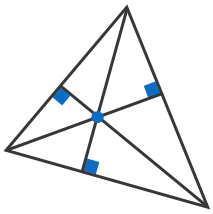


HÖJDPUNKTEN 2024

Lösningsförslag öppen tavling

UVS MATEMATIKER

Skrivtid: 3 timmar
Hjälpmedel: endast penna, sudd, passare och linjal
Motivera alla lösningar. Enbart svar ger inga pöang om inte annat anges.

Problem 1. Låt n vara ett positivit heltal. Visa att det finns en följd $\{a_0, a_1, a_2, \ldots, a_n\}$ av heltal större än 1 sådana att

$$a_0! \cdot a_1! \cdot a_2! \cdots a_{n-1}! = a_n!.$$

Lösningsförslag. Vi använder induktion. Basfall: Om $n = 1$ så löses ekvationen trivialt genom att sätta $a_0 = a_1$. Anta nu att $a_0! \cdot a_1! \cdots a_{n-1}! = a_n!$. För att skapa en liknande produkt med en till faktor, skriv

$$(a_n!)! = a_n! \cdot (a_n! - 1)! = a_0! \cdot a_1! \cdots a_{n-1}!(a_n! - 1)!$$

Denna metod låter oss induktivt skapa produkter med godtyckligt många faktorer. □

Kommentar: Fakulteter känns väldigt kombinatoriska, så en rimlig fråga är om det finns någon trevlig kombinatorisk tolkning av problemet. Lösningen ovan är så enkel att vi förmodligen inte bör hoppas på något mer koncist, men det är alltid trevligt när det finns flera sätt att lösa ett problem. Och faktiskt, det finns en smart metod att göra detta utan att skriva ner nästan några ekvationer!

Först observera att ett naturligt tal är en fakultet om och endast om det är antalet sätt att ordna elementen i en ändlig mängd S. Nu låt

- *S_0 vara mängden $1, 2, 3, ..., a$*
- *S_{k+1} vara mängden av permutationer av elementen i S_k*

Uppenbarligen är storleken på S_{k+1} en fakultet, enligt observationen ovan. Men det är också lika med antalet sätt att välja det första elementet från S_k, vilket är exakt $|S_k|$, gånger antalet sätt att permutera de resterande elementen i S_k, vilket också är en fakultet enligt observationen ovan. Genom induktion får vi att $|S_k|$ är en produkt av k fakulteter, och således är $|S_{k+1}|$ en produkt av $k + 1$ fakulteter. Därmed är vi klara!

Problem 2. En ändlig mängd med positiva heltal $\{k_1, k_2, \ldots, k_n\}$ är given. Visa att det finns ett positivt heltal m så att talen $mk_1, mk_2, \ldots, mk_n$ alla har olika antal delare.

Lösningsförslag (1). Enligt aritmetikens fundamentalteorem kan vi hitta ett heltal r och en matris $A \in \mathbb{N}^{n\times r}$ så att $k_i = p_1^{A_{i,1}} p_2^{A_{i,2}} \cdots p_r^{A_{i,r}}$ för varje $i \in \{1, \ldots, n\}$. Om primtalsfaktoriseringen av m är $p_1^{\mu_1} p_2^{\mu_2} \cdots p_r^{\mu_r}$ är antalet delare av mk_i då

$$d(mk_i) = \prod_{j=1}^{r} (\mu_j + A_{i,j} + 1).$$

Hur kan vi göra alla dessa produkter olika? Låt oss konstruera $\mu_1, \ldots, \mu_r$ så att $d(mk_i)$ är delbart med en unik uppsättning primtal för varje i. Låt $A_{\max}$ vara det största elementet i A, och låt $B \in \mathbb{N}^{n\times r}$ vara en matris av parvis olika primtal som alla är större än $A_{\max}+1$. Enligt den kinesiska restsatsen kan vi välja $\mu_1, \ldots, \mu_r$ så att för alla $i \in \{1, \ldots, n\}$ och $j_1, j_2 \in \{1, \ldots, r\}$,

$$\begin{cases} \mu_{j_2} \equiv -1 - A_{i,j_2} \pmod{B_{i,j_1}} & \text{om} \quad j_1 = j_2, \\ \mu_{j_2} \equiv 0 \pmod{B_{i,j_1}} & \text{om} \quad j_1 \neq j_2. \end{cases} \tag{1}$$

Vi hävdar att detta gör att $mk_1, mk_2, \ldots, mk_n$ har olika antal delare som önskat. Betrakta två godtyckliga k_{i_1} och k_{i_2} där $i_1 \neq i_2$. Eftersom k_{i_1} och k_{i_2} har olika primtalsfaktoriseringar måste det finnas ett tal j_1 så att $A_{i_1,j_1} \neq A_{i_2,j_1}$. Från (1) får vi att

$$\begin{aligned} &\mu_{j_1} A_{i,j_1} + 1 \equiv 0 \pmod{B_{i,j_1}} \\ &\implies B_{i_1,j_1} \mid d(mk_{i_1}) \end{aligned}$$

