi(a + (-a)) &= \varphi(e_R) \\ \varphi(a) + \varphi(-a) &= e_S \quad \text{by homomorphism, now add inverse of } \varphi(a) \\ \varphi(a) - \varphi(a) + \varphi(-a) &= e_S - \varphi(a) \\ e_S + \varphi(-a) &= -\varphi(a) \\ \varphi(-a) &= -\varphi(a) \quad \text{but } -\varphi(a) \in I \\ &\Rightarrow \varphi(-a) \in I \\ &\Rightarrow -a \in J \end{aligned}$$

So J is abelian, which makes it a normal subgroup.

ad 6)
Let $a \in R, b \in J$

$$
\begin{aligned}
a * b \in R \quad &\text{by R being a Ring} \\
\varphi(a * b) &\in \varphi(R) \\
\varphi(a) * \varphi(b) &\in S \quad \text{by homomorphism} \\
\varphi(a) \in S, \varphi(b) \in I &\Rightarrow \varphi(a) * \varphi(b) \in I \\
\varphi(a) * \varphi(b) \in I &\Rightarrow \varphi(a * b) \in I \quad \text{by homomorphism} \\
&\Rightarrow a * b \in J
\end{aligned}
$$

1.4

A Hasse diagram of a poset was given. Determine the value of the Möbius function $\mu(0,1)$

⚠ Not Relevant

Not in the 6 ECTS version of *Discrete Math*

2 2024-10-04 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_exam_2024-10-04

2.1

1. How many multisets of $\{a, b\}$ are there of size 12?
2. How many multisets which are subsets of $M = \{a, a, a, a, b, b, b, b, b, b, c, c, c, c, c\}$ are there of size 12? Answer this question by
   1. Determining the number of multisets which are not subsets of M because they contain too many a's
   2. Using the principle of inclusion-exclusion

✨ Solution for 2.1 by arch user ✨

ad 1)
ordered k-Multisets: 212
ot ordered: $\binom{n+k-1}{k} = \binom{2+2-1}{12} = \binom{13}{12}$

ad 2)
$4 \times a, 6 \times b, 5 \times c$
2.1
with 5 a: $\Rightarrow \binom{3+7-1}{7} = \binom{9}{7} = \binom{9}{2} = \frac{9 \cdot 8}{2 \cdot 1} = 36$
2.2)
god help....

✨ Solution for 2.1 by acrobatic aviator ✨

ad 1)
#multisets of size k with ground set size n:
$\binom{n+k-1}{k} = \binom{12+2-1}{12} = \binom{13}{12} = \frac{13!}{12! \cdot (13-12)!} = \frac{13!}{12!} = 13$

ad 2)
$|S| = \binom{3+12-1}{12} - (|A_{\text{too many}}| + |B_{\text{too many}}| + |C_{\text{too many}}|) + (|AB_{\text{too many}}| + |BC_{\text{too many}}| + |AC_{\text{too many}}|) - (|ABC_{\text{too many}}|)$

$$|X_{\text{too many}}| = \sum_{i=\#x}^{12} \binom{2+(12-i)-1}{12-i} = \sum_{i=\#x}^{12} \binom{13-i}{12-i} = \sum_{i=0}^{12-\#x} \binom{13-(i+\#x)}{12-(i+\#x)} =$$
$$= \sum_{i=0}^{12-\#x} \binom{13-\#x-i}{12-\#x-i} = \sum_{i=0}^{12-\#x} 13 - \#x - i = \sum_{i=0}^{12-\#x} i + 1 = \sum_{i=1}^{13-\#x} i$$

$$|A_{\text{too many}}| = \sum_{i=1}^{8} i = 9 \cdot 4 = 36$$
$$|B_{\text{too many}}| = \sum_{i=1}^{6} i = 7 \cdot 3 = 21$$
$$|C_{\text{too many}}| = \sum_{i=1}^{7} i = 8 \cdot 3 + 4 = 28$$

$|AB_{\text{too many}}|$: $\#a \geq 5 \wedge \#b \geq 7 \implies 5+7=12 \implies$ only one option
$|AB_{\text{too many}}| = 1$

$|AC_{\text{too many}}|$: $\#a \geq 5 \wedge \#c \geq 6 \implies 5+6=11 \implies$ **one** option with one b, **two** options with no b
$|AC_{\text{too many}}| = 3$

$|BC_{\text{too many}}|$: $\#b \geq 7 \wedge \#c \geq 6 \implies 7+6=13 \not\leq 12 \implies$ no possible option
$|BC_{\text{too many}}| = 0$

$|ABC_{\text{too many}}|$: $a \geq 5 \wedge \#b \geq 7 \wedge \#c \geq 6 \implies 5+7+6=18 \not\leq 12 \implies$ no possible option
$|ABC_{\text{too many}}| = 0$

$|S| = \binom{3+12-1}{12} - (36+21+28) + (1+0+3) - (0) = \binom{14}{12} - 85 + 4 = \frac{13 \cdot 14}{2} - 81 = 10$

✨ Solution for 2.1 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

1. $\binom{n+k-1}{k} = \binom{2+12-1}{12} = \binom{13}{12} = 13$
2. What we know:

$$1 \leq \#a \leq 4$$
$$3 \leq \#b \leq 6$$
$$2 \leq \#c \leq 5$$

$S \subset M$ where $|S| = 12$

$$\#S = \underbrace{\binom{3+12-1}{12}}_{=91} - (|A_{\text{too many}}| + |B_{\text{too many}}| + |C_{\text{too many}}|) +$$
$$+(|AB_{\text{too many}}| + |BC_{\text{too many}}| + |AC_{\text{too many}}|) - (|ABC_{\text{too many}}|)$$

$|\boldsymbol{A_{\text{too many}}}|$

$$\#a' := \#a - 5$$
$$\#a' + \#b + \#c = 7$$
$$\#a', \#b, \#c \geq 0$$
$$|A_{\text{too many}}| = \binom{7+3-1}{3-1} = 36$$

$|\boldsymbol{B_{\text{too many}}}|$

$$\#b' := \#b - 7$$
$$\#a + \#b' + \#c = 5$$
$$\#a, \#b', \#c \geq 0$$
$$|B_{\text{too many}}| = \binom{5+3-1}{3-1} = 21$$

$|\boldsymbol{C_{\text{too many}}}|$

$$\#c' := \#c - 6$$
$$\#a + \#b + \#c' = 6$$
$$\#a, \#b, \#c' \geq 0$$
$$|C_{\text{too many}}| = \binom{6+3-1}{3-1} = 28$$

$\boldsymbol{|AB_{\text{too many}}|}$

$$\#a' := \#a - 5$$
$$\#b' := \#b - 7$$
$$\#a' + \#b' + \#c = 0$$
$$\#a', \#b', \#c \geq 0$$
$$|AB_{\text{too many}}| = 1$$

$\boldsymbol{|AC_{\text{too many}}|}$

$$\#a' := \#a - 5$$
$$\#c' := \#c - 6$$
$$\#a' + \#b + \#c' = 1$$
$$\#a', \#b, \#c' \geq 0$$
$$|AC_{\text{too many}}| = \binom{1+3-1}{3-1} = 3$$

$\boldsymbol{|BC_{\text{too many}}|}$

$$\#b' := \#b - 7$$
$$\#c' := \#c - 6$$
$$\#a + \#b' + \#c' = -1$$
$$\#a, \#b', \#c' \geq 0$$
$$|BC_{\text{too many}}| = 0$$

$\boldsymbol{|ABC_{\text{too many}}| = 0}$ (obv.)

$$\#S = 91 - (36 + 21 + 28) +$$
$$+(1 + 3 + 0) - (0) =$$
$$= 10$$

2.2

Let R be an integral domain, and $a \in R$. Prove that $(a) = \{ar \mid r \in R\}$

⚠ Missing Details

Maybe some details in the tasks are missing: problem could be too easy or unsolvable!

The proof is just the definition of the principal ideal

✨ Solution for 2.2 by BlauBarschBube ✨

By definition (a) is the smallest ideal of R containing a

$\mathbb{I} := \{a \cdot r \mid r \in R\}$
We want to show that $\mathbb{I}$ is an ideal of R and that $\mathbb{I} = (a)$
Show that:
1. $a \in \mathbb{I}$
2. $(\mathbb{I}, +)$ is normal subgroup of R
3. $\mathbb{I}$ is closed under multiplication with elements from R

1) $a \cdot 1 = a \Rightarrow a \in \mathbb{I}$

2) Choose $k, m \in R$
Then $a \cdot k, a \cdot m \in \mathbb{I}$
$a \cdot k - a \cdot m = a \cdot \overbrace{(k - m)}^{\in R} \in \mathbb{I}$
$\Rightarrow$ additive inverses and the neutral element is in $\mathbb{I}$
Commutativity and associativity are given by R being a ring
$\Rightarrow \mathbb{I}$ abelian group and thus normal subgroup of R

3) Choose $a \cdot x \in \mathbb{I}$ and $y \in R$
$y \cdot (a \cdot x) = a \cdot \overbrace{y \cdot x}^{\in R} \in \mathbb{I}$
$\Rightarrow \mathbb{I}$ is ideal containing a
$\Rightarrow (a) \subseteq \mathbb{I}$

Now show $\mathbb{I} \subseteq (a)$
As (a) is an ideal with a, all $a \cdot r, r \in R$ are in (a)
$\Rightarrow \mathbb{I} \subseteq (a)$
$\Rightarrow (a) = \{a \cdot r, r \in R\}$

2.3

Let $G = (V, E)$ be a simple, undirected graph of $n = |V|$ vertices and $m = |E|$ edges. Also let $A \in \{0,1\}^{n \times n}$ be the adjacency matrix, $B \in \{0,1\}^{n \times m}$ the incidence matrix and D the degree matrix of G, where $a_{ij} = 1 \iff (v_i, v_j) \in E$ and $b_{ij} = 1 \iff v_i$ incident to e_j. Prove that $A + D = BB^T$

✨ Solution for 2.3 by arch user ✨

$$A = \begin{pmatrix} 0 & \dots & \dots \\ \dots & 0 & \dots \\ \dots & \dots & 0 \end{pmatrix} \dots \text{ diagonal is zero because no loops}$$

$$D = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix} \dots \text{ only diagonal } \neq 0 \text{ only there are the degrees}$$

Solved by *Double Counting*:

$$a_{ij} + d_{ij} = \sum_{j=0}^{m} b_{ij} \cdot b_{ji}$$

$$(BB^T)_{ij} = \sum_{p=0}^{m} b_{ip} \cdot b_{jp}$$

Case distinction:
for $i = j$:

$$b_{ip} \cdot b_{ip} = \begin{cases} 1 & \text{if } v_i \text{ is incident to } e_p \\ 0 & \text{otherwise} \end{cases}$$

$$\Rightarrow (BB^T) = \sum_{e_p \text{ is incident to } v_i} 1 = d(v_i) = d_{ii} + \underbrace{a_{ii}}_{=0}$$

G is a simple graph $\Rightarrow$ no double edges **for $i \neq j$:**

$$b_{ip} \cdot b_{jp} = \begin{cases} 1 & \text{if } (v_i \text{ is incident to } e_p) \wedge (v_j \text{ is incident to } e_p) \\ 0 & \text{otherwise} \end{cases}$$

$$\Rightarrow \sum_{p=0}^{m} b_{ip} \cdot b_{jp} = \underbrace{d_{ij}}_{=0} + a_{ij}$$

$$\Rightarrow \forall 1 \leq i, j \leq n : \sum_{p=0}^{m} b_{ip} \cdot b_{jp} = a_{ij} + d_{ij}$$

✨ Solution for 2.3 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

$R_{BB^T} := BB^T$

$r_{BB^T_{i,j}} = \sum_{k=0}^{m} b_{i,k} b_{j,k}$

$r_{BB^T_{i,j}} = \#$ common edges of i, j

In particular:

$$r_{BB^T_{i,i}} = d(i)$$
$$i \neq j \Rightarrow r_{BB^T_{i,j}} = 1 \Leftrightarrow i \text{ adjacent to } j$$

$$\left.\begin{array}{l} a_{i,i} = 0 \\ a_{i,j} = r_{BB^T_{i,j}} \text{ if } j \neq i \\ b_{i,j} = 0 \text{ if } i \neq j \\ b_{i,i} = r_{BB^T_{i,i}} \end{array}\right\} \Rightarrow A + D = BB^T$$

✨ Solution for 2.3 by BlauBarschBube ✨

$$(D+A)_{i,j} = \begin{cases} D_{i,i} \mid i = j \\ A_{i,j} \mid i \neq j \end{cases}$$

$$(B \cdot B^T) = \sum_{k=1}^{m} b_{i,k} \cdot b_{j,k}$$
$$= \begin{cases} \sum_{k=1}^{m} b_{i,k} \mid i = j \\ \sum_{k=1}^{m} b_{i,k} \cdot b_{j,k} \mid i \neq j \end{cases}$$

Case distinction:
for $i = j$:
The sum over the incident edges of a vertex is just the vertex degree ✓
for $i \neq j$:
G is a simple graph ⇒ no double edges

$$\sum_{k=1}^{m} b_{i,k} \cdot b_{j,k} = 1 \Leftrightarrow \text{vertex i and vertex j are incident to the same edge}$$

$$\text{Otherwise it is } 0 \Rightarrow \sum_{k=1}^{m} b_{i,k} \cdot b_{j,k} = A_{i,j}$$

So $D + A = B \cdot B^T$

2.4

Solve the following two systems of linear congruences or prove that there is no solution:

1. $\begin{cases} 2x \equiv 4 \bmod 8 \\ 5x \equiv 2 \bmod 11 \\ 4x \equiv 5 \bmod 15 \end{cases}$
2. $\begin{cases} 4x \equiv 4 \bmod 2 \\ 5x \equiv 2 \bmod 2 \\ 4x \equiv 5 \bmod 5 \end{cases}$

✨ Solution for 2.4 by arch user ✨

1)

$$\begin{aligned} 2x &\equiv 4 \bmod 8 \\ 5x &\equiv 2 \bmod 11 \\ 4x &\equiv 5 \bmod 15 \end{aligned}$$

first equation factor 2 can be cancelled everywhere

$$\begin{aligned} \Rightarrow x &\equiv 2 \bmod 4 \\ x &\equiv 2 \cdot 5^{-1} \bmod 11 \\ x &\equiv 5 \cdot 4^{-1} \bmod 15 \end{aligned}$$

$$\begin{aligned} x &\equiv 2 \bmod 4 \\ x &\equiv 2 \cdot 9 \bmod 11 \equiv 7 \bmod 11 \\ x &\equiv 5 \cdot 4 \bmod 15 \equiv 5 \bmod 15 \end{aligned}$$

all moduli are co-prime ⇒ CRT is allowed

$$x \equiv \sum a_i \cdot b_i \cdot \frac{m}{m_i} \bmod m$$

$$m = \prod m_i$$

$$b_i = \left(\frac{m}{m_i}\right)^{-1} \bmod m_i$$

$$\dots$$

$$\text{doing CRT}$$

$$\dots$$

$$x \equiv 2 \cdot 1 \cdot (11 \cdot 15) + 7 \cdot 9 \cdot (4 \cdot 15) + 5 \cdot 14 \cdot (4 \cdot 11) \bmod (4 \cdot 11 \cdot 15)$$

$$x \equiv 590 \bmod 660$$

2)

$$\begin{aligned} 4x &\equiv 4 \bmod 2 \\ 5x &\equiv 2 \bmod 2 \\ 4x &\equiv 5 \bmod 5 \end{aligned}$$

$$\begin{aligned} 0x &\equiv 0 \bmod 2 \\ 1x &\equiv 0 \bmod 2 \\ 4x &\equiv 5 \bmod 5 \end{aligned}$$

⚠️ You don't have to calculate b_i because they will all get eliminated due to the $a_i = 0$ ⚠️

✨ Solution for 2.4 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

1. $$\begin{cases} 2x \equiv 4 \bmod 8 \\ 5x \equiv 2 \bmod 11 \\ 4x \equiv 5 \bmod 15 \end{cases} = \begin{cases} 1x \equiv 2 \bmod 4 \\ 5x \equiv 2 \bmod 11 \\ 4x \equiv 5 \bmod 15 \end{cases} = \begin{cases} x \equiv 2 \bmod 4 \\ x \equiv 7 \bmod 11 \\ x \equiv 5 \bmod 15 \end{cases}$$

