

Några extra exempel

Övning 1, to 1 september

1. Minns **fibonaccitalen** F_n : 0, 1, 1, 2, 3, 5, 8, 13, ..., rekursivt definierade av

$$\begin{cases} F_0 = 0, F_1 = 1 \\ F_{n+2} = F_{n+1} + F_n, \quad n = 0, 1, \dots \end{cases}.$$

Visa att för alla $n = 1, 2, \dots$ gäller

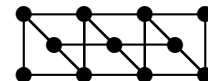
$$F_1^2 + \dots + F_n^2 = \sum_{i=1}^n F_i^2 = F_n F_{n+1} \text{ och } \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n.$$

2. En familj med två vuxna och två barn vill korsa en flod, men deras båt bär högst vikten av en vuxen person. Varje barns vikt är hälften av en vuxens. Använd en riktad graf för att finna ett sätt för dem att komma över.
3. I en graf med åtta hörn har sju av hörnen valenserna 1, 3, 3, 4, 5, 6, 7. Vilka värden är möjliga för det åttonde hörnets valens?
4. Visa att om valensen för alla hörn i grafen $G = (V, E)$ delas av primtalet $p \neq 2$, dvs $p \mid \delta(v)$, för alla $v \in V$, så gäller att talet p delar antalet kanter e , dvs $p \mid |E|$.
5. Hur många hörn kan en graf med 28 kanter ha som mest, om valensen hos varje hörn är minst 3?

Övning 2, on 7 september

1. Rita grafer som är respektive varken hamiltonsk eller eulersk, eulersk men inte hamiltonsk, hamiltonsk men inte eulersk och både hamiltonsk och eulersk.
2. Det är i allmänhet svårt att avgöra om en (stor) graf har någon hamiltoncykel (i motsats till att avgöra om den har någon eulerkrets). Detta exempel illustrerar ett sätt (som fungerar ibland) att visa att en graf **inte** har någon hamiltoncykel.
- a. Visa att om m och n är udda heltal (inte båda = 1) kan en springare inte i en följd drag besöka alla rutor på ett $m \times n$ -schackbräde precis en gång och återkomma till startpunkten. (En springare går i ett drag två rutor framåt och en åt sidan.)
- b. Visa samma sak för ett bräde av format $4 \times n$, n heltal.

3. Har grafen till höger någon hamiltoncykel?
Ge exempel eller förklara varför ingen finns.



4. Visa att om för varje par av hörn x och y i en graf G med n hörn gäller att

$$\delta(x) + \delta(y) \geq n - 1$$

så är grafen sammanhängande.

5. Visa att om en graf G är osammanhängande så måste komplementgrafen $\overline{G}$ vara sammanhängande.
6. Låt $G = (V, E)$ vara en graf. Visa att hörnen i V kan färgas med högst två färger, så att varje hörn har samma färg som högst hälften av sina grannar.

7*. Visa att man i en godtycklig graf $G = (V, E)$ kan rikta kanterna så att skillnaden mellan in- och utvalensen i varje hörn blir högst ett. (Invalensen $\delta^-(v)$ är antalet kanter som går in till hörnet v och utvalensen $\delta^+(v)$ antalet som går ut från det.)

Övning 3, to 8 september

1. Antag att G är en sammanhängande 4-reguljär graf som dessutom är planär. Hur många ytor har en plan ritning av G om G har 16 kanter?

2. (Från planaritetstencilen) I en sammanhängande plan graf har alla hörn valens 3 eller 5. Antalet hörn är 12 och antalet ytor är 11. Hur många hörn har valens 3 och hur många har valens 5?

3. (Från planaritetstencilen) I en 3-reguljär, plan, sammanhängande graf har alla ytor antingen 4 eller 6 kanter (också den obegränsade ytan). Hur många ytor har 4 kanter?

4. Den s.k. Petersens graf (se även Biggs 15.2:2 och 15.8:3) har grannlista

a	b	c	d	e	f	g	h	i	j		(Ett vanligare (än som i fig. 15.14 i Biggs)
b	a	b	c	a	a	b	c	d	e		sätt att rita grafen är som en femhörning
e	c	d	e	d	h	i	f	f	g		med hörn i ordningen $abcde$ och innanför
f	g	h	i	j	i	j	j	g	h		dem deras respektive grannar $fghij$ (som
											blir spetsar i en inre stjärna).)