Vi visar nu att $B_{i_1,j_1} \nmid d(mk_{i_2})$ genom att visa att B_{i_1,j_1} inte delar $\mu_{j_2} + A_{i_2,j_2} + 1$ för något j_2. Om $j_2 \neq j_1$, får vi

$$\mu_{j_2} + A_{i_2,j_2} + 1 \equiv A_{i_2,j_2} + 1 \pmod{B_{i_1,j_1}},$$

vilket, eftersom $A_{i_2,j_2} + 1 \leq A_{\max} + 1 < B_{i_1,j_1}$, innebär att

$$B_{i_1,j_1} \nmid \mu_{j_2} + A_{i_2,j_2} + 1.$$

Detta lämnar en sista faktor av $d(mk_{i_2})$ att kontrollera, nämligen $\mu_{j_1} + A_{i_2,j_1} + 1$. För detta tillämpar vi första fallet av (1) och får

$$\mu_{j_1} + A_{i_2,j_1} + 1 \equiv A_{i_2,j_1} - A_{i_1,j_1}$$

vilket som tidigare inte kan vara delbart med B_{i_1,j_1}, eftersom $A_{i_2,j_1} - A_{i_1,j_1}$ är nollskilt och har en magnitud som inte är större än $A_{\max}$ □

Lösningsförslag (2). Vi kan också visa detta med induktion på n. Detta är vår plan:

Basfall: För $n = 1$ finns det inget att visa.

Induktionssteg: Anta att vi har löst problemet för $n-1$, det vill säga att vi kan välja ett tal c så att $ck_1, ..., ck_{n-1}$ har olika antal delare. Vår plan härifrån är att välja ett primtal p (vi kommer att bestämma vilket senare), och multiplicera $k_1, ..., k_n$ med $p^\alpha c$ för något icke-negativt heltal α. Nedan kommer vi att visa att det alltid finns ett val av p och α för vilka $p^\alpha ck_1, ..., p^\alpha ck_n$ har parvis olika antal delare, vilket avslutar induktionen.

Innan vi bevisar induktionssteget, låt oss introducera viss notation. Anta att vi redan har valt vårt primtal p.

- Låt d_i beteckna antalet delare av ck_i, för $i = 1, 2, ..., n$.
- Låt $\alpha_i - 1$ beteckna antalet gånger som ck_i är delbart med primtalet p (så α_i är en *mer* än antalet gånger p delar ck_i. Vi gör detta underliga val för att förenkla algebran senare).

Det är lätt att visa att antalet delare av ett tal med primtalsfaktorisering $q_1^{\beta_1} \cdot ... \cdot q_m^{\beta_m}$ är exakt $(\beta_1 + 1) \cdot ... \cdot (\beta_m + 1)$ (detta beror på att det finns $\beta_i + 1$ sätt att välja antalet gånger som q_i förekommer i faktoriseringen av vårt delare). Därför, eftersom antalet gånger som p delar $p^\alpha ck_i$ är $\alpha + \alpha_i - 1$, får vi:

$$\text{antal delare av } p^\alpha ck_i = d_i \frac{\alpha + \alpha_i}{\alpha_i}$$

Antag att det finns några $i \neq j$ sådana att

$$\begin{aligned} & d_i \frac{\alpha + \alpha_i}{\alpha_i} = d_j \frac{\alpha + \alpha_j}{\alpha_j} \\ \iff \quad & d_i(\alpha + \alpha_i)\alpha_j = d_j(\alpha + \alpha_j)\alpha_i \\ \iff \quad & \alpha(d_i\alpha_j - d_j\alpha_i) = \alpha_i\alpha_j(d_j - d_i) \end{aligned}$$

Om $d_i\alpha_j - d_j\alpha_i \neq 0$, finns det exakt ett (rationellt) α för vilket detta är sant. Om $d_i\alpha_j - d_j\alpha_i = 0$, är vänsterledet alltid 0 oavsett vårt val av α, och det kan därför endast vara sant om $d_j = d_i$. Vi kan alltså dra slutsatsen att för varje par $i \neq j$, antingen:

- $d_i\alpha_j - d_j\alpha_i \neq 0$ och det finns exakt en α som vi måste undvika, eller
- $d_i\alpha_j - d_j\alpha_i = 0$ och $d_i \neq d_j$, i vilket fall vilket α som helst fungerar, eller
- $d_i\alpha_j - d_j\alpha_i = 0$ *och* $d_i = d_j$, i vilket fall det inte finns något α som är tillräckligt bra.

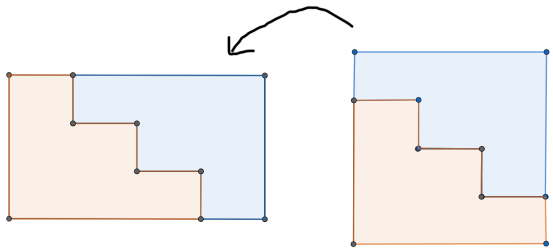
Eftersom vi alltid kan undvika ändligt många val av α, är det enda vi måste se till att det inte finns något $i \neq j$ för vilket vi hamnar i det tredje fallet. Enligt induktion vet vi redan att $d_i \neq d_j$ för $i, j \leq n - 1$. Detta innebär också att det högst finns ett i sådant att $d_n = d_i$, och för att avsluta måste vi bara välja p så att $d_i\alpha_n - d_n\alpha_i \neq 0$ för det ena i. Men vi vet att $d_i = d_n$, så detta är ekvivalent med att välja ett p sådant att $\alpha_i \neq \alpha_n$. Ett sådant p finns alltid enligt vårt antagande om att $k_1 \neq k_n$. Beviset är således färdigt. □

Problem 3.

