

## Ekstra ugeopgaver

- [GRP2: 16] \*Lad  $k = k(\sigma)$  være tallet defineret i GRP(2.18.1), altså som summen  $k = \sum (p-1)m_p(\sigma) = n - m(\sigma)$ . Som nævnt kan  $\sigma$  skrives som produkt af  $k$  transpositioner. Vis, at  $\sigma$  ikke kan skrives som produkt af færre end  $k$  transpositioner.
- [TAL3: 17] Lad  $a, n$  være to naturlige tal, og lad  $d$  være den største fælles divisor for  $a, n$ . Der findes da fremstillinger  $d = xa - yn$  med hele tal  $x, y$ . Vis, at der er et entydigt valg af  $x, y$  således, at  $1 \leq x \leq n/d$ , og at der med dette valg gælder  $0 \leq y < a/d$ .
- Bestem cykelfremstillingen af  $(1\ 2\ 3 \dots n) \dots (1\ 2\ 3\ 4)(1\ 2\ 3)(1\ 2)$ .
- \*Bestem cykelfremstillingen af  $(1\ 2)(1\ 2\ 3)(1\ 2\ 3\ 4) \dots (1\ 2\ 3 \dots n)$ .
- For primtallene 5, 13 og 17 har vi  $5 = 2^2 + 1^2$ ,  $13 = 3^2 + 2^2$ , og  $17 = 4^2 + 1^2$ . Derimod kan 7, 11 og 19 ikke skrives som en sum af to kvadrater. Prøv med nogle flere primtal, og formuler en sætning. \*Bevis sætningen.
- For hvilke  $n = 2, 3, \dots, 25$  er gruppen af primiske restklasser  $(\mathbb{Z}/n)^*$  cyklisk? Prøv eventuelt med nogle flere værdier af  $n$ , og formuler en sætning. \*Bevis sætningen.
- Lad  $N$  være en normal undergruppe af gruppen  $G$ . To sideklasser,  $A_1 = g_1N$  og  $A_2 = g_2N$ , er specielt delmængder af  $G$ . Produktet  $A_1A_2$  har derfor to definitioner, i GRP(4.1) og i GRP(4.15). Giver de to definitioner samme resultat?
- Findes der 1.000.000 på hinanden følgende ikke-kvadratfrie naturlige tal?
- Bestem antallet af løsninger modulo  $n$  til kongruensen  $x^2 \equiv 1$ .
- [GRP1: 21] \*Vis, at en ikke-tom mængde  $G$  med en associativ komposition '\*' er en gruppe, hvis og kun hvis der for alle  $a, b \in G$  gælder, at ligningerne  $a * x = b$  og  $y * a = b$  har løsninger  $x, y \in G$ .
- [TAL3: 16] Vis, for  $n \geq 3$ , at der er uendelig mange primtal  $p$  med  $p \not\equiv 1 \pmod{n}$ .
- [GRP4: 23] \*Dirichlet's sætning udsiger, at når  $(a, n) = 1$ , så findes der uendelig mange primtal  $p$  med  $p \equiv a \pmod{n}$ . Vis, at der findes uendelig mange primtal  $p$  med  $p \equiv 1 \pmod{4}$ . [Vink: kig på en primdivisor  $p$  i  $(2p_1 \dots p_k)^2 + 1$ , og anvend GRP(4.17) på  $G := (\mathbb{Z}/p)^*$  og et passende  $g$ .]
- Er det muligt at dele en terning i 1992 terninger (naturligvis ikke alle af samme størrelse)? [Kilde: Lettisk konkurrence — for 9. klasse! Jeg syntes, den var svær!]
- [GRP7: 22] For en undergruppe  $H$  af en endelig gruppe  $G$  virker  $G$  ved translation på mængden  $X = G/H$  af sideklasser. Bestem isotropigruppen for en given sideklasse  $xH$ . Bestem kernen for den tilhørende repræsentation  $G \rightarrow \text{Perm}(G/H)$ .
- [GRP7: 23] Antag, at  $p$  er den mindste primdivisor i ordenen af  $G$ , og at  $H$  er en undergruppe af index  $p$ . Vis, at  $H$  er normal.
- [RNG1: 20] Kvaternion-enhederne  $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$  tilhører ringen  $\text{Mat}_2(\mathbb{C})$ . Vis, at matricerne af formen  $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ , for reelle tal  $(a, b, c, d)$ , udgør en delring  $\mathbb{H}$  af  $\text{Mat}_2(\mathbb{C})$ . Vis, at  $\mathbb{H}$  er et skævlegeme.