   $i \neq j \Rightarrow \gcd(m_i, m_j) = 1 \checkmark \Rightarrow$ Use chinese remainder threorem

   $$\begin{aligned} a_1 &= 2 \\ a_2 &= 7 \\ a_3 &= 5 \\ m_1 &= 4 \\ m_2 &= 11 \\ m_3 &= 15 \\ m &= 660 \end{aligned}$$

   $$b_i = \left(\frac{m}{m_i}\right)^{-1} \bmod m_i$$

   $$b_1 = \left(\frac{660}{4}\right)^{-1} \bmod 4 = (1)^{-1} \bmod 4 = 1 \bmod 4$$

   $$b_2 = \left(\frac{660}{11}\right)^{-1} \bmod 11 = (5)^{-1} \bmod 11 = 9 \bmod 11$$

   $$b_3 = \left(\frac{660}{15}\right)^{-1} \bmod 15 = (14)^{-1} \bmod 15 = 14 \bmod 15$$

   $$x \equiv \sum_{i=0}^{3} \frac{m}{m_i} b_i a_i \bmod m \equiv 7190 \bmod 660 \equiv 590 \bmod 660$$

2. $$\begin{cases} 4x \equiv 4 \bmod 2 \\ 5x \equiv 2 \bmod 2 \\ 4x \equiv 5 \bmod 5 \end{cases} = \begin{cases} 0x \equiv 0 \bmod 2 \\ x \equiv 0 \bmod 2 \\ x \equiv 0 \bmod 5 \end{cases}$$

   First congruence is a tautology $\Rightarrow$ we can remove it.

   $$\begin{cases} x \equiv 0 \bmod 2 \\ x \equiv 0 \bmod 5 \end{cases}$$

   Chinese remainder theorem can be applied since $\gcd(2, 5) = 1$

   $x \equiv 0 \bmod 10$

✨ Solution for 2.4 by acrobatic aviator ✨

1. Look at other solutions
2.

$$
\begin{aligned}
& 4x \equiv 4 \mod 2 \\
1) \quad & 0 \equiv 0 \mod 2 \implies \text{Always true, equation can be ignored} \\
& 5x \equiv 2 \mod 2 \\
2) \quad & x \equiv 0 \mod 2 \\
& 4x \equiv 5 \mod 5 \\
& 4x \equiv 0 \mod 5 \\
3) \quad & x \equiv 0 \mod 5
\end{aligned}
$$

Remove equation 1 from the system because it is always true to get the new system:

$$
\begin{aligned}
x &\equiv 0 \mod 2 \\
x &\equiv 0 \mod 5
\end{aligned}
$$

Then the chinese remainder theorem can be applied, since $\gcd(2, 5) = 1$.

But you can also trivially see that the solution is $x \equiv 0 \mod 10$

3 2024-07-02 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_Exam_2024-07-02

3.1

Is the polynomial $p(x) = x^6 + x^5 + x^2 + x + 1$ a primitive in $\mathbb{Z}_2$?

✨ Solution for 3.1 by acrobatic aviator + BlauBarschBube ✨

Theory

A generator a of $K \setminus \{0\}$ is called a **primitive element of K**, its minimal polynomial over $P(K) \cong \mathbb{Z}_p$ is called a **primitive polynomial** with root a.

$p(x)$ is primitive $\iff p(x)$ irreducable $\wedge\ \exists a \in K \setminus \{0\} : p(a) = 0 \wedge (a) = K \setminus \{0\}$

1. **to prove**: $p(x)$ irreducable over $\mathbb{Z}_2[x]$
   - there are no linear factors, since $p(0) = 1$ and $p(1) = 1$
   - try splitting into a polynomial of second degree:

$$\begin{aligned} p(x) &= (x^4 + ax^3 + bx^2 + cx + 1) \cdot (x^2 + dx + 1) \\ &= x^6 + x^5 \cdot (d + a) + x^4 \cdot (1 + ad + b) + x^3 \cdot (a + bd + c) + x^2 \cdot (b + cd + 1) + x \cdot (d + c) + 1 \end{aligned}$$

compare coefficients:

$$\begin{aligned} 1: &\quad 1 = d + a \\ 2: &\quad 0 = 1 + ad + b \\ 3: &\quad 0 = a + bd + c \\ 4: &\quad 1 = b + cd + 1 \\ 5: &\quad 1 = d + c \end{aligned}$$

$$\begin{aligned} 1: &\quad d = 1 + a \\ 2: &\quad 0 = 1 + \underbrace{a \cdot (1 + a)}_{=0} + b \implies b = 1 \\ 4: &\quad b = cd = 1 \\ 5: &\quad 1 = c + d \end{aligned}$$

4 and 5 are a contradiction, since $c \cdot d$ and $c + d$ cannot be both 1 in $\mathbb{Z}_2$.

   - try splitting into two polynomials of third degree:

$$\begin{aligned} p(x) &= (x^3 + ax^2 + bx + 1) \cdot (x^3 + cx^2 + dx + 1) \\ &= x^6 + x^5 \cdot (a + c) + x^4 \cdot (b + ca + d) + x^3 \cdot (bc + ad) + x^2 \cdot (c + bd + a) + x \cdot (d + b) + 1 \end{aligned}$$

compare coefficients:

$$\begin{aligned} 1: &\quad 1 = a + c \\ 2: &\quad 0 = b + ca + d \\ 3: &\quad 0 = bc + ad \\ 4: &\quad 1 = c + bd + a \\ 5: &\quad 1 = b + d \end{aligned}$$

$$5: \quad d = b + 1$$
$$2: \quad 0 = b + ca + b + 1 \implies ca = 1$$

1 and 2 are a contradiction, since $a + c$ and $a \cdot c$ cannot be both 1 in $\mathbb{Z}_2$

$\implies$ $p(x)$ is irreducable ✓

2. **to prove**: $\exists a \in \mathbb{F}_{64}$ with $p(a) = 0 \wedge (a) = \mathbb{Z}_2[x]/p(x) \setminus \{0\}$

$$|\mathbb{Z}_2[x]/p(x) \setminus \{0\}| = 2^6 - 1 = 63 \implies \text{ord}(a) \mid 63 = 3^2 \cdot 7$$

So we need to check all the divisors of 63, which are $1, 3, 7, 9, 21$.

The check we need is that for every d divisor of 63, $a^d \neq 1$.
If this check holds for every divisor < 63, then $\text{ord}(a)$ has to be 63. Then it generates the whole field.

$p(a) = 0 = a^6 + a^5 + a^2 + a + 1 \implies a^6 = a^5 + a^2 + a + 1$

$$\begin{aligned}
&\longrightarrow \quad a^1 \neq 1 \checkmark \\
&\qquad\quad a^2 \neq 1 \checkmark \\
&\longrightarrow \quad a^3 \neq 1 \checkmark \\
&\qquad\quad a^4 \neq 1 \checkmark \\
&\qquad\quad a^5 \neq 1 \checkmark \\
&\qquad\quad a^6 = a^5 + a^2 + a + 1 \neq 1 \checkmark \\
&\longrightarrow \quad a^7 = a^6 \cdot a = a^5 + a^3 + 1 \neq 1 \checkmark \\
&\qquad\quad a^8 = a^7 \cdot a = a^5 + a^4 + a^2 + 1 \neq 1 \checkmark \\
&\longrightarrow \quad a^9 = a^8 \cdot a = a^3 + a^2 + 1 \neq 1 \checkmark \\
&\qquad\quad a^{16} = a^8 \cdot a^8 = a^5 + a^4 + a^3 + a^2 + a \neq 1 \checkmark \\
&\longrightarrow \quad a^{21} = a^{16} \cdot a^5 = a^5 + a^3 + a^2 \neq 1 \checkmark \\
&\implies a^{63} = 1 \checkmark
\end{aligned}$$

Therefore a as a generator of $\mathbb{Z}_2[x]/p(x) \setminus \{0\}$ and with $p(a) = 0$ exists.

$\implies$ $p(x)$ is primitive

✔ **Approved by arch user**

done the same way

✨ **Solution for 3.1 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$** ✨

Theory

Polynomial $p(x)$ is primitive in $\mathbb{Z}_2 \iff$
1. $p(x)$ is irreducible
2. $\exists a \in (\mathbb{Z}_2[x]/p(x)) \setminus \mathbf{0} : p(a) = 0 \wedge \{a^k | \ k \in \mathbb{Z}\} = (\mathbb{Z}_2[x]/p(x)) \setminus \mathbf{0}$

1st order: No linear factors

2nd and 3rd order see solution acrobatic aviator

Ireducible ✓

Let $a \in (\mathbb{Z}_2[x]/p(x)) \setminus \mathbf{0} \wedge p(a) = 0 \overset{!}{\Longrightarrow} \{a^k |\ k \in \mathbb{Z}\} = (\mathbb{Z}_2[x]/p(x)) \setminus \mathbf{0}$

Group order: 64
Without 0: 63

$63 = 7 \cdot 3 \cdot 3$

relevant $k \in \{7, 3, 9, 21\}$

Check $a^k \overset{!}{\neq} 1$

$$p(a) = 0 = a^6 + a^5 + a^2 + a + 1$$
$$a^6 = a^5 + a^2 + a + 1$$

rest see acrobatic aviator

😀🔫

3.2

Compute the number of integers x with $1 \leq x \leq 1000000$ where x is neither a square nor a 3rd, 4th or 5th power of some positive integer y.

✨ Solution for 3.2 by arch user ✨

$$N_0 = \{x \in \mathbb{Z} \mid 1 \leq x \leq 10^6\} \text{... all numbers}$$

$$N_2 = \{x \in N_0 \mid x = \sqrt[2]{y}\}, \quad |N_2| = \sqrt[2]{10^6} \text{... numbers with a perfects root of 2}$$

$$N_3 = \{x \in N_0 \mid x = \sqrt[3]{y}\}, \quad |N_3| = \sqrt[3]{10^6} \text{... numbers with a perfects root of 3}$$

$$N_5 = \{x \in N_0 \mid x = \sqrt[5]{y}\}, \quad |N_5| = \sqrt[5]{10^6} \text{... numbers with a perfects root of 5}$$

$$N_4 \text{... not important because already included in } N_2$$

Principle of Inclusion-Exclusion:

$$N = |N_0| - |N_2| - |N_3| - |N_5| + |N_2 \cap N_3| + |N_2 \cap N_5| + |N_3 \cap N_5| - |N_2 \cap N_3 \cap N_5|$$

with

$$\text{e.g. } N_2 \cap N_3 = N_{23} = \{x \in N_0 \mid x = \sqrt[2]{y} \wedge x = \sqrt[3]{y}\}$$

$$|N_{23}| = \sqrt[2 \cdot 3]{10^6} = \sqrt[6]{10^6}$$

$$|N_{25}| = \sqrt[2 \cdot 5]{10^6} = \sqrt[10]{10^6}$$

$$\dots$$

$$|N| = |N_0| - |N_2| - |N_3| - |N_5| + |N_{23}| + |N_{25}| + |N_{35}| - |N_{235}|$$

✨ Solution for 3.2 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

$n_k = \left|\{x \in (1, 10^6) | \ x = y^k, y \in \mathbb{Z}\}\right|$

$\#x = 1000000 - n_2 - n_3 - n_5 + n_{2 \cdot 3} + n_{2 \cdot 5} + n_{3 \cdot 5} - n_{2 \cdot 3 \cdot 5}$

$$n_2 = \sqrt{10^6} = 1000$$

$$n_3 = \sqrt[3]{10^6} = 100$$

$$n_5 = \left\lfloor \sqrt[5]{10^6} \right\rfloor = \left\lfloor \sqrt[5]{10^5 10} \right\rfloor = \left\lfloor 10 \sqrt[5]{10} \right\rfloor = 15 \text{ (How to calc without calculator?)}$$

$$n_{2 \cdot 3} = 10$$

$$n_{2 \cdot 5} = 3$$

$$n_{3 \cdot 5} = 2$$

$$n_{2 \cdot 3 \cdot 5} = 1$$

$\#x = 998899$

3.3

For any simple, undirected graph G, prove via induction over $\alpha_0(G)$, that the following holds: $\chi(G) \leq 1 + \max_{v \in V} d(v)$.

✨ Solution for 3.3 by BlauBarschBube ✨

Let $\alpha_0(G) = 1$:
Then $\chi(G) = 1 \leq 1 + 0$

$$\text{Let} \quad \alpha_0(G) = n + 1$$
$$\text{Let} \quad \Delta(G) = \max_{\{v \in G\}} d(v)$$

Take out a vertex v to make new Graph G' with $\alpha_0(G') = n$

$$\text{Then} \quad \chi(G') \leq 1 + \Delta(G')$$
$$\Delta(G') \leq \Delta(G)$$
$$\text{So} \quad \chi(G') \leq 1 + \Delta(G)$$

G' can be colored in at most $1 + \Delta(G)$ colors.
Consider the removed vertex v: $\deg(v) \leq \Delta(G)$
$\Rightarrow$ it has at most $\Delta(G)$ neighbours
$\Rightarrow$ it can be colored in one of the $1 + \Delta(G)$ colors
$\Rightarrow$ G is properly colored
$\Rightarrow \chi(G) \leq 1 + \Delta(G)$

✨ Solution for 3.3 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

Theory

$$\alpha_0(G) = |V|$$
$\chi(G)$... Chromatic Number

Induction hypothesis: $\chi(G) \leq 1 + \max_{v \in V} d(v)$

Induction base:

$$\alpha_0(G) = 1$$
$$\chi(G) = 1$$
$$\max_{v \in V} d(v) = 0$$

$$\chi(G) \leq 1 + \max_{v \in V} d(v)$$
$$1 \leq 1 + 0 \checkmark$$

Induction step:

$$G' = (V', E')$$
$$V' = V \cup \{v'\}$$

For $\alpha_0(G) = k : \chi(G) \leq 1 + \max_{v \in V} d(v) \overset{!}{\Longrightarrow} \alpha_0(G') = k+1 : \chi(G') \leq 1 + \max_{v \in V'} d(v)$

By adding a vertex $v' : \chi(G') - \chi(G) = \begin{cases} 1 \text{ if } v' \text{ has edge to vertices of all colors in G (new color will be assigned to } v' \\ 0 \text{ otherwise (Color of vertex } v_u \in V : \nexists v' v_u \in E' \text{ can be used)} \end{cases}$

- Case $\chi(G') - \chi(G) = 0$ trivially correct since $\max_{v \in V'} d(v)$ is not less than for G since we do not remove edges ✓
- Case $\chi(G') - \chi(G) = 1$:
  $\forall c \in \text{colors of } V \exists uv' \in E' : \text{color}(u) = c \Rightarrow d(v') = \chi(G) \Rightarrow \max_{v \in V'} d(v) \geq \chi(G)$

$$\begin{aligned} \chi(G) &\leq \max_{v \in V'} d(v) && \mid +1 \\ \chi(G) + 1 &\leq 1 + \max_{v \in V'} d(v) && (\chi(G') - \chi(G) = 1 \Rightarrow \chi(G') = \chi(G) + 1) \\ \chi(G') &\leq 1 + \max_{v \in V'} d(v) \end{aligned}$$

✨ Solution for 3.3 by acrobatic aviator ✨

Theory

α_0 ... Number of vertices

- Induction base: $\alpha_0(G) = 0 \Longrightarrow \chi(G) = 0,\ 1 + \max_{v \in V} d(v) = 1$ ✓
- Induction step:
  - **to prove**: equation true for $\alpha_0 = n \Longrightarrow$ equation true for $\alpha_0 = n + 1$

    Let G' be a graph with $\alpha_0(G') = n$, add one vertex (v_{new})and call that graph $G \Longrightarrow \alpha_0(G) = n + 1$

    Then we can look at the two following cases:

    1. $\chi(G) = \chi(G') + 1$

       This means, that the new vertex got a new color.

       $\Longrightarrow$ the vertex must be connected to at least one of vertex of each color in G' to receive a new one

       $\Longrightarrow d(v_{\text{new}}) \geq \chi(G') = \chi(G) - 1$

       $\Longrightarrow 1 + \max_{v \in V} d(v) \geq 1 + d(v_{\text{new}}) \geq \chi(G)$ ✓

    2. $\chi(G) = \chi(G')$

       This means, that the new vertex did **not** get a new color.