Visa med hjälp av dels Kuratowskis och dels Wagners sats (se planaritetstencilen) att Petersens graf inte är planär.

5. Tio tentander har gjort en tentamen med tio uppgifter. Varje uppgift klarades av minst sex skrivande. Varje skrivande klarade minst fyra uppgifter. Visa att man kan fördela uppgifterna med en per tentand, så att var och en har klarat sin uppgift.

6*. Visa att det i en enkel graf $G = (V, E)$ finns minst

$$\sum_{v \in V} \frac{1}{\delta(v) + 1}$$

oberoende hörn (dvs hörn utan inbördes kanter). $\delta(v)$ är valensen för $v \in V$.

Övning 4, ti 13 september

1. Finn den största gemensamma delaren till talen 2373 och 1638, $\text{sgd}(2373, 1638)$ (i boken kallad $\text{gcd}(2373, 1638)$) och använd den för att beräkna samma tals minsta gemensamma multipel, $\text{mgm}(2373, 1638)$ (i boken kallad $\text{lcm}(2373, 1638)$).

2. Låt k vara ett heltal. Visa att $3k + 2$ och $5k + 3$ är relativt prima, dvs att $\text{sgd}(3k + 2, 5k + 3) = 1$.

3. Emma har 75 kr, allt i 16 st kronmynt (dvs 1-, 5- och 10-kronor). Hur många mynt av varje sort har hon?

4. Är det för alla heltal n sant att om $10 \mid n^2$ så gäller $10 \mid n$?

Är det för alla heltal n sant att om $9 \mid n^2$ så gäller $9 \mid n$?

5. Visa att för alla heltal n gäller att $6 \mid n^5 + 5n$.

6*. Att skriva ett tal $n \in \mathbb{N}$ i binär form innebär ju att skriva det som en summa av olika 2-potenser (så för varje par av termer är den ena en delare till den andra). Visa att varje $n \in \mathbb{N}$ kan skrivas som en summa av tal av form $2^i \cdot 3^j$ ($i, j \in \mathbb{N}$) där ingen av termerna är en delare till någon av de andra. (T.ex. är $17 = 8 + 9 = 2^3 + 3^2$, $19 = 4 + 6 + 9 = 2^2 + 2 \cdot 3 + 3^2$, $114 = 24 + 36 + 54 = 2^3 \cdot 3 + 2^2 \cdot 3^2 + 2 \cdot 3^3$.) Är summan för alla $n \in \mathbb{N}$ unik (bortsett från ordningen, förstås)?

Övning 5, to 15 september

1. Finn alla heltal x så att $16x \equiv 26 \pmod{42}$.
2. Finn alla heltal x så att $x \equiv 5 \pmod{8}$ och $x \equiv 73 \pmod{81}$.
- 3*. Talet 2^{29} har (i bas 10) 9 siffror, alla olika. Vilken siffra fattas?
4. Visa att om heltalen x, y, z uppfyller $x^3 + 3y^3 = 9z^3$ så är $x = y = z = 0$.
5. Kalla en trippel heltal (a, b, c) för en **pythagoreisk trippel** om $a^2 + b^2 = c^2$, dvs om a, b, c är (mätetal för) sidorna i en rätvinklig triangel. Exempel på pythagoreiska trippler är $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$ och $(3312, 16766, 17090)$. Visa att om (a, b, c) är en pythagoreisk trippel måste
 - a. minst en av a och b vara delbar med 3,
 - b. minst en av a, b och c vara delbar med 5,
 - c. minst en av a och b vara delbar med 4.
- 6*. Finn alla heltal x, y och z så att $x^2 + y^2 + z^2 = 2xyz$.
- 7*. Alla primtal utom ett (vilket?) är $\equiv 1$ eller $\equiv 3 \pmod{4}$. Visa att det finns oändligt många primtal som är $\equiv 3 \pmod{4}$.