17. Vis det omvendte af Wilson's sætning, for  $n \geq 2$ : Hvis  $(n-1)! \equiv -1 \pmod{n}$ , så er  $n$  et primtal. Hvad med det omvendte af Fermat's sætning?
18. [RNG6: 19] Lad  $\xi$  være et (irrationalt) kvadratisk tal med diskriminant  $D$ . Vis, for et ulige primtal  $p$ , at  $p$  er et primelement i  $\mathbb{Z}[\xi]$ , hvis og kun hvis  $D$  modulo  $p$  ikke er et kvadrat.
19. Når  $n$  er primopløst,  $n = p_1^{v_1} \cdots p_r^{v_r}$ , er det let at bestemme antallet af (positive) divisorer i  $n$ : det er produktet  $(v_1 + 1) \cdots (v_r + 1)$ . Kan du finde en formel for summen  $\sigma(n)$  af divisorerne i  $n$ ?
20. Et tal  $n$  kaldes *fuldkomment*, hvis  $n$  er lig med summen af sine divisorer, fraregnet  $n$  selv, altså hvis  $\sigma(n) = 2n$ . Eksempler:  $6 = 1 + 2 + 3$  og  $28 = 1 + 2 + 4 + 7 + 14$ . Vis (Euklid), at hvis  $2^k - 1$  er et primtal, så er  $n = 2^{k-1}(2^k - 1)$  fuldkomment. Vis omvendt (Euler), at ethvert lige fuldkomment tal er af denne form. (Man ved ikke om der findes ulige fuldkomne tal.)
21. Bestem modulo 101 en liste med mindst 20 primiske restklasser og deres inverse – på højst 2 minutter. [Vink: prøv at faktorisere 100 og 102.]
22. For antallet  $p(n)$  af cykeltyper i  $S_n$  (altså partitioner af  $n$ ) gælder trivielt, at  $p(n) = \sum p_h(n)$ , hvor  $p_h(n)$  er antallet af cykeltyper med  $h$  som den mindste længde af en cykel. Øjensynlig er  $p_n(n) = 1$  og  $p_h(n) = 0$  for  $n/2 < h < n$ . Vis for  $h < n$ , at  $p_h(n) = \sum_{h \leq k \leq n-h} p_k(n-h)$  og overvej, at dette kan bruges til en rekursiv bestemmelse af  $p(n)$ .
23. For en permutation  $\sigma = (\sigma_1, \dots, \sigma_n)$  (i den direkte notation) bestemmes antallet af inversioner  $\ell(\sigma)$  sådan: man gennemløber pladserne, for  $i = 1, \dots, n$ , og tæller for hver plads  $i$  hvor mange gange, der på en senere plads står et tal, der er mindre end det  $i$ 'te:  $\sigma_j < \sigma_i$ . Antag, at  $\sigma_k > \sigma_{k+1}$ , og lad  $\sigma'$  være permutationen, der (i den direkte notation) fås fra  $\sigma$  ved at ombytte tallene  $\sigma_k$  og  $\sigma_{k+1}$ . Vis, at  $\ell(\sigma') = \ell(\sigma) - 1$ . Slut heraf, at  $\sigma$  kan skrives som produkt af  $\ell(\sigma)$  nabotranspositioner, og specielt, at  $\text{sign}(\sigma) = (-1)^{\ell(\sigma)}$ .
24. [RNG2: 11] Lad  $R$  være en kommutativ ring, og lad  $\mathfrak{a}$  være et ægte ideal. Antag, at  $R \setminus \mathfrak{a} \subseteq R^*$  (altså at hvert  $r \in R$  med  $r \notin \mathfrak{a}$  er invertibelt i  $R$ ). Vis, at  $R/\mathfrak{a}$  er et legeme og at  $\mathfrak{a}$  er et maksimalideal. Vis, at  $\mathfrak{a}$  er det eneste maksimalideal i  $R$ .
25. [RNG6: 18] Lad  $p$  være et ulige primtal. Vis for hele tal  $b, c$  og  $D := b^2 - 4c$ , at kongruensen  $z^2 - bz + c \equiv 0 \pmod{p}$  har løsninger, hvis og kun hvis kongruensen  $x^2 \equiv D \pmod{p}$  har løsninger.
26. [RNG6: 20] Afgør om den diofantiske ligning  $x^2 + xy - y^2 = 17$  har løsninger.
27. [RNG6: 21] Lad  $R = \mathbb{Z}[\xi]$  være en kvadratisk talring med diskriminant  $D$ . Vis, at  $R$  er euklidisk for  $D = -3, -4, -7, -8, -11$ . Vis, at  $R$  er euklidisk for  $D = 5, 13$ . Vis, at  $R$  er euklidisk for  $D = 17$ .
28. [GRP4: 24] \*Bestem kommutatorundergrupperne  $S'_n$  og  $A'_n$ . [Vink: For  $n \geq 5$  er enhver 3-cykel en kommutator af to 3-cykler. Undersøg også hvad der sker for  $n \leq 4$ .]
29. [TAL2: 15] En følge af naturlige tal  $a_1, a_2, a_3, \dots$  defineres ved forskriften