       $\Longrightarrow d(v_{\text{new}}) < \chi(G') = \chi(G)$

       $\Longrightarrow d(v_{\text{new}}) + 1 \leq \chi(G) = \chi(G') \leq 1 + \max_{v \in V'} d(v)$

       $\Longrightarrow d(v_{\text{new}}) \leq \max_{v \in V'} d(v)$

       $\Longrightarrow$ The max-degree of the graph will not increase by adding v_{new}

       $\Longrightarrow \max_{v \in V'} d(v) = \max_{v \in V} d(v)$

       $\chi(G') \leq 1 + \max_{v \in V'} d(v) \Longleftrightarrow \chi(G) \leq 1 + \max_{v \in V} d(v)$ ✓

✔ Approved by arch user

done the same way

3.4

Use the Chinese Remainder Theorem to solve the following system of congruence relations:

$$\begin{aligned} 3x &\equiv 12 \bmod 13 \\ 5x &\equiv 7 \bmod 22 \\ 2x &\equiv 3 \bmod 7 \end{aligned}$$

✨ Solution for 3.4 by arch user ✨

I think we have done enough CRT to understand it, even thou this example is very brain-resource intense...

$$x \equiv 173 \bmod 2002$$

✨ Solution for 3.4 by BlauBarschBube ✨

$$\begin{aligned} \gcd(3, 13) &= 1 \\ \gcd(5, 22) &= 1 \\ \gcd(2, 7) &= 1 \end{aligned}$$

So we dont need to divide by the gcd and the system of congruences is solvable as $\forall i \in \{1, 2, 3\} : a_i \cdot x \equiv b_i \bmod n_i : \gcd(a, n) \mid b$
Finding and multiplying by inverses yields

$$\begin{aligned} x &\equiv 4 \bmod 13 \\ x &\equiv 19 \bmod 22 \\ x &\equiv 5 \bmod 7 \end{aligned}$$

Furthermore:

$$\begin{aligned} \gcd(13, 22) &= 1 \\ \gcd(13, 7) &= 1 \\ \gcd(22, 7) &= 1 \end{aligned}$$

So CRT is applicable with modulo $13 \cdot 22 \cdot 7 = 2002$

$$\begin{aligned} x &\equiv \overbrace{22 \cdot 7 \cdot 6}^{\bmod 13} \cdot 4 + \overbrace{13 \cdot 7 \cdot 15}^{\bmod 22} \cdot 19 + \overbrace{13 \cdot 22}^{\bmod 7} \cdot 2 \bmod 2002 \\ &\equiv 3696 + 25935 + 8580 \bmod 2002 \\ &\equiv 1694 + 1911 + 572 \bmod 2002 \\ &\equiv 3605 + 572 \bmod 2002 \\ &\equiv 1603 + 572 \bmod 2002 \\ &\equiv 2175 \bmod 2002 \\ &\equiv 173 \bmod 2002 \end{aligned}$$

✔ Approved by arch user

Thanks for writing it down

4 2023-04-12 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_Exam_2023-04-12

4.1

In a room there are m chairs and n people ($n \leq m$). The people take a break and leave the room. How many ways can the n people sit on the m chairs such that no one sits on the same chair as before the break.

✨ Solution for 4.1 by arch user + god ✨

Principle of Inclusion-Exclusion:

$$= n! \cdot \binom{m}{n} + \sum_{i}^{n} (-1)^i \binom{n}{i} \cdot \binom{m-i}{n-i} \cdot (n-i)!$$

Explanation:

$$n! \cdot \binom{m}{n} \text{... all options (ordered)}$$

$$\sum_{i=1}^{n} \text{...} i \text{ people sit at the same chair as before}$$

$$(-1)^i \text{... exclude because doubled counted same sitting people}$$

$$\binom{n}{i} \text{... options to choose } i \text{ people who sit wrong (unordered, since we cannot reorder them)}$$

$$\binom{m-i}{n-i} \cdot (n-i)! \text{... options to choose right sitting people (ordered)}$$

✔ Approved by acrobatic aviator

✨ Solution for 4.1 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

$$= n!\binom{m}{n} + \sum_{i=1}^{n} \left((-1)^i \underbrace{\binom{n}{i}}_{\#\text{ i fixed people of n}} \cdot \overbrace{\binom{m-i}{n-i}}^{\#\text{ n-i people take m-i remaining chairs}} (n-i)! \right)$$

4.2

Let R be an integral domain. Two elements a, b of R are called associated if $a = b * r$ with r being a unit (so element of R^*). Prove that two elements x, y of R are associated if and only if $x|y$ and $y|x$.

✨ Solution for 4.2 by arch user ✨

📖 Theory

Integral Domain
- commutative ring with 1
- no zero-divisors

$$x = r \cdot y \Leftrightarrow x \mid y \wedge y \mid x$$
$$x \mid y \Rightarrow y = x \cdot k,\ k \in R$$
$$y \mid x \Rightarrow x = y \cdot l,\ l \in R$$
einsetzen
$$y = y \cdot l \cdot k$$
$$\Leftrightarrow l \cdot k = 1$$
$$\Leftrightarrow l = k^{-1}$$
$$\Leftrightarrow l, k \in R^* \text{ (they have inverse so the are units)}$$

$$x = l \cdot y,\ l \in R^*$$
$$y = k \cdot x,\ k \in R^*$$
$$x \sim y \quad \square$$

✨ Solution for 4.2 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

$$x \mid y \Rightarrow y = kx,\ k \in R$$
$$y \mid x \Rightarrow x = ly,\ l \in R$$
$$\Longrightarrow$$
$$x = lkx,\ l, k \in R$$
$$\Rightarrow l, k \in R^*$$
$$\Longrightarrow x \mid y \wedge y \mid x \Rightarrow a, b \text{ associated}$$

$$x = y * r,\ r \in R^*$$
$$\Rightarrow y = x * r^{-1}$$
$$\Longrightarrow x, y \text{ associated} \Rightarrow x \mid y \wedge y \mid x$$

4.3

Let I be an integral domain. Define $a \sim b$ the equivalence relation as $a - b \in I$. Prove that $\sim$ is an equivalence relation. Furthermore show that $[x]$ (which is the set of all elements related to x) is equal to $x + I$ (or something similar to this)

Missing Details

Maybe some details in the tasks are missing: problem could be too easy or unsolvable!

4.4

Show that $\sqrt{3}+i$ is algebraic over $\mathbb{Q}$ and determine its primitive polynomial.

✨ Solution for 4.4 by arch user ✨

algebraic: there must be a $p(x)$ in $\mathbb{Q}[x]$ which has $\sqrt{3}+i$ as its root

$$\left(\sqrt{3}+i\right)^2 = 2+2\sqrt{3}i$$
$$\left(\sqrt{3}+i\right)^3 = 8i$$
$$\left(\sqrt{3}+i\right)^4 = i\sqrt{3}i-8$$

build $p(x)$ so it is zero with $\sqrt{3}+i$

$$p(x) = x^4 - 4x^2 + 16$$

Is it irreducible?
check if it can be build with two polynomials

- $\deg(r(x)) = 1 \wedge \deg(s(x)) = 3$... not possible because a $\sqrt{3}+i$ has no linear root
- only two polynomials with deg $= 2$ possible (both of them are monic again)

$$\begin{aligned} p(x) &= r(x)\cdot s(x) \\ x^4 - 4x^2 + 16 &= (x^2+ax+b)\cdot(x^2+cx+d) \quad \text{with} \quad a,b,c,d \in \mathbb{Q} \\ &= x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd \end{aligned}$$

this gives the following systems of equations:

$$\begin{aligned} a+c &= 0 \\ b+d+ac &= -4 \\ ad+bc &= 0 \\ bd &= 16 \\ &\Rightarrow \\ -cd^2+16c &= 0 \\ c(16-d^2) &= 0 \end{aligned}$$

Case 1: $c = 0$

$$\begin{aligned} a &= 0 \\ b &= d-4 \\ d^2+4d+16 &= 0 \end{aligned}$$

d cannot be $\in \mathbb{Q}$ (no root in $\mathbb{Q}$).

Case 2: $16-d^2 = 0 \wedge d = 4$

$$b = 4, a\cdot c = -12 \Rightarrow -c^2 = -12 \Rightarrow c^2 = 12$$

Case 3: $16-d^2 = 0 \wedge d = -4$

$$d = -4, b = -4, a\cdot c = 4 \Rightarrow -c^2 = 4 \Rightarrow c^2 = -4$$

In both cases (2,3) $c \notin \mathbb{Q}$ so $p(x)$ is not reducible to two factors of degree 2. $\Rightarrow$ **irreducible**

✨ Solution for 4.4 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

Theory

algebraic over $\mathbb{Q}$ means that it is a root of a polynomial of $\mathbb{Q}[x]$

$$\begin{aligned}\left(\sqrt{3}+i\right)^2 &= 3+2i\sqrt{3}-1 \quad = 2+2\sqrt{3}i\\ \left(\sqrt{3}+i\right)^4 &= 4+8i\sqrt{3}-12 = -8+8\sqrt{3}i\end{aligned}$$

$$\left(\sqrt{3}+i\right)^4 - 4\left(\sqrt{3}+i\right)^2 + 16 = 0$$

$$p(x) = x^4 - 4x^2 + 16$$

Test if $p(x)$ is irreducible
Second degree only since root is not in $\mathbb{Q}$

$$(x^2+bx+c)(x^2+dx+e) = x^4+dx^3+ex^2+bx^3+bdx^2+bex+cx^2+cdx+ce$$

$$\begin{aligned}0 &= d+b\\ -4 &= e+bd+c\\ 0 &= be+cd\\ 16 &= ce\end{aligned}$$

$$b = -d$$

$$0 = b^2(e-c) \Rightarrow \begin{cases} b=0 \Rightarrow e+c=-4 \wedge ce=16 \lightning \\ e-c=0 \Rightarrow e=c=4 \Rightarrow b^2=12 \lightning \end{cases}$$

$\lightning$ $p(x)$ is irreducible.

$p(x)$ is monic.

$\Longrightarrow$ $p(x)$ is primitive polynom

5 2023-01 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_Exam_2023-01

5.1

Solve:

$$\begin{aligned} x^2 &\equiv 1 \bmod 4 \\ 3x &\equiv 4 \bmod 5 \\ 6x &\equiv 3 \bmod 9 \end{aligned}$$

✨ Solution for 5.1 by arch user ✨

First check if CRT is allowed:

$$\gcd(4,5) = 1 \wedge \gcd(4,9) = 1 \wedge \gcd(5,9) = 1 \Rightarrow \text{ CRT is allowed}$$

first we see, that in the 3rd equation we can cancel a factor 3.

$$\begin{aligned} x^2 &\equiv 1 \bmod 4 \\ 3x &\equiv 4 \bmod 5 \\ 2x &\equiv 1 \bmod 3 \end{aligned}$$

$$\begin{aligned} x^2 &\equiv 1 \bmod 4 \\ x &\equiv 4 \cdot 3^{-1} \bmod 5 \\ x &\equiv 1 \cdot 2^{-1} \bmod 3 \end{aligned}$$

to solve the equation with $x^2 \equiv 1 \bmod 4$ we need to check which square of an element in $\mathbb{Z}_4$ is 1. $0^1 = 0, 1^2 = 1, 2^2 = 0, 3^2 = 1$ which leads to the conclusion, that x^2 has two solutions in $\mathbb{Z}_4$. This means we have to do a case distinction and we'll have to solutions in the end ($a_{1,1} = 1$ and $a_{1,2} = 3$).
Else proceed with the normal CRT:

$$\begin{aligned} a_2 &= 3 \\ a_3 &= 2 \\ b_i &\equiv \left(\frac{m}{m_i}\right)^{-1} \bmod m_i \\ b_1 &\equiv 3 \bmod 4 \\ b_2 &\equiv 3 \bmod 5 \\ b_3 &\equiv \bmod 3 \end{aligned}$$

Case $a_{1,1}$:

$$\begin{aligned} x_1 &\equiv 1 \cdot 3 \cdot (5 \cdot 3) + 3 \cdot 3(4 \cdot 3) + 2 \cdot 2(4 \cdot 5) \bmod 4 \cdot 5 \cdot 3 \\ &\equiv 53 \bmod 60 \end{aligned}$$

Case $a_{1,2}$:

$$\begin{aligned} x_2 &\equiv 3 \cdot 3 \cdot (5 \cdot 3) + 3 \cdot 3(4 \cdot 3) + 2 \cdot 2(4 \cdot 5) \bmod 4 \cdot 5 \cdot 3 \\ &\equiv 23 \bmod 60 \end{aligned}$$

✨ Solution for 5.1 by acrobatic aviator ✨

This is a solution without the case distinction from arch user.

Divide out the common factor 3 from the third equation:

$$2x \equiv 1 \bmod 3$$

To solve the square in the first equation, look at the solutions in $\mathbb{Z}_4$ for this.

$$\begin{aligned} 0^2 \bmod 4 &\equiv 0 \neq 1 \\ 1^2 \bmod 4 &\equiv 1 \\ 2^2 \bmod 4 &\equiv 0 \neq 1 \\ 3^2 \bmod 4 &\equiv 1 \\ \implies x &\equiv 1 \bmod 2 \end{aligned}$$

So the system to solve is the following (after calculating the needed inverses):

$$\begin{aligned} 1: &\quad x \equiv 1 \bmod 2 \\ 2: &\quad x \equiv 3 \bmod 5 \\ 3: &\quad x \equiv 2 \bmod 3 \end{aligned}$$

CRT can be done since all modulos are prime.

... do CRT ...

$$x \equiv 23 \bmod 30$$

✨ Solution for 5.1 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

Check out first congruence:

$$\begin{aligned} 0^2 &\equiv 0 \bmod 4 \\ 1^2 &\equiv 1 \bmod 4 \\ 2^2 &\equiv 0 \bmod 4 \\ 3^2 &\equiv 1 \bmod 4 \\ \implies & \\ x &\equiv 1 \bmod 2 \end{aligned}$$

Simplify first congruence:

$$\begin{aligned} 6x \equiv 3 \bmod 9 \quad &\mid \div 3 \\ 2x \equiv 1 \bmod 3 \quad &\mid \cdot 2 \\ x \equiv 2 \bmod 3 & \end{aligned}$$

Congruences:

$$\begin{aligned} x &\equiv 1 \bmod 2 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 2 \bmod 3 \end{aligned}$$

$$\begin{aligned} m &= 30 \\ b_1 &= 1 \\ b_2 &= 1 \\ b_3 &= 1 \end{aligned}$$

$$x \equiv 15 + 18 + 20 \bmod 30 \equiv 23 \bmod 30$$

5.2

Prove (E, S) with $|E| = n$ and $S = \{X \subseteq E : |X| \leq m\}$ is a matroid

✨ Solution for 5.2 by arch user ✨

💻 Theory

Matroid Properties

1. $\forall x : \forall y \subseteq x \in S$
2. $\forall A, B \in S : |B| = |A| + 1$
   $\Rightarrow v \in B \setminus A : A \cup \{v\} \in S$

❗ Correction by BlauBarschBube

Missing property

1. $S \neq \emptyset$

The smallest possible S is when

$$\begin{aligned} m &= 0, \text{but} \\ |\emptyset| &= 0 \\ &\Rightarrow \emptyset \in S \\ &\Rightarrow S \neq \emptyset \end{aligned}$$

💻 Theory

A powerset is closed under inclusion

✏️ Assumption (by us)

$m \leq n$

ad property 1:

$$\begin{aligned} A \in S &\Rightarrow |A| \leq m \\ B &\subseteq A \\ |B| &\leq |A| \\ &\Rightarrow |B| \leq m \\ \Rightarrow B &\in S \quad \square \end{aligned}$$

ad property 2:

$$|B| = |A| + 1, v \in B \setminus A$$
$$\text{to show: } A \cup \{v\} \in S :$$
$$A \cup \{v\} \subset E \land |A \cup \{v\}| \leq m$$
$$A \subset E, v \in B, B \subset E$$
$$\Rightarrow v \in B \subset E \Rightarrow v \in E \quad \square$$
$$\text{check size property:}$$
$$|B| := k \leq m$$
$$|A| = |B| - 1 = k - 1 < m$$
$$\Rightarrow |A \cup \{v\}| = |A| + 1 = k - 1 + 1 = k \leq m \quad \square$$

✔ Approved by acrobatic aviator

The assumption always holds.

if $m \geq n$, redefine m to be n. This does not change anything, since there are no subsets with a size greater than the base set.