(a) Tilda har en rektangulär bräda som är 1 dm lång och 16/9 dm bred. Visa att hon kan såga isär den i två delar som kan sättas ihop till en kvadrat.

(b) Hitta oändligt många tal x sådana att en 1 dm gånger x dm bräda kan sågas isär i två delar som kan sättas ihop till en kvadrat.

Lösningsförslag. Del (a): Den kan sedan byggas om till en kvadrat enligt figuren nedan:



Del (b): Från en kvadrat kan man skapa en rektangel med följande metod:

1. Dela upp kvadraten i ett $n \times (n+1)$ rutnät.
2. Rita en trappa längs rutnätet som delar upp kvadraten i två lika stora delar.
3. Flytta ner den översta delen ett trappsteg.

Den resulterande rektangeln består då av ett $n \times (n+1)$ rutnät av $n \times (n+1)$ rutor. Dessa förhållandet mellan dess sidor blir därmed $(n+1)^2 : n^2$. Om vi sätter $x = \frac{(n+1)^2}{n^2}$ för något heltal n så kan vi utföra samma process baklänges och på så vis transformera en $1 \times x$ rektangel till en $\frac{n+1}{n} \times \frac{n+1}{n}$ kvadrat. För följande värden på x är alltså möjliga:

$$\frac{4}{1}, \frac{9}{4}, \frac{16}{9}, \frac{25}{16}, \ldots, \frac{(n+1)^2}{n^2}, \ldots$$

□

Problem 4. Ett polynom kallas *inversigt* om för alla rötter a så är $1/a$ också en rot. Låt f vara ett irreducibelt rationellt polynom av grad ≥ 2. Antag att f har en rot $b \in \mathbb{C}$ med $|b| = 1$. Visa att f är inversig och har jämn grad.

Lösningsförslag (1). Låt $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Först påstår vi att f inte har några dubbelrötter. Detta är en sats om irreducibla polynom som kan bevisas på följande sätt: Låt a vara en rot till f med multiplicitet åtminstone 2. Då kan f skrivas som $f(x) = (x-a)^2 q(x)$ för något rationellt polynom q. Då har vi att derivatan $f'(x) = 2(x-a)q(x) + (x-a)^2 q'(x)$ också har a som rot. Så den största gemensamma delaren $\gcd(f, f')$ har grad minst 1, men då f är irreducibel måste den vara lika med f. Det är dock omöjligt för f att vara en delare till f' då den senare har lägre grad.

Nu betraktar vi det rationella polynomet $g(x) = x^n f(1/x)$. Om α är en rot till f så är $\frac{1}{\alpha}$ en rot till g. Eftersom f och g har samma grad, och f inte har några dubbelrötter, så är rötterna till g exakt de multiplikativa inverserna till rötterna av f.

Betrakta nu talet b. Notera att b inte kan vara 1 eller -1, då f annars hade haft grad 1. Alltså är b icke-reellt, och eftersom f har rationella koefficienter måste även $\overline{b} = \frac{1}{b}$ vara en rot till f. Vi har alltså att b och $\frac{1}{b}$ är rötter till både f och g. Men då måste den största gemensamma delaren $\gcd(f, g)$ ha grad minst 2, och därför vara lika med f. Då f och g har samma grad måste vi ha $f = g$, så att f är inversigt. Att f har jämn grad följer av att det inte har några dubbelrötter och inte har rötter 1 eller -1, så att man kan para ihop varje rot av f till sin multiplikativa invers. □

Lösningsförslag (2 (Galoisteori)**).** Vi visar att f inte har dubbelrötter och att $\frac{1}{b}$ är en rot till f på samma sätt som i lösningsförslag 1. Vi använder följande lemma från galoisteori.

Lemma 1. *Om α och β är rötter till samma irreducibla polynom över $\mathbb{Q}$, så finns det en funktion $\varphi : \mathbb{C} \to \mathbb{C}$ så att, för alla $a, b \in \mathbb{C}$ och för alla $q \in \mathbb{Q}$:*

- $\varphi(\alpha) = \beta$
- $\varphi(a + b) = \varphi(a) + \varphi(b)$.
- $\varphi(ab) = \varphi(a)\varphi(b)$.
- *φ är bijektiv.*
- $\varphi(q) = q$.

Med andra ord så är φ en $\mathbb{Q}$-bevarande automorfism av $\mathbb{C}$ som skickar α till β.

Låt a vara en rot till f som inte är b eller $1/b$. Vi vill visa att $1/a$ även är en rot till f. Vi använder lemma 1 för att hitta:

- φ: en $\mathbb{Q}$-bevarande automorfism av $\mathbb{C}$ som skickar a till b.
- ψ: en $\mathbb{Q}$-bevarande automorfism av $\mathbb{C}$ som skickar b till $\frac{1}{b}$.