$$a_n := \lfloor 10^{n-1} \pi / 2 \rfloor \bmod 10^{100} + 1,$$

hvor  $[\alpha]$  er den hele del af det reelle tal  $\alpha$  og  $x \bmod d$  betegner den principale rest af  $x$  ved division med  $d$ . Vis, at  $S := \{a_n \mid n \in \mathbb{N}\}$  er en begrænset delmængde af  $\mathbb{N}$ . Lad  $m$  være det mindste tal i  $S$ . Vis, at  $1 \leq m \leq 2$ . Kan du afgøre hvilken af de to muligheder, der indtræffer?

**30.** \*Et berømt resultat af Lagrange udsiger, at ethvert naturligt tal er en sum af fire ikke-negative kvadrater; her må nogle af kvadraterne altså være 0. Angiv eksplicit en funktion  $f: \{5, 6, 7, \dots\} \rightarrow \mathbb{N}$  således, at der for ethvert  $k \geq 5$  gælder: Hvis  $n \geq f(k)$ , så er  $n$  en sum af  $k$  positive kvadrater.

**31.** [GRP1: 22] \*Antag, at  $G$  er en mængde med en associativ komposition '\*', som har et venstre neutralt element  $e$ , dvs  $e * x = x$  for alle  $x \in G$ . Vis, at hvis hvert element  $x$  har et venstre invers  $x'$ , dvs  $x' * x = e$ , så er  $G$  en gruppe.

Vis, at hvis hvert element  $x$  har et højre invers  $x'$ , dvs  $x * x' = e$ , så er  $G$  ikke nødvendigvis en gruppe.

Vis, at hvis man ud over eksistensen af højre inverse elementer yderligere antager: af  $a * x = b * x$  for alle  $x$  følger  $a = b$ , så er  $G$  en gruppe.