✨ Solution for 5.2 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

✏ Assumption (by us)

$m \geq 0$

Assumption implies $S \neq \emptyset$

Take $A, B \in S : |A| + 1 = |B|$

Take any element $x \in B \setminus A$ then $\{x\} \cup A \in S$ since all subsets of E with size $\leq m$ are in S. Since A is at most $m - 1 \exists A' \in S : A' = A \cup \{x\}$

Furthermore $\forall X \in S : \forall Y \subseteq X : Y \in S$ per construction.

5.3

Show that for a set of distinct numbers $A \subset \{1...15\}$ of size 8, there always exist two numbers which sum up to 16

✨ Solution for 5.3 by arch user ✨

✏️ Assumption (by us)

The two numbers used for the sum to 16 do not have to be different numbers.
Otherwise, $\{1, 2, ..., 8\}$ would be a counterexample.

$$|\{1...15\}| = 15$$
$$|\{1...7\}| = 7 \Rightarrow \exists a \geq 8$$
(there exists one number in out set which is greater or equal to 8)

pairs: how to build 16 with two numbers:

$1 + 15$
$2 + 14$
$3 + 13$
$4 + 12$
$5 + 11$
$6 + 10$
$7 + 9$
8

Case 1:
$8 \in A \Rightarrow 16 = 8 + 8$ □
Case 2:

$$8 \notin A \Rightarrow |A| = 8 \text{ (still)}$$

that means that we must have taken at least one complete pair (its red and blue part)

📖 Theory

Pigeonhole Principle

✨ Solution for 5.3 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

Counterexample: $\{1, 2, 3, 4, 5, 6, 7, 8\} = A \subset \{1, ..., 15\}$
No two numbers add up to 16 since the largest possible sum out of 2 is $7 + 8 = 15$

5.4

Prove if $\mathbb{Z}_3/(x^2+x+1)$ is a field, list all elements.
Is $x+1$ a unit? If yes, give its multiplicative inverse.

✨ Solution for 5.4 by arch user ✨

All elements in this quotient ring:

$$\mathbb{Z}_3/p(x) = \{\forall q(x) \text{ of degree } \leq 1 \mid a_0, a_1 \in \mathbb{Z}_3\}$$

if the degree of $q(x)$ would be bigger than > 2, then it could be divided by $p(x)$ again. Only the remainder is left.

is it a field?

- $\mathbb{Z}_3$ is a field
- $\Rightarrow p(x)$ has to be **irreducible**
  - $p(0) = 1$
  - $p(1) = 0$ this is a root $\Rightarrow$ not irreducible

$p(x) = x^2+x+1$ is a reducible polynomial $\Rightarrow \mathbb{Z}_3/p(x)$ is not a field.

Is $x+1$ a unit? to check, try to calculate the inverse of it
What is it the inverse of $x+1$?

$$(x+1)^{-1} = ?$$
$$(x+1)\cdot q(x) \equiv 1 \bmod p(x)$$

Polynomial Division:

$$\begin{array}{l} x^2+x+1 : x+1 = \mathrm{x} \\ x^2+x \\ \text{---} \\ +1 \quad \text{(constant rest is ok)} \end{array}$$

To get the inverse of $x+1$ we take the result from the divison and multiply it with the negative inverse of the rest:

$$\begin{aligned} (x+1)^{-1} &= -(1)^{-1}\cdot \mathrm{x} \\ &= -x \\ &= 2x \end{aligned}$$

✨ Solution for 5.4 by acrobatic aviator ✨

$$\mathbb{Z}_3/x^2+x+1 = \{\{(x^2+x+1)\cdot q(x) + r(x) \mid q(x) \in \mathbb{Z}_3[x]\} \mid r(x) = ax+b \text{ with } a,b \in \mathbb{Z}_3\}$$
$$\mathbb{Z}_3/x^2+x+1 = \{\overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2}\}$$

📖 Theory

$K/p(x)$ is field $\iff$ $p(x)$ irreducable on $K[x]$

to prove: x^2+x+1 irreducable on $\mathbb{Z}_3[x]$

$$\begin{aligned} p(x) = x^2 + x + 1 &= (ax + b)(cx + d) \\ &= ac \cdot x^2 + (ad + bc) \cdot x + bd \end{aligned}$$

$$\begin{aligned} \implies ac = \overline{1} &\Rightarrow a = c^{-1} \land c = a^{-1} \land a \neq \overline{0} \land c \neq \overline{0} \\ bd = \overline{1} &\Rightarrow b = d^{-1} \land d = b^{-1} \land b \neq \overline{0} \land d \neq \overline{0} \\ ad + bc = \overline{1} &\Rightarrow ab^{-1} + ba^{-1} = \overline{1} \end{aligned}$$

try $a = \overline{1} \Rightarrow a^{-1} = \overline{1}$:

$$\begin{aligned} b + b^{-1} = \overline{1} &\implies b = \overline{2} \\ \implies a = c = \overline{1};\ b = d &= \overline{2} \end{aligned}$$

$$\begin{aligned} \implies x^2 + x + 1 &= (x + 2)(x + 2) \\ &= x^2 + 2 \cdot 2 \cdot x + 4 = x^2 + x + 1 \end{aligned}$$

$\implies p(x)$ is **not** irreducable on $\mathbb{Z}_3[x]$

$\implies \mathbb{Z}_3[x]/x^2 + x + 1$ is **not** a field

Therefore, the inverse of $(x + 1)$ does not necessarily exist. But let's check it anyways.

$$\begin{aligned} x^2 + x + 1 &\equiv (x + 1) \cdot x + 1 \\ 1 &\equiv (x^2 + x + 1) + (x + 1)(-x) \\ 1 &\equiv (x^2 + x + 1) + (x + 1)(2x) \\ \implies (x + 1)^{-1} &\equiv 2x \end{aligned}$$

Just to check if that is actually correct:

$x^2 + x + 1 \equiv 0 \implies x^2 \equiv 2x + 2$

$$\begin{aligned} (x + 1) \cdot 2x &\equiv 2x^2 + 2x \\ &\equiv 4x + 4 + 2x \equiv 1 \ \checkmark \end{aligned}$$

✨ Solution for 5.4 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

Theory

$\mathbb{Z}_3/(x^2 + x + 1)$ is field $\Leftrightarrow \mathbb{Z}_3$ is field $\land$ $(x^2 + x + 1)$ is irreducible

1. $\mathbb{Z}_3$ is field ✓

$$\begin{aligned} (x + a)(x + b) &= x^2 + ax + bx + ab \\ ab = 1 &\Rightarrow a, b \neq 0 \\ a + b = 1 &\Rightarrow a = b = 2 \end{aligned}$$

$\Rightarrow$ polynomial is reducible

$\implies \mathbb{Z}_3/(x^2 + x + 1)$ is not field $\mathbb{Z}_3/(x^2 + x + 1) = \left\{\overline{ax + b} \mid a, b \in \mathbb{Z}_3\right\}$

2. Is $x + 1$ a unit?

$$x^2 + x + 1 = (x+1) \cdot x + 1 \Longrightarrow 1 = (x^2 + x + 1) - (x+1)(x)$$
$$(x+1) \cdot (2x) = 2x^2 + 2x \equiv 1 \bmod x^2 + x + 1$$

$x + 1$ is unit

3. $(x+1)^{-1} = (2x)$

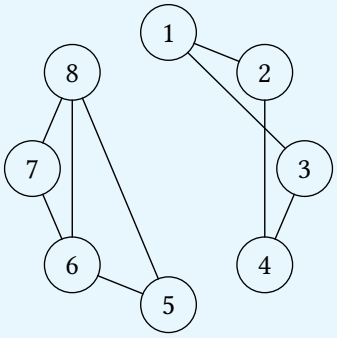
6 2022-11-25 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_Exam_2022-11-25

6.1

Compute the number of spanning trees of the given Graph $G = (V, E), V = \{1...8\}$ and $E = \{(1,2),(1,3),(2,4),(3,4),(5,8),(5,6),(6,8),(6,7),(7,8)\}$.

✨ Solution for 6.1 by arch user ✨



Graph on the left is called G_1, on the right G_2 (same for all matrices)

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad D_1 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

now cross one line and column of each matrix

$$\det(D_1' - A_1') = \begin{vmatrix} 2 & -1 & 0 \\ -1 & 3 & -1 \\ 0 & -1 & 2 \end{vmatrix} = 2 \cdot \begin{vmatrix} 3 & -1 \\ -1 & 2 \end{vmatrix} + (-1) \cdot \begin{vmatrix} -1 & -1 \\ 0 & 2 \end{vmatrix} \cdot (-1)^{2+1}$$

$$= 10 - 2 = 8$$

$$A_2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad D_2 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

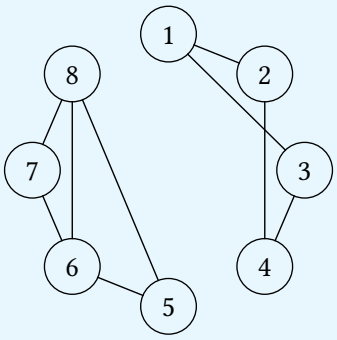
now cross one line and column of each matrix

$$\det(D_2' - A_2') = \begin{vmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{vmatrix} = 2 \cdot \begin{vmatrix} 2 & -1 \\ -1 & 2 \end{vmatrix} + (-1) \cdot \begin{vmatrix} 0 & -1 \\ 2 & -1 \end{vmatrix} \cdot (-1)^{3+1}$$

$$= 4$$

The number of the spanning forests in total is the number of the spanning trees of each single graph multiplied: $8 \cdot 4 = 32$

✨ Solution for 6.1 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨



$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \qquad D = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$D_1 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \qquad D_2 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

$$D_1 - A_1 = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 2 & 0 & -1 \\ -1 & 0 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix} \qquad D_2 - A_2 = \begin{pmatrix} 2 & -1 & 0 & -1 \\ -1 & 3 & -1 & -1 \\ 0 & -1 & 2 & -1 \\ -1 & -1 & -1 & 3 \end{pmatrix}$$

$$(D_1 - A_1)' = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix} \qquad (D_2 - A_2)' = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 3 & -1 \\ 0 & -1 & 2 \end{pmatrix}$$

$$\det\big((D_1 - A_1)'\big) = \begin{vmatrix} 2 & -1 & -1 \\ -1 & 2 & 0 \\ -1 & 0 & 2 \end{vmatrix} = \qquad \det\big((D_2 - A_2)'\big) = \begin{vmatrix} 2 & -1 & 0 \\ -1 & 3 & -1 \\ 0 & -1 & 2 \end{vmatrix} =$$

$$= 8 - 2 - 2 = 4 \qquad = 12 - 2 - 2 = 8$$

Not connected graphs have 0 spanning trees.

✏️ Assumption (by us)

Looking for # spanning forest

$8 \cdot 4 = 32$

There are 32 spanning forest

✏️ Assumption (by us)

Looking for # spanning trees of subgraphs of G

$8 + 4 = 12$

There are 12 spanning trees subgraph of G

6.2

Compute the value of $\mu(0, 1)$ for the given Hasse diagram

⚠ Not Relevant

Not in the 6 ECTS version of *Discrete Math*

6.3

Solve the following recurrence relation using generating functions (*something like this*)
$a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n = 1$ with $a_0 = 1, a_1 = 3, a_2 = 0$

Comment by arch user

Error in the given formula from vowi, but fixed here

✨ Solution for 6.3 by arch user ✨

✏️ Assumption (by us)

given formula is correct and nothing is missing, changed $+a_n$ to $-a_n$ from vowi (else it's not possible)

$$a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n = 1$$

$$\frac{1}{z^3}\sum_{n\geq 0}(a_{n+3}z^{n+3}) - \frac{3}{z^2}\sum_{n\geq 0}(a_{n+2}z^{n+2}) + \frac{3}{z}\sum_{n\geq 0}(a_{n+1}z^{n+1}) - \sum_{n\geq 0}(a_n z^n) = \sum_{n\geq 0}(z^n)$$

$$\frac{1}{z^3}\sum_{n\geq 3}(a_n z^n) - \frac{3}{z^2}\sum_{n\geq 2}(a_n z^n) + \frac{3}{z}\sum_{n\geq 1}(a_n z^n) - \sum_{n\geq 0}(a_n z^n) = \sum_{n\geq 0}(z^n)$$

$$\frac{1}{z^3}(A(z) - a_2z^2 - a_1z - a_0) - \frac{3}{z^2}(A(z) - a_1z - a_0) + \frac{3}{z}(A(z) - a_0) - A(z) = \frac{1}{1-z}$$

$$\frac{A(z) - 3z - 1}{z^3} - 3\frac{A(z) - 3z - 1}{z^2} + 3\frac{A(z) - 1}{z} - A(z) = \frac{1}{1-z} \qquad |\cdot z^3$$

...

$$A(z)(-z^3 + 3z^2 - 3z + 1) + 6z^2 - 1 = \frac{z^3}{1-z}$$

$$A(z)(1-z)^3 + 6z^2 - 1 = \frac{z^3}{1-z}$$

$$A(z) = \frac{7z^3 - 6z^2 - z + 1}{(1-z)^4}$$

partial fraction decomposition ....

$$A(z) = -\frac{7}{1-z} + \frac{15}{(1-z)^2} - \frac{8}{(1-z)^3} + \frac{1}{(1-z)^4}$$

$$A(z) = \sum_{n\geq 0}\left(-7\binom{n}{0}z^n + 15\binom{n+1}{1}z^n - 8\binom{n+2}{2}z^n + \binom{n+3}{3}z^n\right)$$

$$\Rightarrow a_n = -7\binom{n}{0} + 15\binom{n+1}{1} - 8\binom{n+2}{2} + \binom{n+3}{3}$$

6.4

Show the identity:

$$\sum_{k=0}^{n}\binom{m+k}{k}=\binom{n+m+1}{m+1}$$

using combinatorial interpretation.
⚠️ **Hint:** Consider $\{0,1\}$ sequences and group them according to the position of the last 1.

✨ Solution for 6.4 by arch user ✨

$\binom{a}{b}$ can calculate the number of permutations of $b \times$ `1`s in a a-bit string.

Left Side $\sum_{k=0}^{n}\binom{m+k}{k}$**:**

- m... starting length of the bit string
- n... new added elements

Example with $n=3, m=4$

$$k=0: \quad \underbrace{\bigcirc\bigcirc\bigcirc\bigcirc\bigcirc}_{m \text{ times}}\underbrace{\square\square\square}_{n \text{ times}}$$

$$k=1: \quad \underbrace{\bigcirc\bigcirc\bigcirc\bigcirc\bigcirc}_{m \text{ times}}\underbrace{\square}\ \underbrace{\square\square}_{n-1 \text{ times}}$$

If we have a bit vector, we are not able to see m or n from it, therefore we fill all m bits with `0`s and all n `1`s (if we take them).

Right Side $\binom{n+m+1}{m+1}$**:**
🚧 **Work in Progress** 🚧

✨ Solution for 6.4 by discord ✨

Right side:

Counts the number of bit sequences with n zeros and $m+1$ ones. So they have length $n+m+1$, from which we choose $m+1$ positions for the ones.

Left side:

Group the bit sequences by the position of the last one and sum up all possibilities for each position. Since the sequence contains $m+1$ ones, the last one can be at position $m+1$ at the earliest.

$$\sum_{k=m+1}^{n+m+1}\binom{k-1}{m}=\sum_{k=0}^{n}\binom{k+m+1-1}{m}=\sum_{k=0}^{n}\binom{k+m}{m}=\sum_{k=0}^{n}\binom{k+m}{k} \quad \square$$

7 2022-09-30 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_Exam_2022-09-30

7.1

Use the Chinese remainder theorem to solve the following system of congruence relations:

$$3x \equiv 12 \bmod 13,$$
$$5x \equiv 7 \bmod 22,$$
$$2x \equiv 3 \bmod 7$$

i Duplicate

This exercise is equivalent to Section 3.4

✨ Solution for 7.1 ✨

Same as Section 3.4 (page 27)

7.2

Compute the number of integers x with $1 \leq x \leq 1000000$ where x is neither a square nor a 3rd, 4th or 5th power of some positive integer y.

i Duplicate

This exercise is equivalent to Section 3.2

✨ Solution for 7.2 ✨

see Section 3.2 (page 23)

7.3

List all elements of $\mathbb{Z}_3[x]/(x^2+x+1)$. Examine whether or not this is a field and whether or not $x+1$ is a unit in it. If $x+1$ is a unit, compute its multiplicative inverse.

i Duplicate

This exercise is equivalent to Section 5.4

✨ Solution for 7.3 ✨

Same as: Section 5.4 (page 39)

7.4

List all sets S such that $(\{1,2,3\}, S)$ is a matroid.