Övning 6, ti 20 september

1. Avgör om sambandet $f(x) = x^2$ definierar en injektiv, surjektiv, bijektiv och/eller inverterbar funktion i följande fall
 - a. $f : \mathbb{R} \rightarrow \mathbb{R}$
 - b. $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$,
 - c. $f : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$
 - d. $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$. $\mathbb{R}_{\geq 0}$ betecknar här de icke-negativa reella talen $\{x \in \mathbb{R} \mid x \geq 0\}$.
2. Är $f : \mathbb{Z}_9 \rightarrow \mathbb{Z}_9$ injektiv, surjektiv, bijektiv och/eller inverterbar då
 - a. $f(x) = x^3 + 3x + 7$,
 - b. $f(x) = x^3 + 4x + 5$,
 - c. $f(x) = x^3 + 5x + 4$?
3. Ge exempel på mängder X, Y, Z och funktioner $f : X \rightarrow Y, g : Y \rightarrow Z$, så att sammansättningen $gf : X \rightarrow Z$ är en bijektion, trots att varken f eller g är det.
Lite svårare: Samma uppgift, men med kravet att $X = Y = Z$.
- 4a. Finns det $f : \mathbb{R} \rightarrow \mathbb{Q}$ och $g : \mathbb{Q} \rightarrow \mathbb{R}$, så att $gf : \mathbb{R} \rightarrow \mathbb{R}$ är en bijektion?
b. Finns det $f : \mathbb{Q} \rightarrow \mathbb{R}$ och $g : \mathbb{R} \rightarrow \mathbb{Q}$, så att $gf : \mathbb{Q} \rightarrow \mathbb{Q}$ är en bijektion?
- 5*. Enligt den sats av Cantor som presenterades på föreläsningen är potensmängden till $\mathbb{N}$ inte uppräknelig, dvs det finns överuppräkneligt många mängder av naturliga tal, $|\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$.
Visa att antalet **ändliga** mängder av naturliga tal är uppräkneligt, dvs

$$|\mathcal{P}_{fin}(\mathbb{N})| = |\mathbb{N}|,$$

där $\mathcal{P}_{fin}(\mathbb{N}) = \{A \mid A \subset \mathbb{N}, |A| < \infty\}$.

Ledning: Det finns en enkel bijektion mellan $\mathbb{N}$ och $\mathcal{P}_{fin}(\mathbb{N})$.

6*. (En klassisk illustration av märkligheter med oändligheten.)

Vi har en (stor) låda och ett (uppräkneligt) oändligt antal bollar, numrerade $0, 1, 2, \dots$. Från början ligger bara boll nummer 0 i lådan.

Vid varje tidpunkt $t = -\frac{1}{2^n}, n = 0, 1, 2, \dots$ tar vi ut och kastar bort den lägst numrerade bollen och lägger i alla återstående bollar upp till nummer 2^n .

Under allt kortare intervall kommer alltså följande bollar att ligga i lådan:

0; 1; 2; 3, 4; 4–8; 5–16; 6–32; 7–64; 8–128; ...

Hur många bollar ligger i lådan vid $t = 0$ (efter ett oändligt antal operationer)?

7. Hur många positiva delare till talet 2 646 000 finns det?

8. På hur många sätt kan 13 personer placeras på 13 (särskiljbara) stolar kring ett runt bord, utan att Lisa och Olle (som är bland de 13) sitter bredvid varandra?

9*. Vad är för $n \in \mathbb{N}$

$$\binom{n}{0} + \binom{n-1}{1} + \dots + \binom{n - \lfloor \frac{n}{2} \rfloor}{\lfloor \frac{n}{2} \rfloor} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k}?$$

Visa det. ($\lfloor \frac{n}{2} \rfloor$ är heltalsdelen av $\frac{n}{2}$, det största heltalet som är $\leq \frac{n}{2}$.)

10. Låt $a_1, a_2, \dots, a_n$ vara heltal. Visa att det finns en icke-tom delmängd av dem, vars summa är delbar med n .

11*. Låt $k > 0$ vara ett naturligt tal.

Visa att det finns ett $n > 0$, så att $k \mid F_n$, där F_n är fibonaccitalet nr n , som vanligt definierat av

$$\begin{cases} F_0 = 0, F_1 = 1 \\ F_{n+2} = F_{n+1} + F_n, \quad \text{alla } n \in \mathbb{N}. \end{cases}$$

Övning 7, on 28 september

1. Hur många följder med tre siffror och tre bokstäver bland A, B, C, D, E kan man bilda, om den skall inledas med en bokstav och ingen bokstav får vara med mer än en gång (t.ex. CD2A09, D07B0E, ABC444, men inte 123ABC eller B30A4B)?