Vi påstår att $h(a) := \varphi^{-1} \circ \psi \circ \varphi(a) = \frac{1}{a}$. Vi beräknar

$$\begin{aligned} a(\varphi^{-1} \circ \psi \circ \varphi)(a) = 1 &\iff \varphi(a(\varphi^{-1} \circ \psi \circ \varphi)(a)) = \varphi(1) = 1 \\ &\iff \varphi(a)\psi(\varphi(a)) = 1 \\ &\iff b \cdot \frac{1}{b} = 1 \end{aligned}$$

Notera nu att h är en $\mathbb{Q}$-bevarande automorfism av $\mathbb{C}$. Vi har alltså att

$$0 = h(0) = h(f(a)) = f(h(a)) = f\left(\frac{1}{a}\right)$$

så att $\frac{1}{a}$ också är en rot av f. Vi har alltså att f är inversigt. Att f har jämn grad visas på samma sätt som i lösningsförslag 1.

□

Problem 5. Ung Vetenskapssport har växt! Vi är nu många som är engagerade och vill ha tillgång till alla UVS olika kanaler för att nå ut till våra fantastiska medlemmar. Men ju fler som får tillgång, desto större blir säkerhetsrisken; vad händer om någon får sitt konto hackat? Vi behöver nu er hjälp för att lösa detta problem!
Det är n personer som vill ha tillgång till UVS konton. Vi vill hitta på ett system som garanterar att om $1 \leq m \leq n$ personer tillsammans vill logga in så kan de göra det, men om $m-1$ personer vill logga in så har det inte nog med information för att göra det.
Efter långa diskussioner kom vi fram till följande förslag. Vi väljer ett lösenord med M siffror $x_1x_2...x_M$, och avslöjar sedan någon delmängd av dessa siffror för varje person som vill ha tillgång till våra konton.

(a) Är det möjligt att dela ut siffrorna så att kravet ovan är uppfyllt?

(b) Om svaret är ja, vilket är det minsta M för vilket det är möjligt (uttryckt i n och m)?

Lösningsförslag.

(a) Ja. Skapa ett lösenord med $\binom{n}{m-1} = \binom{n}{n-m+1}$ siffror och visa en siffra för varje mängd av $n-m+1$ personer. Om $m-1$ personer träffas så kommer de sakna siffran som resterande $n-m+1$ personer känner till. Men om m personer träffas så kommer åtminstone en person från varje mängd av $n-m+1$ personer vara med i träffen.

(b) Vi påstår att konstruktionen ovan är optimal. Anta därför att lösenordet består av färre än $\binom{n}{m-1}$ siffror och att varje mängd av $m-1$ personer har en siffra som de inte känner till. Det finns då (enligt lådprincipen) två olika mängder av $m-1$ personer som saknar samma siffra. Unionen av dessa två mängder (som tillsammas har minst m personer) saknar alltså också en siffra. Detta bevisar att lösenordet måste ha åtminstone $\binom{n}{m-1}$ siffror.

□

Kommentar. En naturlig fråga är vad som händer om vi har mer komplicerade krav än "vilken m personer som helst bör tillåtas att gå in, men inte $m-1$ personer". Vad händer om till exempel styrelsen ska ha speciella befogenheter som tillåter dem att gå in även om endast två av dem är närvarande, men om ingen styrelsemedlem är närvarande kräver vi åtminstone tio personer för att vara närvarande? Lösningen ovan hanterar sådana frågor ganska bra också.
Säg att vi har en lista $S_1, S_2, ..., S_r \subset 1, 2, ..., n$ av grupper av personer som ska tillåtas att gå in (där vi numrerar de personer som vill ha tillgång som $1, 2, ..., n$), och anta att varje delmängd av $1, 2, ..., n$ som inte finns med i listan inte ska få tillträde. Då är ett uppenbart krav för att det ska finnas en lösning på vårt problem att $S_i \subset B \implies B = S_j$ för något j (eller ekvivalent: om en mängd B inte finns med i listan, kan ingen delmängd av B heller finnas med i listan). Men detta är faktiskt tillräckligt! Om listan över mängder som inte finns med i listan är $R_1, ..., R_m$, så kan vi välja en siffra för varje mängd $1, ..., n \setminus R_i$ och ge den endast till dessa personer. ...

Problem 6. Låt $\triangle ABC$ vara en triangel sådan att $|AB| < |AC|$. Låt B' vara punkten på sidan AC sådan att $|AB| = |AB'|$. Låt D vara en punkt sådan att $|AB| = |AD|$, skild från B och B'. Den omskrivna cirkeln till $\triangle B'CD$ skär linjen BC en andra gång i punkten E, skild från C. Bevisa att det existerar en fixpunkt K oberoende av D, sådan att linjen DE går genom K för alla möjliga val av punkten D.

Lösningsförslag. Låt ω beteckna cirkeln med medelpunkt A och som innehåller B, B' och D. Låt M vara projektionen av B' på BC och låt K vara (den andra) skärningspunkten av ω och $B'M$. Låt även L vara (den andra) skärningspunkten av ω och AB'. Eftersom LB' är en diameter till ω så är $\angle LKB' = 90°$, därav $\triangle LKB' \sim CMB'$. Alltså är (riktade vinklar)

$$\angle KDB' = \angle KLB' = \angle MCB' = \angle ECB' = \angle EDB'.$$

vilket innebär att K, D och E ligger på samma linje. □

Problem 7. Låt $\triangle ABC$ vara en triangel med omskriven cirkel Ω, och låt dess inskrivna cirkel ha medelpunkt I. Låt ω vara cirkeln med medelpunkt A som passerar genom I. Låt ω skära Ω i punkterna P och Q. Låt X vara skärningspunkten mellan linjerna PQ och BC. Låt ω_P och ω_Q vara de omskrivna cirklarna till $\triangle PXI$ respektive $\triangle QXI$. Låt ω_P och ω_Q skära linjen BC igen i punkterna P' respektive Q', skilda från X. Bevisa att linjerna PP' och QQ' skär varandra på ω.