✨ Solution for 7.4 by arch user ✨

💻 Theory

Matroid Properties

1. $\forall x : \forall y \subseteq x \in S$
2. $\forall A, B \in S : |B| = |A| + 1$
   $\Rightarrow \exists v \in B \setminus A : A \cup \{v\} \in S$

$$
\begin{aligned}
S = \{ & \\
& \{\emptyset\} \\
& \{\emptyset, \{1\}\} \\
& \{\emptyset, \{2\}\} \\
& \{\emptyset, \{3\}\} \\
& \{\emptyset, \{1\}, \{2\}\} \\
& \{\emptyset, \{1\}, \{3\}\} \\
& \{\emptyset, \{2\}, \{3\}\} \\
& \{\emptyset, \{1\}, \{2\}, \{3\}\} \\
& \{\emptyset, \{1\}, \{2\}, \{1,2\}\} \\
& \{\emptyset, \{1\}, \{3\}, \{1,3\}\} \\
& \{\emptyset, \{2\}, \{3\}, \{2,3\}\} \\
& \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}\} \\
& \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}\} \\
& \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,3\}, \{2,3\}\} \\
& \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}\} \\
& \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\} \\
\} &
\end{aligned}
$$

because, these are all set combinations where

$$\forall A, B \text{ sets with } |B| = |A| + 1$$

you can always find an element in $B \setminus A$ (Note the $\exists$ quantifier in the definition) which when added to A still gives a set from the independendence system.

💡 The number of subsets with 1 element has to be bigger with difference of 1 than the subsets with 2 elements:

$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}\}$$

✨ Solution for 7.4 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

$\{\{1,2,3\},\{1,2\},\{2,3\},\{1,3\},\{1\},\{2\},\{3\},\emptyset\}$
$\{\{1,2\},\{2,3\},\{1,3\},\{1\},\{2\},\{3\},\emptyset\}$
$\{\{2,3\},\{1,3\},\{1\},\{2\},\{3\},\emptyset\}$
$\{\{1,2\},\{1,3\},\{1\},\{2\},\{3\},\emptyset\}$
$\{\{1,2\},\{2,3\},\{1\},\{2\},\{3\},\emptyset\}$
$\{\{1,2\},\{1\},\{2\},\emptyset\}$
$\{\{2,3\},\{2\},\{3\},\emptyset\}$
$\{\{1,3\},\{1\},\{3\},\emptyset\}$
$\{\{1\},\{2\},\{3\},\emptyset\}$
$\{\{2\},\{3\},\emptyset\}$
$\{\{1\},\{3\},\emptyset\}$
$\{\{1\},\{2\},\emptyset\}$
$\{\{1\},\emptyset\}$
$\{\{2\},\emptyset\}$
$\{\{3\},\emptyset\}$
$\{\emptyset\}$

✨ Solution for 7.4 by acrobatic aviator ✨

$S \in \{$

$\{\emptyset\}$	$\longrightarrow$ Empty set is always a matroid
$\{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$	$\longrightarrow$ Powerset of $\{1,2,3\}$
$\{\emptyset,\{1\}\}$	$\longrightarrow$ One set of size 1
$\{\emptyset,\{2\}\}$	$\longrightarrow$ One set of size 1
$\{\emptyset,\{3\}\}$	$\longrightarrow$ One set of size 1
$\{\emptyset,\{1\},\{2\}\}$	$\longrightarrow$ 2 sets of size 1
$\{\emptyset,\{1\},\{3\}\}$	$\longrightarrow$ 2 sets of size 1
$\{\emptyset,\{2\},\{3\}\}$	$\longrightarrow$ 2 sets of size 1
$\{\emptyset,\{1\},\{2\},\{3\}\}$	$\longrightarrow$ 3 sets of size 1
$\{\emptyset,\{1,2\},\{1\},\{2\}\}$	$\longrightarrow$ 1 set of size 2 with subsets
$\{\emptyset,\{1,3\},\{1\},\{3\}\}$	$\longrightarrow$ 1 set of size 2 with subsets
$\{\emptyset,\{2,3\},\{2\},\{3\}\}$	$\longrightarrow$ 1 set of size 2 with subsets
$\{\emptyset,\{1,2\},\{1,3\},\{1\},\{2\},\{3\}\}$	$\longrightarrow$ 2 sets of size 2 with subsets
$\{\emptyset,\{1,2\},\{2,3\},\{1\},\{2\},\{3\}\}$	$\longrightarrow$ 2 sets of size 2 with subsets
$\{\emptyset,\{1,3\},\{2,3\},\{1\},\{2\},\{3\}\}$	$\longrightarrow$ 2 sets of size 2 with subsets
$\{\emptyset,\{1,2\},\{1,3\},\{2,3\},\{1\},\{2\},\{3\}\}$	$\longrightarrow$ 3 sets of size 2 with subsets

$\}$

8 2022-05-06 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_Exam_2022-05-06

8.1

Given $A = \{a, b, c\}$

1. What is the number of multisets of cardinality 12 built up from A?
2. How many of these sets are subsets of $B = \{...\}$ (where B was a specific multiset) Answer by ...
   1. restricting the number of multisets found in 1?
   2. using the principle of inclusion-exclusion (*some more hints were given*)

⚠ Missing Details

If you want to try it anyways, $B = \{a, a, a, a, a, b, b, b, c, c, c, c, c, c\}$ should work.

✨ Solution for 8.1 by arch user ✨

1.

Number of multisets of cardinality 12:

$$\binom{n+k-1}{k} = \binom{12+3-1}{12} = \frac{14!}{12! \cdot 2!} = \frac{14 \cdot 13}{2} = 91$$

✨ Solution for 8.1 by acrobatic aviator + BlauBarschBube ✨

1.

Number of multisets of cardinality 12:

$$\binom{n+k-1}{k} = \binom{12+3-1}{12} = \frac{14!}{12! \cdot 2!} = \frac{14 \cdot 13}{2} = 91$$

2.

✏ Assumption (by us)

$B = \{a, a, a, a, a, b, b, b, c, c, c, c, c, c\}$

$$91 - |\text{too many } a| - |\text{too many } b| - |\text{too many } c| + |\text{too many } a, b| + \\ + |\text{too many } a, c| + |\text{too many } b, c| - |\text{too many } a, b, c|$$

Assume there are max. n_x x-elements in B:

$$
\begin{aligned}
|\text{too many } x| &= \sum_{i=n_x+1}^{12} \binom{2+(12-i)-1}{12-i} \\
&= \sum_{i=n_x+1}^{12} \binom{13-i}{12-i} \\
&= \sum_{i=n_x+1}^{12} 13-i \\
&= \sum_{i=1}^{13-(n_x+1)} i \\
&= \sum_{i=1}^{12-n_x} i
\end{aligned}
$$

$$
\begin{aligned}
|\text{too many } a| &= \sum_{i=1}^{12-5} i = \frac{7\cdot 8}{2} = 28 \\
|\text{too many } b| &= \sum_{i=1}^{12-3} i = \frac{9\cdot 10}{2} = 45 \\
|\text{too many } c| &= \sum_{i=1}^{12-6} i = \frac{6\cdot 7}{2} = 21
\end{aligned}
$$

Assume there are max. n_x x-elements and n_y y-elements in B:

$$
\begin{aligned}
|\text{too many } x,y| &= \sum_{i=(n_x+1)+(n_y+1)}^{12} \overbrace{\binom{1+(12-i)-1}{12-i}}^{\text{1 possibility for } z} \cdot \overbrace{\binom{2+(12-i)-1}{12-i}}^{\text{fill in the rest with } x \text{ or } y} \\
&= \sum_{i=(n_x+1)+(n_y+1)}^{12} 13-i \\
&= \sum_{i=1}^{13-(n_x+1)-(n_y+1)} i \\
&= \sum_{i=1}^{11-n_x-n_y} i \\
&= \frac{(11-n_x-n_y)\cdot(12-n_x-n_y)}{2}
\end{aligned}
$$

$$
\begin{aligned}
|\text{too many } a,b| &= \frac{(11-5-3)\cdot(12-5-3)}{2} = 6 \\
|\text{too many } a,c| &= 0 \quad \text{since} \quad n_a + n_b \not\leq 12 \\
|\text{too many } b,c| &= \frac{(11-3-6)\cdot(12-3-6)}{2} = 3
\end{aligned}
$$

$\implies \text{sol} = 91-28-45-21+6+3 = 100-94 = \mathbf{6}$

✨ **Solution for 8.1 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$** ✨

1. $\binom{3+12-1}{3-1} = \binom{14}{2} = 91$
2. $$\#a \leq 5$$
$$\#b \leq 3$$
$$\#c \leq 6$$
$$\#a_{\text{too many}} = \binom{6+3-1}{3-1} = 28$$
$$\#b_{\text{too many}} = \binom{8+3-1}{3-1} = 45$$
$$\#c_{\text{too many}} = \binom{5+3-1}{3-1} = 21$$
$$\#ab_{\text{too many}} = \binom{2+3-1}{3-1} = 6$$
$$\#ac_{\text{too many}} = 0$$
$$\#bc_{\text{too many}} = \binom{1+3-1}{3-1} = 3$$
$$\#abc_{\text{too many}} = 0$$
$$x \subseteq B$$
$$\#x = 91 - 28 - 45 - 21 + 6 + 3 = \mathbf{6}$$

8.2

Let R be an integral domain. Prove that $(a) = \{ra \mid r \in R\}$

⚠ Missing Details

That's the definition of a principal ideal...
The task ("prove that *this* is an ideal" or something similar) is missing.

✨ Solution for 8.2 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

📖 Theory

$$(x) = \bigcup_{i>0 \mid a \in I_i, I_i \text{ Ideal of } R} I_i$$

$\Longrightarrow$

(a) is the smallest Ideal I where $a \in I$ called principal Ideal

- Is $\{ra \mid r \in R\}$ Ideal?

$$I - I \in I \Rightarrow \{ra - sa \mid rs \in R\} = \{(r-s)a \mid (r-s) \in R\} \checkmark$$
$$fI \in I (\text{with } f \in R) \Rightarrow \{fra \mid r \in R\} = \{fra \mid fr \in R\} \checkmark$$

- Is it smallest Ideal?

Assume Ideal $I : |I| < |\{ra \mid r \in R\}|$

By definition $r \cdot I \in I = \{ri \mid r \in R \land i \in I\} \in I$ with $r \in R$

Since $a \in I \Rightarrow \{ra \mid r \in R\} \in I \Rightarrow \lightning \; |i| \not< |\{ra \mid r \in R\}|$

✨ Solution for 8.2 by acrobatic aviator + BlauBarschBube ✨

📖 Theory

Integral domain $\iff$ comm. ring with $1 \land$ **no** zero dividers

$$(a) = \bigcap_{I \subseteq R, I \text{ ideal}, a \in I} I$$

I is ideal $\iff (I, +)$ subgroup of $R \land \forall r \in R, \forall a \in I : a \cdot r \in I \land r \cdot a \in I$

1. to prove: $\{ra \mid r \in R\}$ is ideal

   take $x, y \in \{ra \mid r \in R\}$:
   $\exists c, d \in R : x = c \cdot a \land y = d \cdot a$

   - is $\{ra \mid r \in R\}$ a subgroup? $x - y \overset{!}{\in} \{ra \mid r \in R\}$

     $x - y = ca - da = (c-d) \cdot a \in \{ra \mid r \in R\}$ ✓

   - Ideal?

$d \cdot x = d \cdot c \cdot a = (d \cdot c) \cdot a \in \{ra \mid r \in R\}$ ✓

$\Longrightarrow \{ra \mid r \in R\} =: I$ is an ideal

Since I is an ideal, $(a) \subseteq I$ must hold.

2. to prove: $I \subseteq (a)$:

   we know: $a \in I, \forall r \in R : ra \in I, (a)$ is an ideal

   $\Longrightarrow \forall s \in R : sa \in (a)$

   $\Longrightarrow I \subseteq (a)$

$\Longrightarrow I = (a)$ □

8.3

Given an undirected Graph G. Let D be the degree matrix and A the adjacency matrix. Define B the incidence matrix with nodes as rows and edges as columns and $B[i][e] = 1$ iff node i is incident to edge e and $B[i][e] = 0$ otherwise. Prove that $A + D = B \cdot B^T$ where B^T is the transpose of B.

✏️ Assumption (by us)

undirected, *simple* graph is important, else we could have loops or double-edges

i Duplicate

This exercise is equivalent to Section 2.3

✨ Solution for 8.3 ✨

see Section 2.3 (page 15)

8.4

Given the following two systems of congruences. Either give the solutions using CRT or prove that there is none:

1. $2x \equiv 2 \bmod 8$
2. $4x \equiv 2 \bmod 8$

⚠ Missing Details

Maybe some details in the tasks are missing: problem could be too easy or unsolvable!

✨ Solution for 8.4 by arch user ✨

Problem is way too easy, I think something is wrong or missing

$$
\begin{aligned}
2x &\equiv 2 \bmod 8 \\
4x &\equiv 2 \bmod 8 \\
&\text{kürzen erlaubt} \\
\Rightarrow x &\equiv 1 \bmod 4 \\
2x &\equiv 1 \bmod 4
\end{aligned}
$$

search for $2^{-1} \bmod 4$

$$
\begin{aligned}
2 \cdot 0 &\equiv 0 \bmod 4 \\
2 \cdot 1 &\equiv 2 \bmod 4 \\
2 \cdot 2 &\equiv 0 \bmod 4 \\
2 \cdot 3 &\equiv 2 \bmod 4
\end{aligned}
$$

2^{-1} does not exists, so the system of congruences is not solvable

✨ Solution for 8.4 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

$$
\begin{aligned}
\gcd(4, 8) &= 4 \\
4 &\nmid 2 \\
\Longrightarrow &\text{ not solvable}
\end{aligned}
$$

9 2022-03-11 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_Exam_2022-03-11

9.1

Let A, B be bases of a matroid. prove that $|A| = |B|$

✨ Solution for 9.1 by arch user ✨

Theory

$M = (E, S)$ is matroid $\Leftrightarrow$
- $A \subset B \in S \Rightarrow A \in S$
- $|B| = |A| + 1, \exists v \in B \setminus A \Rightarrow A \cup \{v\} \in S$

Theory

$A \in S$ is basis $\Leftrightarrow$ A is a maximal independece set, with respect to inclusion.

(E, S) is matroid
Assume $|B| > |A|$ *w.l.o.g*:

$$\text{Augmentation Axiom:}$$
$$\exists v \in B \setminus A \Rightarrow A \cup \{v\} \in S$$

↯ Contradiction A is not maximal

Theory

The rank of a matroid is the cardinality of a basis

$$\text{rank}(M) = |A| = |B|$$

✨ Solution for 9.1 by acrobatic aviator + $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

Let A, B be bases where $|A| < |B|$

Since A, B are bases which are maximal under inclusion

$$\nexists e \in E \setminus A : A \cup \{e\} \in S$$
$$\nexists e \in E \setminus B : B \cup \{e\} \in S$$

$$\exists x \in B \setminus A : \{x\} \cup A \in S \text{ ↯ by matroid condition}$$
$$\Longrightarrow \neg \text{ matroid}$$

9.2

Is $\sqrt{2}+\sqrt{3}$ algebraic over $\mathbb{Q}$, determine its minimal polynomial.