**32.** Lad  $p(n)$  være antallet af cykeltyper i  $S_n$ , altså antallet af partitioner af  $n$ , og lad  $p_h(n)$  være antallet af typer, hvor længden af den største cykel er  $h$ . Øjensynlig er  $p(n) = \sum_{h=1}^n p_h(n)$ . Vis rekursionsformlen:  $p_n(n) = 1$  og for  $h < n$  er  $p_h(n) = \sum_{k=1}^h p_k(n-h)$ .

**33.** Lad der være givet en bijektiv afbildning  $\mu: X \rightarrow Y$ . Gør rede for, at hvis  $\sigma$  er en permutation af  $X$ , så er  ${}^\mu\sigma := \mu\sigma\mu^{-1}$  en permutation af  $Y$ . Vis, at hvis  $\sigma$  er produkt af disjunkte cykler  $(x_1 \dots x_p)$ , så er  ${}^\mu\sigma$  produkt af de tilsvarende disjunkte cykler  $(\mu(x_1) \dots \mu(x_p))$ .

**34.** [TAL2: 16] Vis, at  $1^4 + 2^4 + \dots + n^4 = n(6n^4 + 15n^3 + 10n^2 - 1)/30$ .

**35.** [TAL6: 12] Lad  $n$  være et naturligt tal, fremstillet med  $k$  cifre i 10-talssystemet. Antag, at  $n'$  er fremkommet af  $n$  ved ombytning af de  $k$  cifre. Vis, at tallet  $n - n'$  er deleligt med 9.

**36.** [TAL3: 18] Et naturligt tal  $p > 1$  har følgende egenskab:  $p \mid ab \implies p \mid a$  eller  $p \mid b$ . Vis, at  $p$  er et primtal.

**37.** [TAL2: 17] Vis, at alle naturlige tal  $n$  er karakteriseret ved en interessant egenskab. [Vink: brug Velordningsprincippet.]

**38.** Lad  $n$  være et naturligt tal primisk med 10. Vis, at der findes et multiplum af  $n$ , som i 10-talssystemet skrives med lutter 1-taller.

**39.** [TAL3: 19] Antag for naturlige tal  $a, b, c, d$ , at  $ab = cd$ . Vis, at  $a \mid c \iff d \mid b$ .

**40.** [TAL3: 20] Antag, at  $n \mid ab$  ( $n \geq 1$ ), og sæt  $d := (a, n)$ . Vis, at  $\frac{n}{d} \mid b$  ved at bruge en fremstilling  $d = xa + yn$ . [Vink: Indsæt fremstillingen i  $bd$ .]

**41.** Antag, at  $X$  er en ordnet mængde med  $n$  elementer. Vis, at enhver permutation  $\sigma$  af  $X$  har en entydig fremstilling som et produkt af følgende form (med  $r \geq 0$  transpositioner):

$$(*) \quad \sigma = (i_1 j_1) \cdots (i_r j_r), \text{ hvor } i_s < j_s \text{ for } s = 1, \dots, r \text{ og } j_1 < \dots < j_r.$$

[Vink: For  $\sigma = \text{id}$  anvendes den tomme fremstilling ( $r = 0$ ). For  $\sigma \neq \text{id}$  kan man lade  $j(\sigma)$  betegne det største element, der flyttes af  $\sigma$ . Begrund, at i en fremstilling (\*) må der gælde

$j(\sigma) = j_r$  og  $\sigma(i_r) = j_r$ , og benyt dette til at vise påstanden ved fuldstændig induktion efter  $j(\sigma)$ .]

Vis, at  $n - r$  er antallet af baner for  $\sigma$ . [Vink: Denne påstand kan medtages i induktionsbeviset for den første påstand.]