Lösningsförslag. Låt $Y = PP' \cap QQ'$. Då blir (riktade vinklar)

$$\begin{aligned}\angle PYQ &= \angle P'YQ' = \angle YP'Q' + \angle P'Q'Y \\ &= \angle PP'X + \angle XQ'Q = \angle PIX + \angle XIQ \\ &= \angle PIQ.\end{aligned}$$

Alltså ligger Y på ω, vilket skulle visas. □

Problem 8. Kevin vill simulera en tärning med n sidor. Till sin hjälp har han en $p-$sidig tärning för varje primtal $p < n$. Eftersom Kevin inte har hur mycket tid som helst för att slå tärningar, så vill han gärna minimera väntevärdet på antalet tärningskast. *Anmärkning: Detta problem är värt 10 poäng totalt.*

(a) Visa att om $n = pq$ för två primtal p, q (som inte nödvändigtvis är olika), så kan Kevin simulera en $n-$sidig tärning med exakt exakt 2 tärningskast. [1 poäng]

(b) Visa att han alltid behöver minst 2 kast, men att han kan uppnå ett väntevärde som är mindre än 3 för alla $n \geq 12$. [2 poäng]

(c) Visa att det finns oändligt många tal n som inte är på formen pq för två primtal p och q, sådana att Kevin kan simulera en $n-$sidig tärning med exakt 2 tärningskast. [7 poäng]

Lösningsförslag. (a) Låt oss först kasta en tärning med p sidor och sedan omedelbart en tärning med q sidor. Det finns då pq olika möjliga utfall, nämligen $(1,1),(1,2),...,(p,q-1),(p,q)$, och var och en av dem är lika sannolik. Med andra ord låter detta oss simulera en $pq-$tärning.

(b) Ett kast är aldrig tillräckligt, eftersom varje tärning har färre än n sidor och vi kan därför bara få högst $n-1$ olika utfall efter ett kast, varav varje har en sannolikhet $\geq \frac{1}{n-1} > \frac{1}{n}$ att inträffa. Om vi således för något utfall av det första kastet bestämmer oss för att sluta kasta och tilldela ett slutresultat mellan 1 och n, kommer sannolikheten för detta värde vara större än $\frac{1}{n}$, vilket är för mycket.
Å andra sidan behöver vi aldrig mer än 3 kast i väntevärde. Låt oss börja med att kasta en tärning med $p \geq \frac{n}{2}$ sidor två gånger (observera att det alltid finns ett primtal mellan $\frac{n}{2}$ och n enligt Bertrands postulat). Det finns p^2 möjliga utfall av dessa två kast. Vi kan dela in dem i n grupper med $\lfloor \frac{p^2}{n} \rfloor$ utfall i varje grupp, och tilldela ett olika slutresultat till var och en av dessa grupper. Därefter, efter dessa två kast, med sannolikhet $n \cdot \lfloor \frac{p^2}{n} \rfloor$ har vi redan fått vårt slutresultat mellan 1 och n, och var och en av dem är lika sannolikt, och med sannolikhet $1 - n \cdot \lfloor \frac{p^2}{n} \rfloor < \frac{n}{p^2}$ har vi ännu inte fått ett resultat. Om vi inte har fått ett resultat ännu, låt oss helt enkelt upprepa ovanstående process och kasta två $p-$tärningar igen. Vi vill beräkna det förväntade antalet kast som krävs tills vi får vårt resultat med denna algoritm.
Låt x vara det förväntade antalet kast med denna algoritm. Då har vi att

$$\begin{aligned} x &\leq 2 + \frac{n}{p^2}x \\ &\leq 2 + \frac{nx}{n^2/4} \\ &= 2 + \frac{4x}{n} \end{aligned}$$

eftersom vi alltid behöver 2 kast, och efter de första två kasten behöver vi x fler kast i förväntning med sannolikhet högst $\frac{n}{p^2} \leq \frac{n}{n^2/4}$. Genom omformulering får vi att

$$x \leq \frac{2}{1 - \frac{4}{n}} = \frac{2n}{n-4} = 2 + \frac{8}{n-4}$$

Om $n \geq 12$ får vi att $x \leq 3$, vilket skulle visas.