2. Bland de totalt 26 medlemmarna (15 kvinnor och 11 män) i en förening skall en grupp med 5 representanter utses.

a. På hur många sätt kan gruppen sättas samman, om den skall innehålla minst 2 kvinnor och minst 1 man?

b. På hur många sätt går det om det dessutom finns två personer, fru A och herr B, som inte båda samtidigt kan vara med i gruppen av representanter?

3. Vi betraktar ord av längd 5 i alfabetet $\{0, 1, 2, \dots, 9\}$, dvs femsiffriga tal som eventuellt kan inledas med en eller flera 0:or.

a. Hur många sådana ord finns det?

b. Hur många av dem har strikt växande siffror?

c. Hur många av dem har växande (inte säkert strikt) siffror?

d. Hur många av dem har växande eller avtagande (ingendera säkert strikt) siffror?

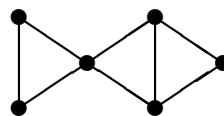
4. Finn arean för en sfärisk triangel med vinklarna α, β, γ på en sfär med radie R . En sfärisk triangel har delar av tre storcirklar som sidor och en sfär med radie R har arean $4\pi R^2$.

5. Låt grafen $G = (V, E)$ vara graferna $G_1 = (V_1, E_1)$ och $G_2 = (V_2, E_2)$ "hopklistrade längs en K_m ", dvs $V = V_1 \cup V_2$, $E = E_1 \cup E_2$ och $(V_1 \cap V_2, E_1 \cap E_2)$ är en graf som är isomorf med den fullständiga grafen K_m .

Visa att det kromatiska polynomet $P_G(\lambda)$ ges av

$$P_G(\lambda) = \frac{P_{G_1}(\lambda) \cdot P_{G_2}(\lambda)}{\lambda(\lambda-1) \dots (\lambda-m+1)}.$$

Illustrera med $P_G(\lambda)$ för grafen G här till höger.



Övning 8, fr 7 oktober

1. Den binära relationen $\mathcal{R}$ på mängden $X = \{a, b, c, d\}$ ges av

$$\mathcal{R} = \{(a, a), (a, b), (b, b), (c, c), (c, d), (d, c)\}.$$

Avgör om $\mathcal{R}$ är reflexiv, symmetrisk, anti-symmetrisk och/eller transitiv.

2. Låt $X = \{a, b, c, d\}$ och ge exempel på en relation på X som är

- a. reflexiv och symmetrisk, men inte transitiv,
- b. reflexiv och transitiv, men inte symmetrisk,
- c. symmetrisk och transitiv, men inte reflexiv.

3. I en familj bestående av 4 personer förekommer alla de sju dödssynderna (högmot, girighet, vällust, avund, frosseri, vrede och lättja). Varje person hemfaller tyvärr åt minst en av synderna, men dessbättre förekommer ingen av synderna hos mer än en av dem.

- a. På hur många sätt kan synderna vara fördelade?
- b. Hur många fördelningar är möjliga om ingen hemfaller åt både girighet och lättja?

4. På hur många sätt kan 7 kulor fördelas på 4 lådor i följande fall?

- a. Särskiljbara kulor, särskiljbara lådor, lådor får vara tomma.
- b. Särskiljbara kulor, särskiljbara lådor, lådor får inte vara tomma.
- c. Identiska kulor, särskiljbara lådor, lådor får vara tomma.
- d. Identiska kulor, särskiljbara lådor, lådor får inte vara tomma.
- e. Särskiljbara kulor, identiska lådor, lådor får vara tomma.
- f. Särskiljbara kulor, identiska lådor, lådor får inte vara tomma.

5*. Finns det andra sätt (än 1,2,3,4,5,6 på båda) att fördela ögonen på två tärningar, så att sannolikheten för varje totalt antal ögon blir samma som för vanliga tärningar (dvs det skall gå att få totalt 4 på 3 sätt, att få totalt 11 på 2 sätt osv)? Om det går, beskriv alla möjligheter.

Tärningarna skall ha normal kubisk form, inte vara viktade och antalet ögon på varje sida skall vara ett positivt heltal.