✨ Solution for 9.2 by arch user ✨

🚧 Work in Progress 🚧

For simple use: $\alpha = \sqrt{2}+\sqrt{3}$

algebraic means, that there is a $p(x)$ in $\mathbb{Q}[x]$ which has α as its root ($\Rightarrow p(\alpha)=0$).

$$
\begin{aligned}
(\alpha)^1 &= \sqrt{2}+\sqrt{3} \\
(\alpha)^2 &= 5+\sqrt{6} \\
(\alpha)^3 &= 5\sqrt{2}+5\sqrt{3}+2\sqrt{12}+2\sqrt{18} \\
(\alpha)^4 &= 49+20\sqrt{6}
\end{aligned}
$$

now build up a polynomial such that it has a root at α. You can do that formally with $p(\alpha)-(\alpha)^4+B(\alpha)^2+C=0$.

$$p(x) = x^4 - 10x^2 + 1$$

❓ *But why don't we take a α^3?* Well this would be more complex because we have to elliminate the many square roots somehow.

But is it irreducible?

$$
\begin{aligned}
p(x) &= (x^2+ax+b)(x^2+cx+d) \\
&= x^4+cx^3+dx^2+ax^2+acx^2+adx+bx^2+bcx+bd \\
&= x^4+(a+c)x^3+(d+ac+b)x^2+(ad+bc)x+(bd) \\
&\text{Koeffizientenvergleich} \\
x^4: &\quad 1=1 \\
x^3: &\quad 0=a+c \\
x^2: &\quad -10=d+ac+b \\
x^1: &\quad 0=ad+bc \\
x^0: &\quad 1=bd
\end{aligned}
$$

✨ Solution for 9.2 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

$$\left(\sqrt{2}+\sqrt{3}\right)^2 = 2+2\sqrt{2}\sqrt{3}+3 = 5+2\sqrt{6}$$

$$\left(\sqrt{2}+\sqrt{3}\right)^4 = 25+2\cdot 5\cdot 2\sqrt{2}\sqrt{3}+4\cdot 2\cdot 3 = 49+20\sqrt{6}$$

$$p(x) = x^4-10x^2+1 \in \mathbb{Q}[x] \Longrightarrow \sqrt{2}+\sqrt{3} \text{ is algebraic over } \mathbb{Q}$$

Test if $p(x)$ is minimal polynomial:

$p(x)$ is monic ✓

Is $p(x)$ irreducible?

- No linear root since $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}$

- Constant and quadratic term have coefficient 1

$$(x^2+ax+1)(x^2+bx+1) = x^4+bx^3+x^2+ax^3+abx^2+ax+x^2+bx+1 =$$
$$0 = b+a$$
$$10 = 2+ab$$
$$8 = ab \lightning$$

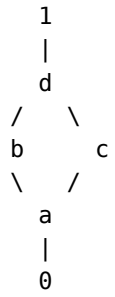
There are no $ab \in \mathbb{Q}$ where $ab = 8$ and $a+b=0$

$\implies p(x)$ is irreducible

$p(x) = x^4 - 10x^2 + 1$ is its minimal Polynomial

9.3

Determine $\mu(0,1)$ of the following partial order:



⚠ Not Relevant

Not in the 6 ECTS version of *Discrete Math*

9.4

Let A, B be two finite sets with $|A| = n$ and $|B| = k$.

1. How many injective mappings: $f : A \mapsto B$ are there?
2. Show that the number of surjective mappings $f : A \to B = k! S_{n,k}$

✨ Solution for 9.4 by arch user ✨

📖 Theory

$f : A \to B$

- **Injective:**
  - *one-to-one*: $\forall a_1 a_2 \in A, b \in B : f(a) = b \wedge a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$
- **Surjective:**
  - *onto*: $\forall b \in B : \exists a : f(a) = b$

📖 Theory

Stirling Numbers 2nd kind
$S_{n,k}$... how many options to partition n object in k (non-empty) boxes

ad 1:
$\#$ of mappings: $n! \cdot \binom{k}{n}$, because the order matters here ($n!$) and we have n elements from k to choose from.

ad 2:
$S_{n,k}$... partition all n elements from set A to all k from set B. Stirling Number guarantees that each partition (elements in B) get chosen at least once. Because Stirling Numbers are unlabeled (indistinguishable), we need to multiply by $k!$ to account for the different orderings of the partitions.

✨ Solution for 9.4 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

1. $n!\binom{k}{n}$
2. **📖 Theory**

   $S_{n,k}$... # k partitions of $\{1, ..., n\}$

   What we know:

   $$k \leq n$$
   $$\forall b \in B \exists a \in A : f(a) = b$$

   $S_{n,k}$... Map each of n elements of A to one of k sets

   $k!$... The partitions have to be mapped to the k Elements which have an order

10 2022-01-26 (vowi)

https://vowi.fsinf.at/wiki/TU_Wien:Discrete_Mathematics_VO_(Gittenberger)/Written_Exam_2022-01-26

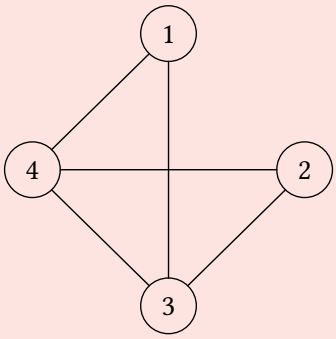
10.1

Calculate the number of spanning forests of a given graph

⚠️ Missing Details

❗ As you can see the graph isn't given 🤡
Maybe take a look at Section 6.1 (page 42)

✏️ Assumption (by us)



✨ Solution for 10.1 by arch user ✨

Number of spanning trees: 8

10.2

$\{a,b\}^* = \{a\}^* \times (\{b\} \times \{b\}^* \times \{a\} \times \{a\}^*)^* \times \{b\}^*$
Explain why this equality holds. Furthermore, state the generating function counting all elements made of $\{a,b\}$ which contain neither aaa or bbb.

✨ Solution for 10.2 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

LHS all strings containing the symbols a, b
RHS is equivalent since we can remove the first and last part which match for all a at the beginning and all b at the end. Then we get $(\{b\} \times \{b\}^* \times \{a\} \times \{a\}^*)^*$.

The remaining string is either an empty string which matches the $(...)^*$ or string (arbitrary often concatenated) which begin with bs and end with as

$\implies$ LHS = RHS

$T = a\{0,2\}(b\{1,2\}a\{1,2\})^*b\{0,2\}$

A_1... strings that end with a
A_2... strings that end with aa
B_1... strings that end with b
B_2... strings that end with bb

$$A_1 = (\varepsilon \cup B_1 \cup B_2) \times \{a\}$$
$$A_2 = A_1 \times \{a\}$$
$$B_1 = (\varepsilon \cup A_1 \cup A_2) \times \{b\}$$
$$B_2 = B_1 \times \{b\}$$

$$A_1(z) = z(1 + B_1(z) + B_2(z))$$
$$A_2(z) = zA_1(z)$$
$$B_1(z) = z(1 + A_1(z) + A_2(z))$$
$$B_2(z) = zB_1(z)$$

$$A_1(z) = z(1 + B_1(z) + zB_1(z))$$
$$B_1(z) = z(1 + A_1(z) + zA_1(z)) = z(1 + (z(1 + B_1(z) + zB_1(z))) + z(z(1 + B_1(z) + zB_1(z)))) =$$
$$= z + z^2 + z^2B_1(z) + z^3B_1(z) + z^3 + z^3B_1(z) + z^4B_1(z)$$
$$B_1(z) = \frac{z + z^2 + z^3}{1 - (z^2 + 2z^3 + z^4)}$$
$$A_1(z) = \frac{z + z^2 + z^3}{1 - (z^2 + 2z^3 + z^4)}$$
$$A_2(z) = \frac{z^2 + z^3 + z^4}{1 - (z^2 + 2z^3 + z^4)}$$
$$B_2(z) = \frac{z^2 + z^3 + z^4}{1 - (z^2 + 2z^3 + z^4)}$$
$$T = \{\varepsilon\} \cup A_1 \cup A_2 \cup B_1 \cup B_2$$
$$t(z) = 1 + A_1(z) + B_1(z) + A_2(z) + B_2(z)$$
$$\boldsymbol{t(z) = 1 + 2\frac{z + z^2 + z^3}{1 - (z^2 + 2z^3 + z^4)} + 2\frac{z^2 + z^3 + z^4}{1 - (z^2 + 2z^3 + z^4)}}$$
$$\boldsymbol{= 1 + 2\frac{z + 2z^2 + 2z^3 + z^4}{1 - z^2 - 2z^3 - z^4}}$$

✨ Solution for 10.2 by acrobatic aviator + BlauBarschBube ✨

1. $\{a, b\}^*$ … All possible strings made from symbols a and/or b

   $\{a\}^* \times (\{b\} \times \{b\}^* \times \{a\} \times \{a\}^*)^* \times \{b\}^*$ … All strings starting with zero or more as, then following zero or more sequences of one or more bs and one or more as. Then the string may end with bs.

   Take a string from $\{a, b\}^*$: if it starts with as, this is captured by the $\{a\}^*$. If it ends with bs, this is captured by $\{b\}^*$. The remaining string then starts with b and ends with a.

   This string can split on every change from a to b into groups containing one or more bs followed by one or more as. This is exactly what is described by the middle part in the definition above.

   Therefore, every string described by $\{a, b\}^*$ can be captured by $\{a\}^* \times (\{b\} \times \{b\}^* \times \{a\} \times \{a\}^*)^* \times \{b\}^*$. Since $\{a, b\}^*$ contains all possibilities to combine a and b, $\{a\}^* \times (\{b\} \times \{b\}^* \times \{a\} \times \{a\}^*)^* \times \{b\}^*$ cannot capture more. This means they are equal.

2. **✏️ Assumption (by us)**

   no aaa also means no $aaaa$ and so on. So every sequence has length max. 2

$$T = \{\varepsilon\} \cup \text{seq}_{1 \le n \le 2}(b) \times \text{seq}_{1 \le n \le 2}(a) \times T$$
$$S = \text{seq}_{n \le 2}(a) \times T \times \text{seq}_{n \le 2}(b)$$

$$
\begin{aligned}
T(z) &= 1 + (z + z^2) \cdot (z + z^2) \cdot T(z) \\
&= 1 + (z + z^2)^2 \cdot T(z) \\
T(z) &= \frac{1}{1 - (z + z^2)^2}
\end{aligned}
$$

$$
\begin{aligned}
S(z) &= \frac{1 - z^3}{1 - z} \cdot T(z) \cdot \frac{1 - z^3}{1 - z} \\
&= \frac{(1 - z^3)^2}{(1 - z)^2} \cdot \frac{1}{1 - (z + z^2)^2} \\
&= \frac{(1 - z^3)^2}{(1 - z)^2 \cdot \left(1 - (z + z^2)^2\right)} \\
&= \frac{(1 - z^3)^2}{(1 - z)^2 - (1 - z)^2 \cdot (z + z^2)^2} \\
&= \frac{1 - 2z^3 + z^6}{1 - 2z + z^2 - (1 - 2z + z^2) \cdot (z^2 + 2z^3 + z^4)} \\
&= \frac{1 - 2z^3 + z^6}{1 - 2z + z^2 - (z^2 + 2z^3 + z^4) + (2z^3 + 4z^4 + 2z^5) - (z^4 + 2z^5 + z^6)} \\
&= \frac{1 - 2z^3 + z^6}{1 - 2z + z^2 - z^2 - 2z^3 - z^4 + 2z^3 + 4z^4 + 2z^5 - z^4 - 2z^5 - z^6} \\
&= \frac{1 - 2z^3 + z^6}{1 - 2z + 2z^4 - z^6}
\end{aligned}
$$

$$
\begin{aligned}
S(z) &= (1 + z + z^2) \cdot T(z) \cdot (1 + z + z^2) \\
&= (1 + z + z^2)^2 \cdot \frac{1}{1 - (z + z^2)^2} \\
S(z) &= \frac{(1 + z + z^2)^2}{1 - (z + z^2)^2}
\end{aligned}
$$

Try to simplify $S(z)$:

$$
1 + z + z^2 = 0
$$

$$
z_{1,2} = z_{3,4} = \frac{-1 \pm \sqrt{1 - 4}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i
$$

$$
z + z^2 = -1
$$

$$
1 + z + z^2 = 0
$$

$z_{1,2}$ are same as above

$$
z + z^2 = 1
$$

$$
-1 + z + z^2 = 0
$$

$$
z_{3,4} = \frac{-1 \pm \sqrt{1 + 4}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}
$$

$$
\begin{aligned}
S(z) &= \frac{\left(z+\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\left(z+\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)\left(z+\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\left(z+\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)}{-\left(z+\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\left(z+-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)\left(z+\frac{1}{2}+\frac{\sqrt{3}}{2}\right)\left(z+\frac{1}{2}-\frac{\sqrt{3}}{2}\right)} \\
&= \frac{\left(z+\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\left(z+\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)}{-\left(z+\frac{1}{2}+\frac{\sqrt{3}}{2}\right)\left(z+\frac{1}{2}-\frac{\sqrt{3}}{2}\right)} \\
&= -\frac{1+z+z^2}{-1+z+z^2} \\
&= -\frac{-1+2+z+z^2}{-1+z+z^2} \\
S(z) &= \frac{-2}{-1+z+z^2} - 1
\end{aligned}
$$

10.3

$$4x \equiv 2 (\mod 11),$$
$$x^2 \equiv 1 (\mod 6),$$
$$12x \equiv 8 (\mod 20)$$

✨ Solution for 10.3 ✨

similar to Section 5.1 (page 33)

✨ Solution for 10.3 by arch user ✨

$$4x \equiv 2 \bmod 11$$
$$x^2 \equiv 1 \bmod 6$$
$$12x \equiv 8 \bmod 22 \Rightarrow 3x \equiv 2 \bmod 5$$

for the second equation there are two solutions: $a_2 = 1 \vee a_2 = 5$ this means we need a case distinction at the end.

$$a_1 = 6$$
$$a_2 = 1 \vee a_2 = 5$$
$$a_3 = 4$$

$$b_1 = 7$$
$$b_2 = 1$$
$$b_3 = 1$$

Case $a_2 = 1$:

$$x \equiv 259 \bmod 330$$

Case $a_2 = 5$:

$$x \equiv 149 \bmod 330$$

10.4

$R = \mathbb{Z}_5[x]/(x^2 + 3x + 1)$ List all elements of R.

1. Is R a field?
2. Is $x + 3$ a unit in R?

✨ Solution for 10.4 by arch user ✨

The elements in this quotient ring are:

$$R = \{ax + b \mid a, b \in \mathbb{Z}_5\}$$

We know that $\mathbb{Z}_5$ is a field, so $\mathbb{Z}_5/p(x)$ is a field too iff:

- $p(x)$ is monic
- $p(x)$ is irreducible

That it's monic can be seen immediately, since the leading coefficient is 1. That it's irreducible can be seen by checking that it has no roots in $\mathbb{Z}_5$.

$$x^2 + 3x + 1 = 0$$

p-q Formel https://www.youtube.com/watch?v=tRblwTsX6hQ

$$x_{1/2} = -\frac{3}{2} \pm \sqrt{\left(\frac{3}{2}\right)^2 - 1}$$

$$= -\frac{3}{2} \pm \underbrace{\sqrt{\frac{5}{4}}}_{\notin \mathbb{Z}}$$

Therefore $p(x)$ is **irreducible** and $\mathbb{Z}_5/p(x)$ is a field.

! Correction by BlauBarschBube

The polynomial $p(x)$ is reducible in $\mathbb{Z}_5$, namely $p(x) = (x + 4)^2$
So it is not a field.
The inverse of $x + 3$ can be found nonetheless.