(c) Den här delen är ganska överraskande; hur skulle vi någonsin kunna komma undan med exakt 2 kast om inte $n = pq$? Den stora insikten är att den andra tärningen vi kastar får *bero på utfallet av den första tärningen.*

Antag att $a, b, c \in \mathbb{N}$ är heltal och p, q, r, Q är primtal sådana att

$$\begin{cases} pqr = n \\ Q < n \\ aqr + brp + cpq = Q \end{cases} \tag{2}$$

Eftersom $Q < n$, kan vi börja med att kasta en Q-sidig tärning och gruppera de möjliga utfallen i tre grupper: en grupp av storlek aqr (grupp p), en av storlek brp (grupp q) och en av storlek cpq (grupp r). Gruppen bestämmer sedan vilken tärning vi kastar näst - en tärning med p, q eller r sidor. Med denna procedur får vi totalt na utfall med sannolikheten $\frac{1}{pQ}$ att

inträffa, nb utfall med sannolikheten $\frac{1}{qQ}$ och nc utfall med sannolikheten $\frac{1}{rQ}$. Dessa utfall kan enkelt tilldelas siffrorna $1, \ldots, n$ på ett sådant sätt att alla siffror är lika sannolika. För att lösa problemet visar vi nu att det finns oändligt många $n = pqr$ för vilka (2) har en lösning:

Sätt $q = 3$ och $r = 2$ och $b = c = 1$. Det återstår då att hitta oändligt många a, p och Q som uppfyller

$$6a + 5p = Q \quad \text{och} \quad Q < 6p,$$

eller med andra ord hitta p och Q så att $5p < Q < 6p$ och $p \equiv Q \bmod 6$. Enligt Dirichlets sats om aritmetiska följder finns det oändligt många primtal som är kongruenta med både 1 och 2 modulo 3. Följaktligen finns det oändligt många par av på varandra följande primtal $p_1 < p_2$ sådana att $p_1 \equiv 1 \bmod 3$ och $p_2 \equiv 2 \bmod 3$. Sätt Q till det minsta primtalet större än $5p_2$. Som en konsekvens av primtalssatsen närmar sig förhållandet mellan stora på varandra följande primtal 1, vilket innebär att

$$\frac{Q}{p_1} = \frac{Q}{5p_2}\frac{5p_2}{p_1} \to 5. \qquad \text{när } \; p_1 \to \infty.$$

I synnerhet, för alla tillräckligt stora p_1 får vi $Q < 6p_1 < 6p_2$. Detta är precis vad vi ville ha. Om $Q \equiv 1 \bmod 3$ kan vi sätta $p = p_2$. Om inte, då är $Q \equiv 2 \bmod 3$ och vi kan sätta $p = p_1$. I båda fallen är $Q - 5p$ delbart med både 2 och 3, vilket innebär att vi kan sätta $a = (Q - 5p)/6$. Detta ger oändligt många möjliga värden på p och därmed oändligt många möjliga värden på n, som önskat.

□

Problem 9. Givet heltal $d < n$ och ett reellt tal ε så säger vi att en uppsättning med d ortonormala vektorer $v_1, ..., v_d \in \mathbb{R}^n$ är $\varepsilon-$*balanserade* om

$$\forall j \in \{1, 2, ..., n\} : \quad \left| \sum_{i=1}^{d} v_{ij}^2 - \frac{d}{n} \right| \leq \varepsilon$$

Låt $n = d + 1$, och antag att $v_1, ..., v_d \in \mathbb{R}^{d+1}$ är en uppsättning ortonormala, $\varepsilon-$balanserade vektorer. Visa att det existerar en uppsättning ortonormala vektorer $w_1, w_2, ..., w_d \in \mathbb{R}^{d+1}$ som är $0-$balanserade och uppfyller

$$\sum_{i,j} (v_{ij} - w_{ij})^2 < Cd\varepsilon$$

för någon konstant C som inte beror på d och ε.

Korrektion: $Cd^2\varepsilon^2$ istället för $Cd\varepsilon$ är en mer naturlig (och starkare) övre gräns, vilket var vad som åvsågs med uppgiften.

Lösningsförslag. Vektorerna $v_1, \ldots, v_d$ kan utökas till en ortonomal bas av $\mathbb{R}^{n+1}$ med en sista vektor x. Vi får att $[v_1, v_2, \ldots, v_d, x]$ är en ortogonal matris, därav

$$x_j^2 + \sum_{i=1}^{d} v_{ij}^2 = 1. \tag{3}$$

Att $v_1, \ldots, v_d$ är ϵ-balanserade är alltså ekvivalent med att

$$|x_j^2 - \frac{1}{d+1}| < \varepsilon$$

för alla $j = 1, \ldots, d+1$. I synnerhet så är $u_1, \ldots, u_d$ 0-balanserade om de bildar en ortogonal matris tillsammans med en vektorn

$$y = \begin{bmatrix} \frac{1}{\sqrt{d+1}} \\ \vdots \\ \frac{1}{\sqrt{d+1}} \end{bmatrix}.$$

Detta är inte ett nödvändigt villkor, ty komponenterna på y kan vara negativa. Om vi dock utan inskränkning antar att alla komponenter av x är positiva så kommer vi kunna se till att komponenterna av y också vara det.