Övning 9, on 12 oktober

1. Låt φ och ψ beteckna nedanstående permutationer (givna på tvåradsform) på mängden $\{1, 2, 3, 4, 5, 6, 7, 8\}$

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 8 & 5 & 2 & 4 & 3 & 7 \end{pmatrix}, \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 4 & 1 & 2 & 6 & 3 & 5 \end{pmatrix}$$

- a. Skriv permutationerna φ och ψ som produkter av disjunkta cykler.
b. Beräkna $\varphi\psi$, $\psi\varphi$, φ^{-1} och ψ^{-1} , dels på tvåradsform och dels på cykelform.
2. Finn permutationer χ, ψ så att $\pi\chi = \sigma$, $\psi\pi = \sigma$, med

$$\pi = (1\ 7\ 2)(3\ 6\ 9\ 8)(4\ 5), \quad \sigma = (1\ 5\ 3\ 9\ 6\ 8)(2\ 4) \quad (\text{cykelform}).$$

Vilka av χ , π , ψ och σ är konjugerade? Varför?

Avgör om χ , π , ψ och σ är jämna eller udda permutationer.

3. I en radhuslänga med sex hus (med nr, i ordning, 1–6) bor sex gifta par (vart och ett bestående av en kvinna och en man), ett par i varje hus.

Var och en av kvinnorna har också (precis) en bror bland de sex männen och omvänt. Ingen bor granne med, eller är gift med, sin syster eller bror.

Anders har bara ett grannhus och bara en svåger (han bor i det ena gavelhuset, nr 1, och hans frus bror är hans systers man). Anders granne Börje däremot, har både två grannhus (förstås) och två svågrar.

a. I vilket hus bor Anders syster Anna?

b. I det andra gavelhuset, nr 6, bor Cecilia med sin man. Börjes syster heter Birgitta. Ange var vart hus frus bror bor.

Övning 10, to 3 november

1. Det går att fylla i vidstående tabell så att den blir multiplikationstabellen för en grupp, dess grupptabell. Gör det.

a. Är gruppen abelsk?

b. Vilket element är identitetsselement?

c. Bestäm inverser till alla element.

d. Bestäm ordningen för alla element och alla cykliska delgrupper till gruppen.

e. Beräkna $a * b * c * d * f * g$. (Behövs här inga parenteser?)

2. Låt G vara en grupp med identitetsselementet 1 och $a, b, c \in G$.

a. Givet att $x \in G$ uppfyller $\begin{cases} ax^2 = b \\ x^3 = 1, \end{cases}$ vad är x ?

b. Givet att $x \in G$ uppfyller $\begin{cases} (xax)^3 = bx \\ x^2a = (xa)^{-1}, \end{cases}$ vad är x ?

c. Visa $bac = a^{-1} \Rightarrow cab = a^{-1}$.

d. Visa $(abc)^{-1} = abc \Rightarrow (bca)^{-1} = bca$.

e. Visa att $a^3 = 1 \Rightarrow a$ har en kvadratrot, dvs för ett $r \in G$ gäller $a = r^2$.

f. Visa att $b^2ab = a^{-1} \Rightarrow a$ har en kubikrot, dvs för ett $s \in G$ gäller $a = s^3$.

3. $(U(\mathbb{Z}_8), \cdot)$ och $(U(\mathbb{Z}_{14}), \cdot)$ är grupper. $U(\mathbb{Z}_n)$ består av de inverterbara elementen i $\mathbb{Z}_n$. Undersök om någon av grupperna är cyklisk.

4. Gruppen $(\mathbb{Z}_{13} \setminus \{0\}, \cdot)$ är cyklisk. Bestäm alla dess generatorer.

5. Minns att den **direkta produkten** av två grupper $(G_1, *_1)$ och $(G_2, *_2)$ definieras som gruppen $(G_1 \times G_2, \circ)$ där för $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$:

$$(g_1, g_2) \circ (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2).$$

a. Låt $g_1 \in G_1$, $g_2 \in G_2$ ha ordningar $o(g_i) = m_i$.

Vad är ordningen för $(g_1, g_2) \in G_1 \times G_2$?

b. För vilka $m, n \in \mathbb{Z}_+$ är $(\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +) \approx (\mathbb{Z}_{mn}, +)$?

c. Gäller för alla grupper G_1 och G_2 att $G_1 \times G_2 \approx G_2 \times G_1$?

d. Om H_1 , H_2 är delgrupper till G_1 respektive G_2 , måste $H_1 \times H_2$ vara en delgrupp till $G_1 \times G_2$?

$*$	a	b	c	d	f	g
a			c			
b					d	c
c		f		g		
d				a		b
f		c	d			
g					a	

Övning 11, to 10 november

1. En given grupp G har delgrupper H och K med 39 respektive 40 element. Bestäm m , det minsta möjliga värdet för $|G|$.

Konstruera också en grupp G med m element som har delgrupper med 39 resp. 40 element.