In a field, every element execpt 0 has a unit, so $x + 3$ has one too. The inverse can be calculated the following way:

$$(x + 3)^{-1} = ?$$

$$p(x) : x + 3 =$$

$$x^2 + 3x + 1 : x + 3 = x$$

$$x^2 + 3x$$

$$-------$$

$$+1 \leftarrow \text{constant rest is ok}$$

so the inverse of $x + 3$ is x

! Correction by BlauBarschBube

The inverse is $-x \equiv 4 \cdot x$
as you need to bring the equation to the form $1 = (x^2 + 3x + 1) - x \cdot (x + 3)$

11 2021-02-05 (vowi, Drmota)

https://vowi.fsinf.at/images/a/af/TU_Wien-Discrete_Mathematics_VO_(Gittenberger)_-_Written_Exam_2021-02-05.pdf

11.1

Determine explicitly the coefficient a_n of the power series

$$f(z) = \frac{1}{(1-z)(1+3z)} + \frac{3}{\sqrt{1+2z}}$$

✨ **Solution for 11.1 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ + acrobatic aviator + BlauBarschBube** ✨

$$\begin{aligned}
\frac{1}{(1-z)(1+3z)} &= \frac{A}{1-z} + \frac{B}{1+3z} \\
1 &= A(1+3z) + B(1-z) \\
1 &= B\left(\frac{4}{3}\right) \\
B &= \frac{3}{4} \\
A &= \frac{1}{4} \\
\frac{1}{(1-z)(1+3z)} &= \frac{1}{4}\frac{1}{1-z} + \frac{3}{4}\frac{1}{1+3z} \\
&= \sum_{n\geq 0} \frac{1}{4} \cdot z^n + \sum_{n\geq 0} \frac{3}{4}(-3)^n \cdot z^n
\end{aligned}$$

Theory

$$(1+b)^k = \sum_{i\geq 0} \binom{k}{i} b^i$$

$$\text{in general: } \binom{\alpha}{k} = \frac{\alpha^{\underline{k}}}{k!} = \frac{\alpha(\alpha-1)(\alpha-2)\ldots(\alpha-(k-1))}{k!}$$

$$n! \cdot 2^n = (1\cdot 2)\cdot(2\cdot 2)\cdot\ldots\cdot(n\cdot 2)$$

$$\frac{(2n)!}{n!\cdot 2^n} = 1\cdot 3\cdot\ldots\cdot(2n-1)$$

$$\frac{3}{\sqrt{1+2z}} = \sum_{n\geq 0} 3\cdot 2^n \cdot \binom{-\frac{1}{2}}{n} \cdot z^n$$

$$
\begin{aligned}
a_n = [z^n]f(z) &= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot 2^n \cdot \binom{-\frac{1}{2}}{n} \\
&= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot 2^n \cdot \frac{(-\frac{1}{2})(-\frac{1}{2}-1)(-\frac{1}{2}-2)\ldots(-\frac{1}{2}-n+1)}{n!} \\
&= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot 2^n \cdot \frac{1}{n!} \cdot \frac{-1}{2} \cdot \prod_{j=1}^{n-1}\left(-\frac{1}{2}-j\right) \\
&= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot 2^n \cdot \frac{1}{n!} \cdot \frac{-1}{2} \cdot \prod_{j=1}^{n-1}\left(\frac{-1-2j}{2}\right) \\
&= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot 2^n \cdot \frac{1}{n!} \cdot \frac{-1}{2} \cdot \left(\frac{-1}{2}\right)^{n-1} \cdot \prod_{j=1}^{n-1} 1+2j \\
&= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot 2^n \cdot \frac{1}{n!} \cdot \left(\frac{-1}{2}\right)^{n} \cdot \prod_{j=1}^{n-1} 1+2j \\
&= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot 2^n \cdot \frac{1}{n!} \cdot \left(\frac{-1}{2}\right)^{n} \cdot (3 \cdot 5 \cdot \ldots \cdot 2n-1) \\
&= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot 2^n \cdot \frac{1}{n!} \cdot \left(\frac{-1}{2}\right)^{n} \cdot \frac{(2n)!}{n! \cdot 2^n} \\
&= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot 2^n \cdot \left(\frac{1}{n!}\right)^2 \cdot (-1)^n \cdot \left(\frac{1}{2}\right)^{2n} \cdot (2n)! \\
&= \frac{1}{4} + \frac{3}{4}(-3)^n + 3 \cdot \left(\frac{1}{n!}\right)^2 \cdot (-1)^n \cdot \left(\frac{1}{2}\right)^{n} \cdot (2n)!
\end{aligned}
$$

11.2

Determine (with the help of the principle of inclusion and exclusion) the number of natural numbers n with $1 \leq n \leq 2000$ such that $\gcd(n, 140) = 5$.
Hint: Reformulate the condition $\gcd(n, 140) = 5$ into several condition of the form $p_i | n$ and p_j does not divide n (for some primes p_i, p_j).

✨ Solution for 11.2 by acrobatic aviator + BlauBarschBube ✨

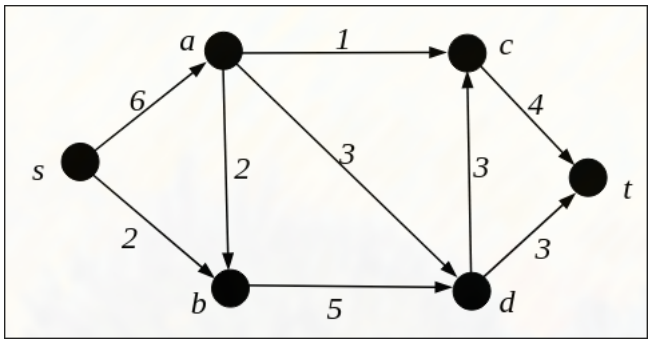
Determine prime factors of 140: $2^4 \cdot 5 \cdot 7$

$$\gcd(n, 140) = 5 \iff 5 \mid n \wedge 2 \nmid n \wedge 7 \nmid n$$

Principle of inclusion and exclusion:

$$\begin{aligned}
&\underbrace{\left\lfloor \frac{2000}{5} \right\rfloor}_{5|n} - \underbrace{\left\lfloor \frac{2000}{5 \cdot 2} \right\rfloor}_{5|n \wedge 2|n} - \underbrace{\left\lfloor \frac{2000}{5 \cdot 7} \right\rfloor}_{5|n \wedge 7|n} + \underbrace{\left\lfloor \frac{2000}{5 \cdot 2 \cdot 7} \right\rfloor}_{5|n \wedge 2|n \wedge 7|n} \\
&= 400 - 200 - 57 + 28 \\
&= 171
\end{aligned}$$

11.3



Determine a maximum flow from s to t on the above network by starting with the zero flow and by determining a series of augmenting paths. Does this maximum flow change if the edge (a, c) (with capacity 1) is cut? Explain your answer

⚠ Not Relevant

Gittenberger skipped *Max Flow/Min Cut* theorem

11.4

1. Which polynomial is irreducible over $\mathbb{Z}_3$
   1. $f(x) = x^3 + x^2 - 1$
   2. $g(x) = x^4 - x + 1$

   - Hint: Be careful with $g(x)$. It has no zeros but ...
2. Furthermore determine all solutions of the following set of congruences
   - Hint: Reduce the given system into a system of the form $x \equiv a_i \bmod m_i$

$$x^2 \equiv 1 \bmod 2,$$
$$28x \equiv 24 \bmod 44$$

✨ Solution for 11.4 by acrobatic aviator + BlauBarschBube ✨

ad 1:
1. irreducable (proof as before)
2. reducable in $(x+1)(x^3 + 2x^2 + x + 1)$

ad 2: $x \equiv 15 \bmod 22$

12 2025-06-27 (Stufler)

12.1 Number Theory

1. For which integers m is the group $(\mathbb{Z}/\langle m\rangle)^*$ cyclic?
2. Compute with Euler's totient function the number of elements in $(\mathbb{Z}/\langle 100\rangle)^*$
3. Compute $7^{100} \bmod 40$

✨ Solution for 12.1 by acrobatic aviator + BlauBarschBube ✨

📖 Theory

$$\varphi(m) = \varphi\left(\underbrace{\prod_{p\in\mathbb{P},\ \nu_{p(m)}>0} p^{\nu_{p(m)}}}_{\text{prime factorization}}\right) = m\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$$

1. $\forall m \in \{2, 4, p^k, 2p^k \mid p \in \mathbb{P}\setminus\{2\}, k \geq 1$
2. $\varphi(100) = \varphi(2^2\cdot 5^2) = 100\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right) = 40$
3. $7^{100} \equiv (7^2)^{50} \equiv 9^{50} \equiv (9^2)^{25} \equiv 1^{25} \equiv 1$ (everything mod 40)

12.2 Combinatorics

Show that each set of integers with 5 elements has 3 elements whose sum is divisible by 3.

✨ Solution for 12.2 by arch user ✨

There are 3 residue classes: $\overline{0}, \overline{1}, \overline{2}$ (0,1,2 written because easy). There are 5 (different) elements (because it's a set, which map to residue classes) to fill 5 places $\Rightarrow$ min. 2 of the classes have at least 2 elements.
Examples: $\{\overline{0}, \overline{0}, \overline{1}, \overline{2}, \overline{2}\}, \{\overline{1}, \overline{2}, \overline{1}, \overline{2}, \overline{1}\}$
If 3 have the same residue class: (it's easy)

$$\overline{0} + \overline{0} + \overline{0} = \overline{0}$$
$$\overline{1} + \overline{1} + \overline{1} = \overline{0}$$
$$\overline{2} + \overline{2} + \overline{2} = \overline{0}$$

If less than 3 have the same residue class (Pigeonhole principle):

$$\forall \text{ residue classes exists at least one element}$$
$$\overline{0} + \overline{1} + \overline{2} = \overline{0}$$

12.3 Finite Fields

Consider the field $\mathbb{F}_2/\langle f \rangle$ with $f = x^4 + x + 1$

1. show that f is a field
2. using euclid's algorithm, determine the inverse of $x^3 + x + 1$

✨ Solution for 12.3 by BlauBarschBube + acrobatic aviator ✨

1. Show f is irreducible
2. Do two steps of euclids algorithm, the inverse is $1 + x^2$

12.4 Graph Theory

Show that every simple graph with $\deg(v) \geq 3$ for all vertices has a cycle with length at least 4.

✨ Solution for 12.4 by $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

Take any spanning subtree if the graph. The leafs have $\deg = 1$

$\Longrightarrow$ There need two edges to be added.

Each edge produces cycle (because it is a spanning subtree)

If connected to two siblings there is a cycle of len 4 with the siblings and the parent.

Otherwise there exists a larger cycle over a higher node in the tree.

13 2025-03-01 (Stufler)

13.1 Graphs

1. prove that for a planar graph with at least 10 vertices, the average degree of vertices must be less than 10
2. prove for a matroid (E, S), if A and B are bases of the matroid, then $|A| = |B|$

✨ Solution for 13.1 by acrobatic aviator + BlauBarschBube ✨

📓 Theory

- Euler's polyhedron formula: $\alpha_0 - \alpha_1 + \alpha_2 = 0$
- Handshaking lemma: $\sum_{v \in V} d(v) = 2\alpha_1$
- For planar graphs: $3\alpha_2 \leq 2\alpha_1$

$$d_{\text{avg}} = \frac{1}{\alpha_0} \cdot \sum_{v \in V} d(v) = \frac{2\alpha_1}{\alpha_0}$$

$$\begin{aligned} 3\alpha_2 &\leq 2\alpha_1 \\ 6 - 3\alpha_0 + 3\alpha_1 &\leq 2\alpha_1 \\ 6 - 3\alpha_0 &\leq -\alpha_1 \\ 3\alpha_0 - 6 &\geq \alpha_1 \end{aligned}$$

$$d_{\text{avg}} = \frac{2\alpha_1}{\alpha_0} \leq \frac{6\alpha_0 - 12}{\alpha_0} = 6 - \frac{12}{\alpha_0} < 6 < 10 \quad \square$$

13.2 Generating Functions

Determine explicitly the coefficient a_n of the power series:

$$f(x) = \frac{1}{(1-x)(1+3x)} + \frac{3}{\sqrt{1+2x}}$$

✨ Solution for 13.2 by BlauBarschBube + acrobatic aviator + $m \cdot \sum_{i=0}^{\infty} \frac{1}{k!}$ ✨

See Section 11.1 (page 72)

13.3 Abstract Algebra

For $\mathbb{Z}_3$, show which is irreducible

1. $f(x) = x^3 + x^2 - 1$
2. $g(x) = x^4 - x + 1$

13.4 Pigeonhole Principle

Given a Set A, which is a subset of $\{1, ..., 41\}$, and $|A| = 21$, prove that there must exist $x, y \in A$ such that $x + y = 42$

✨ Solution for 13.4 by BlauBarschBube + acrobatic aviator ✨

See Section 5.3 (page 38)

14 2025-01-24

14.1 Number Theory (10pt)

Let p denote a prime number, k a positive integer and $\mathbb{F}_{p^k}$ the field with p^k elements.

1. What is the characteristic $\operatorname{char}\left(\mathbb{F}_{p^k}\right)$ [1pt]
2. Prove that if $p = 2$ then $a = -a$ for all $a \in \mathbb{F}_{2^k}$ (Hint: $a = 1 \cdot a$) [1pt]
3. How many elements does the group of units $\mathbb{F}_{p^k}^{\times}$ have? [1pt]
4. How many elements does the group of units $\mathbb{Z}/\langle p^k \rangle^{\times}$ have? [1pt]
5. How many elements does the group of units $\mathbb{Z}/\langle 90 \rangle^{\times}$ have? [1pt]

✨ Solution for 14.1 by BlauBarschBube + acrobatic aviator ✨

1. p, as arithmetic is mod p
2. modulo 2 arithmetic?
3. $p^k - 1$
4. $p \neq 2 \vee (p = 2 \wedge k \in \{1, 2\}) \Rightarrow p^k - 1,$ else $\varphi\left(p^k\right)$
5. $\varphi(90) = 24$

14.2 Polynomials in finite fields (10pt)

Let $\mathbb{F}_8$ denote the field with 8 elements. Let $f, g \in \mathbb{F}_8[x]$ with $f = x^4 + x^3 + x + 1$ and $g = x^3 + x + 1$.

1. Determine $\gcd(f, g)$ [4pt]
2. Find $\lambda, \mu \in \mathbb{F}_8[x]$ with $\lambda f - \mu g = \gcd(f, g)$ [4pt]
3. Is g invertible in $\mathbb{F}_8[x]/\langle f \rangle$? If yes, determine its inverse [2pt]

✨ Solution for 14.2 by acrobatic aviator + BlauBarschBube ✨

1. Euclidian algorithm
2. reverse Euclidian algorithm
3. is invertible $\iff \gcd(f, g) = 1$-element of $\mathbb{F}_8$

14.3 Combinatorics (10pt)

1. let $A = \{1, 2, ..., 6\}$. How many ways are there to partition A into 2-element subsets? (For example $\{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$ is one such partition) [5pt]
2. Show that for any positive integer n the number of positive divisors of n^2 is always odd. (Hint: use prime factor decompositions) [5pt]

✨ Solution for 14.3 by BlauBarschBube + acrobatic aviator ✨

1.

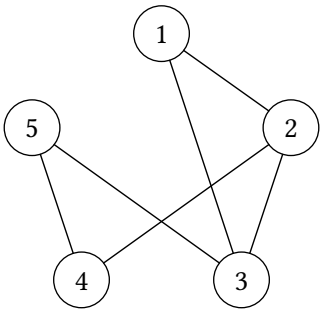
$$\binom{6}{2} \cdot \binom{4}{2} \cdot \frac{1}{3!} = 15 \quad \text{divide by 3! to account for permutations of the blocks}$$

✔ Approved by arch user

2. ?

14.4 Graph Theory (10pt)

Calculate the number of spanning trees of the following graph:



✨ Solution for 14.4 by arch user ✨

$$\#\text{ spanning trees} = 11$$

15 2025-12-18

15.1 Polynomials in finite fields (10pt)

Let K be the field $\mathbb{Z}_7$. Examine whether the quotient ring $K[x]/x^2+5$ is a field or not. Is $x+2$ a unit in it?

✨ Solution for 15.1 by god ✨

Not a field, since x^2+5 is reducible to $(x+3)(x+4)$. Alternatively, show that for $x=3$ the polynomial is zero, so 3 is a root. $x+2$ is a unit, Wöcki got $3x+1$ as the inverse, IIRC.

15.2 Matroids (10pt)

Let E be a set, $1 \leq k \leq |E|$ an integer, and let S denote the set of all subsets $X \subseteq E$ with cardinality at most k. Examine wether $M = (E, S)$ is a matroid.

15.3 Combinatorics (10pt)

Given $A = \{a, b, c\}$

1. What is the number of multisets of cardinality 12 built up from A?
2. How many of these sets are sub-multisets of $M = \{a, a, a, a, b, b, b, b, b, b, c, c, c, c, c\}$? Answer by ...
   1. Showing how many multisets cannot be sub-multisets due to containing too many a's
   2. Using the principle of inclusion-exclusion

15.4 Theory (10pt)

What is an unlabeled combinatorial structure?