Låt P beteckna planet som spänns upp av x och y. Eftersom både x och y har längden 1 och ligger i P så finns det en rotation R av planet P som för x till y. Sätt $w_1 \ldots, w_d$ att vara resultatet av samma rotation utförd på $v_1, \ldots, v_n$. På detta sätt blir $[w_1, \ldots, w_d, y]$ en rotation av ON-basen $[v_1, \ldots, v_d, x]$, vilket innebär att $[w_1, \ldots, w_d, y]$ också är en ON-bas precis som vi ville. Kvar är att visa att

$$D := \sum_{i,j} (v_{ij} - w_{ij})^2 < Cd^2\varepsilon^2$$

för något konstant C. Om vi skriver om summan får vi

$$D = \sum_{i=1}^{d} |v_i - w_i|^2$$

D beror alltså på hur långt $v_1, \ldots, v_d$ förflyttas under rotationen. För att beräkna detta avstånd, skriv $v = v_i' + v_i^\perp$ där v_i' är komponenten av v_i som är i P och $v_i^\perp$ är komonenten av v_i som är ortogonal mot P. Rotationen flyttar v_i lika långt som v_i', nämligen avståndet $|v_i'| \cdot 2\sin\frac{\theta}{2}$, där θ är rotationsvinkeln av R. Ytterligare kan $|v_i'|$ skrivas om som $|v_i \cdot z|$ där z är en enhetsvektor i planet P vinkelrät mot x. Insättning av detta ger

$$D = \sum_{i=1}^{d} (v_i \cdot z)^2 (2\sin\frac{\theta}{2})^2 \tag{4}$$

Men $v_1, \ldots, v_d$ är ju en ON-bas av det ortogonala komplementet till x. Således är

$$\sum_{i=1}^{d} (v_i \cdot z)^2 = |z|^2$$

och (4) simplifieras till

$$D = (2\sin\frac{\theta}{2})^2.$$

Detta uttryck ger precis kvadraten av avståndet som x förflyttas av R. Med andra ord,

$$D = |x - Rx|^2 = |x - y|^2 = \sum_{i=1}^{d+1}(x_i - \frac{1}{\sqrt{d+1}})^2$$

Nu har vi något som liknar (3). Konjugatregeln ger

$$D = \sum_{i=1}^{d+1}\left(\frac{x_i^2 - \frac{1}{d+1}}{x_i + \frac{1}{\sqrt{d+1}}}\right)^2$$

varefter vi kan använda vårt antagande om att $x_1 \ldots, x_{d+1} \geq 0$ och få

$$D \leq \sum_{i=1}^{d+1}(d+1)\left|x_i^2 - \frac{1}{d+1}\right|^2$$

varefter (3) slutligen ger

$$D \leq (d+1)^2\varepsilon^2 \leq 4d^2\varepsilon^2,$$

vilket skulle visas. □

Problem 10. Ivar och Ravi bor i ett stort spökhus som består av n stycken rum. Varje rum har ett antal dörrar som leder till andra rum. Totalt finns det $n-1$ dörrar, och det är möjligt att gå från vilket rum som helst till vilket annat rum som helst genom en serie dörrar.
En dag bestämmer sig husets spöken för att göra alla dörrar enkelriktade! Varje dörr färgas röd på ena sidan och indigo på andra sidan, och för att se till att Ivar och Ravi inte kan hålla ihop ser spökena till att Ivar bara kan gå genom indigo-färgade dörrar medan Ravi bara kan gå genom röda dörrar.
Eftersom spökena inte vill vara allt för elaka, så gav dem Ivar och Ravi möjligheten att vända på dörrar så att färgerna byter plats, men bara enligt vissa regler. Man får bara vända på en dörr om man är i ett rum som man inte kan lämna för att alla dörrar har fel färg, och man måste i så fall vända på *alla* dörrar i det rummet på en gång! Visa att, oavsett hur spökena färgade dörrarna och oavsett vilka rum Ivar och Ravi är i från början, så kan Ivar och Ravi gå runt i huset och vända på dörrarna så att vilken färg-konfiguration som helst uppnås.

Lösningsförslag. Vi gör induktion på antalet rum. I basfallet finns ett rum och inga dörrar, och då är resultatet uppenbart. Anta nu att påståendet är sant när spökhuset innehåller k rum. Vi ska visa att det så också måste vara sant när spökhuset innehåller $k+1$ rum. Betrakta därmed ett spökhus G med $k+1$ rum. Om alla rum hade två eller fler dörrar så hade det funnits åtminstone $k+1$ dörrar totalt. Men det finns bara k dörrar. Alltså måste det finnas åtminstone ett rum som har exakt en dörr. Välj ett godtyckligt sådant rum och kalla det för a.

Lemma 2. *Om Ivar och Ravi är utanför a så kan de vända på alla dörrar utom dörren till a hur de vill, och de kan göra detta så att dörren till a är vänd likadant när de är klara som när de började.*

bevis. Ifall a och dörren till a inte fanns så hade huset haft k rum och $k-1$ dörrar. Enligt induktionshypotesen finns det alltså en sekvens drag som låter Ivar och Ravi vända på alla dörrar åt rätt håll. Om Ivar och Ravi utför dessa drag i huset med $k+1$ dörrar kan dock någon råka vända på dörren till a. Dessutom, om någon vill vända på alla dörrarna från b så kan dörren till a förhindra dem från att göra detta. Dessa problem kan dock lösas med följande justeringar av strategin:

1. Varje gång någon skulle ha vänt dörrarna i b men stoppas på grund av dörren till a, låt dem istället gå in i a, fastna, vända på dörren, och gå tillbaka till b. Därefter kommer personen kunna vända på dörrarna till i b. Dörren till a vänds på detta sätt två gånger så den är vänd likadant efter processen.