2. Visa att vidstående tabell inte kan fyllas i så att den blir en grupptabell.

$*$	a	b	c	d	f	g	h	i	k
a	a	b							
b	b	a							
c									
d									
f									
g									
h									
i									
k									

3. Låt G vara S_4 , gruppen av permutationer av $\{1, 2, 3, 4\}$, och $N \subset G$ ges av (med elementen i cykelform) $N = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

a. Kalla hörnen i en regelbunden tetraeder för 1, 2, 3, 4. Elementen i G svarar då mot stela (dvs avståndsbevarande) avbildningar av rummet, vilka lämnar tetraedern invariant men permuterar hörnen.

Ange för varje konjugatklass i G hurdana avbildningar dess element motsvarar.

b. Vilken typ av avbildning motsvarar jämna respektive udda permutationer i G ?

c. Visa att N är en **normal** delgrupp till G och beskriv kvotgruppen G/N (dvs ange en känd grupp som är isomorf med G/N).

Övning 12, fr 18 november

1. Hur många element har gruppen av oktaederns symmetrirotationer? (Oktaedern är ju den platonska kropp vars sidor är 8 liksidiga trianglar.)

Finn storleken för dels stabilisator och dels bana för ett hörn och för mittpunkten av en sidoyta.

2. Pelle skall tillverka kvadratiske brickor att sälja i sin heminredningsbutik. Brickorna har färgade (gula, röda eller blå) kulor i de fyra hörnen. Hur många väsentligt olika (dvs så att de inte blir lika hur man än vrider dem) sådana brickor finns det i följande fall?

a. Brickornas ovansidor och undersidor är lika, så de ser likadana ut om man vänder på dem.

b. Brickornas ovansidor och undersidor är olika.

c. Vad blir svaren i a. och b. om antalet olika färger på kulorna är k ?

3. Av sex lika långa sugrör formas en käck prydnad i form av en tetraeder (med sugrören som kanter). På hur många väsentligt olika sätt (dvs så att de inte blir lika hur man än vrider dem i rummet) kan det göras, om man har sugrör av k olika färger att tillgå?

Övning 15, to 15 december

1. Du skall tillverka ett RSA-krypto med parametern $n = 77$.
 - a. Förklara varför du inte kan använda parametern $e = 45$.
 - b. Du väljer $e = 13$. Bestäm d .
 - c. Kryptera meddelandet $a = 3$.
 - d. Dekryptera meddelandet $b = 2$.
2. Du betraktar ett RSA-krypto med $n = 265$ och $e = 37$. Försök dekryptera meddelandet $b = 2$.
3. Du har ett RSA-krypto med $n = 1333 (= 31 \cdot 43)$ och $e = 143$. Kryptera meddelandena $x = 718, 719$.
Kontrollera resultaten genom att finna rätt d -värde och dekryptera.
4. Använd ett fermatstest för att visa att talet 63 inte är ett primtal.
5. Beräkna $43^{139802} \pmod{101}$.
6. Beräkna $43^{139802} \pmod{341}$.

Blandade exempel (för den roade) (en del av dem är svåra)

Till dessa kommer det inte att läggas ut lösningar på kurssidan, men den som vill är välkommen att komma och diskutera dem med läraren.