What counting problem regarding it did we formulate in the lecture? How did we approach solving this problem? Why is this solution method appropriate?

To show this, show both basic constructions we used during the lecture, and how this method applies to them. Prove every step of your explanation!

16 Random Exercises

16.1 Matroid

https://vowi.fsinf.at/images/a/a1/TU_Wien-Discrete_Mathematics_UE_(diverse)_-_Ue3.pdf

Let E be a set, $1 \leq k \leq |E|$ an integer, and let S denote the set of all subsets $X \subseteq E$ with cardinality at most k. Examine wether $M = (E, S)$ is a matroid.

✨ **Solution for 16.1 by arch user** ✨

💻 **Theory**

Matroid Properties

1. $S \neq \emptyset$
2. $\forall A \in S, \forall B \subseteq A \Rightarrow B \in S$
3. $|B| = |A| + 1, v \in B \setminus A, A \cup \{v\} \in S$

ad 1)

trivial, because $k \geq 1$ so S cannot be empty

ad 2)

$$A \subseteq E \land B \subseteq A \Rightarrow B \subseteq E$$
$$\Rightarrow B \in S$$

ad 3)

$$|B| = |A| + 1, \quad |B| \leq k \; |A| < k \Rightarrow |A| \leq k - 1$$
$$v \in B \setminus A \Rightarrow |A \cup \{v\}| \geq k - 1 + 1$$
$$\text{with } v \in E \land A \subseteq E$$
$$\Rightarrow A \cup \{v\} \in S$$

16.2 Binom

https://vowi.fsinf.at/images/3/36/TU_Wien-Discrete_Mathematics_UE_(diverse)_-_2023W_Ue7_Lsg.pdf
Prove for all complex numbers x and $k \in \mathbb{N}$ we have

$$\binom{-x}{k} = (-1)^k \binom{x+k-1}{k}$$

✨ Solution for 16.2 by BlauBarschBube ✨

This is true by the definition of the falling factorials

$$\begin{aligned}
\binom{-x}{k} &= \frac{(-x)\cdot(-x-1)\cdot(-x-2)\ldots(-x-k+1)}{k!} \\
&= \frac{1}{k!}\cdot\prod_{i=0}^{k-1}(-x-i) \\
&= (-1)^k\cdot\frac{1}{k!}\cdot\prod_{i=0}^{k-1}(x+i) \\
&= (-1)^k\cdot\frac{1}{k!}\cdot\prod_{i=0}^{k-1}(x+k-1-i) \\
&= (-1)^k\cdot\binom{x+k-1}{k}
\end{aligned}$$

16.3 Squared Fibonacci Generating Function

https://vowi.fsinf.at/images/3/36/TU_Wien-Discrete_Mathematics_UE_(diverse)_-_2023W_Ue7_Lsg.pdf
Prove that the squares of the Fibonacci numbers satisfy the recurrence relation

$$a_{n+3} - 2a_{n+2} - 2a_{n+1} + a_n = 0$$

and solve this recurrence relation with the correct initial conditions

✨ Solution for 16.3 by arch user + god ✨

1) Prove the equality

Fibonacci will be denoted as f_n with $f_{n+2} = f_{n+1} + f_n$.

$$a_{n+3} - 2a_{n+2} - 2a_{n+1} + a_n = 0$$

express the a_n as fibonacci squares

$$(f_{n+3})^2 - 2(f_{n+2})^2 - 2(f_{n+1})^2 + f_n^2 = 0$$

write f_{n+3} as sum of its predecessors

$$(f_{n+2} + f_{n+1})^2 - 2(f_{n+2})^2 - 2(f_{n+1})^2 + f_n^2 = 0$$

$$\cancel{f_{n+2}^2} + 2f_{n+2}f_{n+1} + \cancel{f_{n+1}^2} - \cancel{2}f_{n+2}^2 - \cancel{2}f_{n+1}^2 + f_n^2 = 0$$

write f_{n+2} as sum of its predecessors

$$2(f_{n+1} + f_n)f_{n+1} - (f_{n+1} + f_n)^2 - f_{n+1}^2 + f_n^2 = 0$$

multiply everything out

$$2f_{n+1}^2 + 2f_nf_{n+1} - f_{n+1}^2 - 2f_nf_{n+1} - f_n^2 - f_{n+1}^2 + f_n^2 = 0$$

everything cancels out

$$0 = 0 \quad \square$$

2) Solve the recurence relation

$$a_{n+3} - 2a_{n+2} - 2a_{n+1} + a_n = 0 \qquad | \sum z^n$$

$$\sum_{n\geq 3} a_{n+3}z^n - 2\sum_{n\geq 2} a_{n+2}z^n - 2\sum_{n\geq 1} a_{n+1}z^n + \overbrace{\sum_{n\geq 0} a_n z^n}^{A(z)} = 0$$

$$\frac{1}{z^3}\sum_{n\geq 3} a_{n+3}z^{n+3} - \frac{2}{z^2}\sum_{n\geq 2} a_{n+2}z^{n+2} - \frac{2}{z}\sum_{n\geq 1} a_{n+1}z^{n+1} + A(z) = 0$$

$$\frac{1}{z^3}(A(z) - a_2z^2 - a_1z - a_0) - \frac{2}{z^2}(A(z) - a_2z^2 - a_1z - a_0) - \frac{2}{z}(A(z) - a_2z^2 - a_1z - a_0) + A(z) = 0$$

with $a_0 = 0, a_1 = 1a_2 = 1$

$$\frac{1}{z^3}(A(z) - z^2 - z) - \frac{2}{z^2}(A(z) - z^2 - z) - \frac{2}{z}(A(z) - z^2 - z) + A(z) = 0$$

reformulating

$$A(z) = \frac{z(1-z)}{(z^2 - 3z + 1)(z+1)}$$

✨ Solution for 16.3 by BlauBarschBube ✨

Continuing from previous solution:

$$A(z) = \frac{z(1-z)}{(z-(z_1))\cdot(z-z_2)\cdot(z+1)} \quad \text{with} \quad z_1 = \frac{3}{2}+\frac{\sqrt{5}}{2} \quad \text{and} \quad z_2 = \frac{3}{2}-\frac{\sqrt{5}}{2}$$

Now use partial fractions to find

$$\begin{aligned} A(z) &= \frac{1}{z+1} - \left(\frac{4+\sqrt{5}}{\sqrt{5}}\right)\cdot\frac{1}{z-\frac{3+\sqrt{5}}{2}} + \left(\frac{4-\sqrt{5}}{\sqrt{5}}\right)\cdot\frac{1}{z-\frac{3-\sqrt{5}}{2}} \\ &= \sum_{n\geq 0} z^n - \left(\frac{4+\sqrt{5}}{\sqrt{5}}\right)\cdot\frac{-1}{\frac{3+\sqrt{5}}{2}}\cdot\sum_{n\geq 0}\left(\frac{1}{\frac{3+\sqrt{5}}{2}}\right)^n z^n - \left(\frac{4-\sqrt{5}}{\sqrt{5}}\right)\cdot\frac{-1}{\frac{3-\sqrt{5}}{2}}\cdot\sum_{n\geq 0}\left(\frac{1}{\frac{3-\sqrt{5}}{2}}\right)^n z^n \end{aligned}$$

So we get

$$a_n = 1 + \left(\frac{2}{\left(3+\sqrt{5}\right)}\right)^{(n+1)} + \left(\frac{2}{\left(3-\sqrt{5}\right)}\right)^{(n+1)}$$

16.4 Generating Function

https://vowi.fsinf.at/images/3/36/TU_Wien-Discrete_Mathematics_UE_(diverse)_-_2023W_Ue7_Lsg.pdf
Solve the following recurrence using generating functions:

$$a_{n+1} = 3a_n - 2 \quad \text{for} \quad n \geq 0, a_0 = 2$$

✨ Solution for 16.4 by arch user ✨

$$\sum_{n\geq 1} a_{n+1} z^n = 3 \underbrace{\sum_{n\geq 0} a_n z^n}_{A(z)} - 2 \underbrace{\sum_{n\geq 0} z^n}_{\frac{1}{1-z}}$$

$$\frac{1}{z} \sum_{n\geq 1} a_{n+1} z^{n+1} = 3A(z) - \frac{2}{1-z}$$

$$\frac{1}{z}(A(z) - a_0) = 3A(z) - \frac{2}{1-z}$$

$$\frac{1}{z}A(z) - 3A(z) = \frac{2}{z} - \frac{2}{1-z}$$

$$A(z) = \frac{2z - 4z^2}{z(1-z)(1-3z)}$$

$$= \frac{2-4z}{(1-z)(1-3z)}$$

Partial Fraction Decomposition

$$A(z) = \frac{1}{1-z} + \frac{1}{1-3z}$$

transformation

$$A(z) = \sum_{n\geq 0} \binom{n}{1} z^n + \sum_{n\geq 0} 3^n z^n$$

$$\Rightarrow$$

$$a_n = 1 + 3^n$$

16.5 Ring Family of Ideals

https://sh1.fsinf.at/~prawn/sheet_10.html

Let R be a ring and $\left(I_j\right)_{j\in J}$ be a family of ideals of R. Prove that $\bigcap_{j\in J} I_j$ is an ideal of R.

✨ Solution for 16.5 by BlauBarschBube ✨

Let $\mathbb{I} = \bigcap_{j\in J} I_j$

$$\forall j 0 \in I_j \Rightarrow 0 \in \mathbb{I}$$

$$\text{Let x,y } \in \mathbb{I}$$

$$\Leftrightarrow x, y \in I_j \forall j$$

$$\Rightarrow x - y \in I_j \forall j$$

$$\Rightarrow x - y \in \mathbb{I}$$

$$\text{Let r } \in R \text{ and x } \in \mathbb{I}$$

$$\Rightarrow x \in I_j \forall j$$

$$\Rightarrow r \cdot x \in I_j \forall j$$

$$\Rightarrow r \cdot x \in \mathbb{I}$$

$$\Rightarrow \mathbb{I} \text{ is ideal of R}$$

16.6 Extended Euclidean

https://sh1.fsinf.at/~prawn/sheet_7.html

Use the Euclidean Algorithm to find all the greatest common divisors of $x^3 + 5x^2 + 7x + 3$ and $x^3 + x^2 - 5x + 3$ in $\mathbb{Q}[x]$

✨ Solution for 16.6 by arch user ✨

$$\overbrace{x^3 + 5x^2 + 7x + 3}^{p(x)} = 1 \cdot \overbrace{(x^3 + x^2 - 5x + 3)}^{q(x)} + \overbrace{4x^2 + 12x}^{r_1}$$

$$\overbrace{x^3 + x^2 - 5x + 3}^{q(x)} = \frac{1}{4}x \cdot (4x^2 + 12x) + \overbrace{(x + 3)}^{r_2}$$

$$4x^2 + 12x = 4x \cdot (x + 3) + \overbrace{0}^{r_3}$$

because the constant rest in r_3 is fine, the $\gcd(p(x), q(x)) = a \cdot (x + 3), \quad \forall a \in \mathbb{Q}$

✔ **Approved by god**

16.7 Ideal of $\mathbb{Z}_6$

https://github.com/VeryMilkyJoe/discrete-maths-collection/blob/main/src/sheet_10.md

Let $U = \{\overline{0}, \overline{2}, \overline{4}\} \subseteq \mathbb{Z}_6$. Show that U is an ideal of $\mathbb{Z}_6$

✨ Solution for 16.7 by arch user ✨

📖 Theory

Ideal Properties:

1. closed under $+$
2. absorbing under $\cdot$

To check the first, create an addition table with all elements in U.

$+$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{2}$

For the *absorbing property* you can do the same with multiplication, but here you have to show that for all elements in $\mathbb{Z}_6$.

$\cdot$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{4}$	$\overline{2}$

All elements in both tables are in U, which means that it is closed under addition with the normal subgroup and absorbing.

$$U \text{ is an ideal} \quad \square$$

16.8 Primitive Polynomials over $\mathbb{Z}_3$

Which of the following polynomials are primitive over $\mathbb{Z}_3$?

1. $x^3 + x^2 + x + 1$
2. $x^3 + x^2 + x + 2$
3. $x^3 + 2x + 1$

Comment by arch user

Übungsbeispiel 55

✨ Solution for 16.8 by arch user ✨

Theory

Primitive Polynomial $\iff$
- irreducible
- $\exists a, \mathrm{GF} : p(a) = 0 \land (a) = \mathbb{Z}_3/p(x) \setminus \{0\}$

1) $x^3 + x^2 + x + 1$

irreducible?

search for roots in $\mathbb{Z}_3$,

$$p(2) = 0 \quad ✗$$

$p(x)$ is not irreducible $\Rightarrow$ not a primitive polynomial

2) $x^3 + x^2 + x + 2$

irreducible?

$$p(0) = 2$$
$$p(1) = 2$$
$$p(2) = 1$$
$$✓ \text{ has no roots in } \mathbb{Z}_3$$

polynomial is irreducible ✓

primitive?

$$\exists ? \, a \in \mathrm{GF}(3^3), \mathrm{ord}(\langle a \rangle) = 3^3 - 1 = 26, p(a) = 0$$
$$\iff p(x) \mid x^{26} - 1$$

$\mathrm{GF}(3^3)$ comes from $\mathbb{Z}_p$ and $\mathrm{ord}(p(x))$, $\mathrm{GF}\left(p^{\mathrm{ord}(p(x))}\right)$ First calculate the factors of 26 which are $d \in \{1, 2, 13, 26\}$ because $\mathrm{ord}\left(a^d\right) \mid 26$. So we have to check that $a^d \neq 1, \forall d \in \{1, ...25\}$. We know that $p(x) = 0 = a^3 + a^2 + a + 2$ which can be restructed to $a^3 = -a^2 - a - 2$. This can later be used to plug it in.

a^1: assume $a \equiv 1 \bmod p(x)$ this means that $p \mid a - 1$ but this is not possible because p has higher degree than $a - 1$. Therefore

$$a \not\equiv 1 \bmod p(x)$$

a^2: same problem as before:

$$a \not\equiv 1 \bmod p(x)$$

a^3: same problem as before:

$$a \not\equiv 1 \bmod p(x)$$

a^4: (result not important, because we don't need to check a^4 but it can be used to simplify some terms later)

$$a^4 = a^3 \cdot a = \overbrace{(2a^2 + 2a + 1)}^{a^3} \cdot = 2a^3 + 2a^2 + a = 2a + 2$$

a^{12}:

$$(a^4)^3 = (2a + 2)^3 = a^2 + a + 1$$

a^{13}:

$$a^{12} \cdot a = -2 \bmod 3 = 1 \bmod 3 \quad \text{✗ not primitive, would only create half the field}$$

3) $x^3 + 2x + 1$
irreducible?

$$p(0) = 1$$
$$p(1) = 1$$
$$p(2) = 1$$
$$\checkmark \text{ is irreducible}$$

primitive?

$$p(a) = 0 = a^3 + 2a + 1$$
$$\Rightarrow a^3 = -2a - 1 \bmod 3 = a + 2 \bmod 3$$

a^1: assume $a \equiv 1 \bmod p(x)$ this means that $p \mid a - 1$ but this is not possible because p has higher degree than $a - 1$. Therefore

$$a \not\equiv 1 \bmod p(x)$$

. **a^2:** same problem as before:

$$a \not\equiv 1 \bmod p(x)$$

a^3: same problem as before:

$$a \not\equiv 1 \bmod p(x)$$

a^4:

$$a^4 = a^4 \cdot a = (a + 2) \cdot a$$
$$a^4 \neq 1 \checkmark$$

a^{12}:

$$(a^4)^3 = (2a + 2)^3 = (a^2 + 2a)^3 = a^2 + 2$$

a^{13}:

$$\begin{aligned} a^{13} &= a^{12} \cdot a = a^3 + 2a \\ &= (a+2) + 2a \\ &= 3a + 2 \qquad \text{because we are in } \mathbb{Z}_3, 3a = 0 \\ &= 2 \quad \checkmark \end{aligned}$$

Because none of them were $\equiv 1$ that means that $a^{26} = 1$. Therefore this polynomial is primitive and generates the whole field.