2. Varje gång någon vänder på dörrarna i b, men på så sätt råkar vända på dörren till a, låt de därefter gå in i a, fastna, vända på dörren och gå tillbaka till b. Återgien vänds dörren två gånger, vilket innebär att den är vänd åt samma håll som den var ursprungligen.

Detta bevisar lemmat. □

Nu kan vi beskriva Ivar och Ravis stragegi: Om Ivar eller Ravi är innuti a så går de ut (vilket kan innebära att de behöver vända på dörren dit). När varken Ivar eller Ravi är i a så kollar de om dörren till a är vänd rätt håll. Om den är det använder de Lemma 2 för att bli klara. Om den inte är de så måste antingen Ivar eller Ravi ta sig dit och vända på dörren. Vi kan anta utan inskränkning på problemet att dörren in i a är röd och att det därför är Ravi som måste gå in i rum a och vända på dörren. För att ta sig till rummet kan de använda Lemma 2 och vända på alla dörrar så att Ravi kan ta sig till a från vilket rum som helst (Detta är alltid möjligt eftersom det huset är en sammanhängande trädgraf. "Häng upp" grafen i a och måla varje dörr så att den röda sidan hamnar nedåt.). Ravi kan sedan gå till a, vända på dörren och gå ut. Slutligen använder de Lemma 2 igen för att vända resten av dörrarna hur de vill. Då är de klara, och enligt induktionsprincipen lyckas de oavsett storleken på spökhuset. □

Problem 11. Låt k vara ett positivt heltal. Låt S vara en oändlig mängd punkter i planet sådan att alla slutna cirklar med radie 1 innehåller högst k punkter i S. Visa att det finns en positiv konstant C oberoende av k och S sådan att:

(a) Det finns en cirkel med radie $r = 1 + \dfrac{C}{2^k}$ som innehåller högst k punkter i S.

(b) Det finns en cirkel med radie $r = 1 + \dfrac{C}{k}$ som innehåller högst k punkter i S.

Observera: Om du kan visa (b) behöver du inte ett separat bevis för (a). Om du har något resultat som är starkare än (a) men svagare än (b), kan vi ge poäng för det.

Lösningsförslag. (b) Vi använder probabilistiska metoden. Introducera ett koordinatsystem. Låt A vara slumpmässigt vald punkt bland punkterna $\Omega_A = \{a \in S : |a| < M\}$ där M är något stort tal. Låt slumpvariabeln X vara uniformt fördelad i cirkelskivan $\Omega_X = \{x \in \mathbb{R}^2 : |x| < M + 1\}$. A är alltså diskret medan X är kontinuerlig. Varje cirkel med medelpunkt $a \in \Omega_A$ och radie 1 är helt innuti Ω_X. För varje $a \in \Omega_A$ gäller därmed

$$P(|X - a| \le 1) = \frac{\text{Area}\{x \in \Omega_X : |x - a| \le 1)\}}{\text{Area}(\Omega_X)} = \frac{\pi}{\pi(M+1)^2} = \frac{1}{(M+1)^2}.$$

Å andra sidan, för varje $x \in \Omega_X$ gäller

$$P(|x - A| \le 1) = \frac{\#\{a \in \Omega_A : |x - a| \le 1\}}{\#\Omega_A} \le \frac{k}{\#\Omega_A}.$$

Vi har på så vis visat att

$$\frac{1}{(M+1)^2} = P(|X - A| \le 1) \le \frac{k}{\#\Omega_A} \tag{5}$$

Anta nu att r är sådant att alla cirklar med radie r innehåller åtminstone $k + 1$ punkter från S. Låt sedan slumpvariabeln Y vara uniformt fördelad i cirkelskivan $\{y \in \mathbb{R}^2 : |y| \le M - r\}$. För varje $a \in \Omega_A$ får vi då olikheten

$$P(|Y - a| \le r) = \frac{\text{Area}\{y \in \Omega_Y : |y - a| \le r)\}}{\text{Area}(\Omega_Y)} \le \frac{\pi r^2}{\pi(M-r)^2} = \frac{r^2}{(M-r)^2}.$$

Varje cirkel med mittpunkt $y \in \Omega_Y$ och radie r ligger helt innuti Ω_A. Således gäller

$$P(|y - A| \le r) = \frac{\#\{a \in \Omega_A : |y - a| \le r\}}{\#\Omega_A} \ge \frac{k+1}{\#\Omega_A},$$

därav

$$\frac{r^2}{(M-r)^2} \ge P(|Y - A| \le r) \ge \frac{k+1}{\#\Omega_A}. \tag{6}$$

Division av (6) med (5) ger slutligen

$$r^2 \frac{(M+1)^2}{(M-r)^2} \ge \frac{k+1}{k}$$

vilket när $M \to \infty$ blir

$$r^2 \ge 1 + \frac{1}{k} \quad \Longrightarrow \quad r \ge \sqrt{1 + \frac{1}{k}} > \sqrt{1 + \frac{2}{3k} + \frac{1}{9k^2}} = 1 + \frac{1}{3k}.$$

För alla $r \le 1 + \frac{1}{3k}$ finns alltså en cirkel med radie r som innehåller som högst k punkter. □