- 1**. Visa för fibonaccitalen $\{F_n\}_{n=0}^\infty$ att $\text{sgd}(F_m, F_n) = F_{\text{sgd}(m,n)}$.
- 2**. Två fyrar blinkar med intervall α respektive β (minuter). α och β är irrationella tal sådana att $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ (dvs i medeltal kommer ett blink per minut). Visa att om de båda blinkar vid tiden $t = 0$ kommer det under "heltalsminuten" mellan $n - 1$ och n precis ett blink, för alla heltal $n > 1$.
- 3**. Vilka siffror är de 100:e decimalerna i $(\sqrt{2}+1)^{1000}$ respektive $(\sqrt{2}+1)^{1001}$?
- 4**. På en föreläsning visades att om man utgår från 6 punkter och mellan varje par av dem drar antingen en röd eller en blå linje, uppstår minst en enfärgad triangel.
 - a. Visa att det i själva verket blir minst två enfärgade trianglar.
 - b. Visa att om man i stället utgår från 10 punkter och gör på samma sätt, uppstår antingen en helt röd triangel eller en helt blå "tetraeder" (dvs fyra punkter som alla parvis är förbundna med blå linjer).
 - c. Visa att det i **b** räcker med 9 punkter.
- 5**. Av en cirkulär tårta, med (choklad)brun ovansida och (tårtbottens)vit undersida, skärs bitar med medelpunktsvinkel x intill varandra. Då en bit skurits, vänds den genast upp och ner och läggs in på sin gamla plats (där den på magiskt vis växer fast igen). Detta upprepas runt, runt tårtan.
Låt $nx < 2\pi < (n+1)x$, $n \in \mathbb{Z}_+$. Efter $k \leq n$ vändningar är tårtans ovansida alltså vit på en sektor med vinkel kx , resten brun. Efter $n+1$ vändningar är den vit, bortsett från en mindre brun sektor (som vänts två gånger).
 - a. Kommer tårtan(s ovansida) någonsin att bli helt vit? I så fall, efter hur många vändningar?
 - b. Kommer tårtan(s ovansida) någonsin att bli helt brun igen? I så fall, efter hur många vändningar?

6.** Givet fyra linjer i planet, inga två parallella och inga tre genom samma punkt.

Längs varje linje kryper en lus, var och en med sin konstanta hastighet. Visa att om två löss möts (utan att stanna upp) vid fem av linjernas skärningspunkter, så möts också två löss vid den sjätte skärningspunkten.

7.** I en population med speciella (matematiska) kameleonter finns vid ett tillfälle 116 röda, 97 gula och 84 blå individer.

När två olikfärgade av dessa kameleonter möts, byter de båda färg till den tredje färgen. Kan färgförändringarna upphöra, dvs kan det hända att alla kameleonterna till sist får samma färg?

8.** 100 personer (alla med olika namn) får ett märkligt erbjudande.

I ett rum står, får de veta, 100 lådor, numrerade från 1 till 100. Var och en av personerna får skriva sitt namn på en lapp och de hundra lapparna fördelas slumpmässigt i lådorna, en i varje låda.

Varje person skall sedan gå in i rummet och läsa namnet i en av lådorna. Om det inte är hans eget namn får han försöka en annan låda osv. Om han finner sitt eget namn genom att titta på högst 50 av dem, har han lyckats och skall lämna rummet precis som han fann det (och inte kommunicera med de andra) och nästa person komma in och försöka.

Om de **alla** lyckas, dvs finner lappen med sitt eget namn, får de säckvis med guldpenningar att dela på, annars (om en enda av dem misslyckas) får de ingenting.

a. Vad är sannolikheten att de skall få pengarna om de inte heller får ha kontakt innan de går in (och saknar andra ledtrådar, typ röntgenblick)?

b. Visa att de om de i förväg får bestämma en gemensam strategi kan öka sannolikheten att de skall få pengarna till över 30%(!).

9.** 100 personer har biljett till varsin av de 100 platserna i en biosalong. Den som går in först har dock tappat sin biljett och sätter sig på en slumpmässigt (likafördelat) vald plats. Var och en av de övriga sätter sig på sin egen plats om den är ledig, annars på en lika slumpmässigt vald (ledig) plats.

Vad är sannolikheten att den som kommer in sist hamnar på sin egen plats?

Att den k :e personen från slutet hamnar rätt?

10.** Tre personer får veta att de samtidigt skall få varsin hatt på huvudet, var och en med sannolikhet $\frac{1}{2}$ en röd och sannolikhet $\frac{1}{2}$ en blå hatt, de olika hattarnas färger oberoende. De kan se de två andras hattar, men inte sin egen. De ges chansen att gissa färgen på sin egen hatt, men kan avstå från att gissa om de vill. Om (och endast om) minst en gissar rätt färg på sin egen hatt och ingen gissar fel, får de (alla) ett pris. De får inte veta om eller vad de övriga gissar.

Hur stor sannolikhet att vinna kan de få, om de i förväg kan komma överens om en strategi för gissandet? Om de t.ex. bestämmer att A skall gissa ”röd” och att B och C skall avstå, har de tydligen sannolikheten $\frac{1}{2}$ att vinna, men kan de öka sannolikheten?

Hur stor sannolikhet kan en bra strategi ge om de är femton personer?