**42.** For  $n \geq 0$  kan *Stirling-tallene af første art*,  $\left[ \begin{smallmatrix} n \\ r \end{smallmatrix} \right]$  for  $r = 0, \dots, n$ , defineres ved ligningen mellem polynomier:

$$x(x+1) \cdots (x+n-1) = \sum_r \left[ \begin{smallmatrix} n \\ r \end{smallmatrix} \right] x^r.$$

Vis, ved at multiplicere parenteserne i produktet, at

$$\left[ \begin{smallmatrix} n \\ n-r \end{smallmatrix} \right] = \sum_{1 \leq j_1 < j_2 < \dots < j_r \leq n-1} j_1 j_2 \cdots j_r.$$

Udled heraf, at

$$\left[ \begin{smallmatrix} n \\ r \end{smallmatrix} \right] = \text{antallet af permutationer i } S_n \text{ med } r \text{ baner.}$$

**43.** Lad  $U_1, \dots, U_k$  være delmængder af en endelig mængde  $U$ . Sæt

$$N_r := \sum_{\{i_1, \dots, i_r\}} |U_{i_1} \cap \dots \cap U_{i_r}|;$$

summen er over alle delmængder med  $r$  elementer af indices. Leddet svarende til  $i_1, \dots, i_r$  er antallet af elementer  $u \in U$ , som ligger i alle de  $r$  delmængder  $U_{i_1}, \dots, U_{i_r}$  (og måske i flere af delmængderne  $U_i$ ). Lad  $E_t$  betegne antallet af elementer  $u \in U$ , som opfylder  $u \in U_i$  for præcis  $t$  værdier af  $i$ . Specielt er så

$$N_0 = |U|, \quad E_0 = |U \setminus (U_1 \cup \dots \cup U_k)|, \quad \text{og } N_k = E_k = |U_1 \cap \dots \cap U_k|.$$

Vis, for  $r = 0, \dots, k$ , at

$$N_r = \sum_{r \leq t \leq k} \binom{t}{r} E_t; \quad \text{specielt } N_0 = E_0 + \dots + E_k.$$

Vis, at disse ligninger kan udtrykkes som en enkelt ligning mellem polynomierne  $N(x) := \sum N_r x^r$  og  $E(x) := \sum_r E_r x^r$ , nemlig  $N(x) = E(x+1)$ . Slut heraf, at  $E(x) = N(x-1)$ , og dermed, at

$$E_r = \sum_{r \leq t \leq k} (-1)^{t-r} \binom{t}{r} N_t.$$

Ligningerne udtrykker princippet om *tælling ved inklusion-eksklusion*. Specielt er

$$E_0 = N_0 - N_1 + \dots + (-1)^k N_k \quad \text{og} \quad N_0 - E_0 = N_1 - N_2 + \dots + (-1)^{k-1} N_k.$$

**44.** En farvelægning af  $\{1, \dots, n\}$ , med farver fra en ordnet mængde  $F$  med  $k$  farver, er et  $n$ -sæt  $(f_1, \dots, f_n)$  med  $f_i \in F$ . Lad  $U$  være mængden af farvelægninger og lad  $U_i$  være delmængden af farvelægninger, som *ikke* bruger den  $i$ 'te farve. Vis, med standardbetegnelser for inklusion-eksklusion, at for  $0 \leq r \leq k$  er

$$N_{k-r} = \binom{k}{r} r^n, \quad E_{k-r} = \left\{ \begin{matrix} n \\ r \end{matrix} \right\} k^r.$$

hvor  $\left\{ \begin{matrix} n \\ r \end{matrix} \right\}$  er antallet af klassedeling af en mængde med  $n$  elementer i  $r$  klasser (*Stirling-tallene af anden art*), og  $k^{\underline{r}} := k(k-1) \cdots (k-r+1)$ . Udled formlerne:

$$k^n = \sum \left\{ \begin{matrix} n \\ r \end{matrix} \right\} k^r, \quad \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \frac{1}{k!} \sum (-1)^r \binom{k}{r} (k-r)^n,$$

Hvilken ligning mellem polynomier udledes af den første formel?

**45.** Den symmetriske gruppe  $S_n$  virker på farvelægninger  $(f_1, \dots, f_n)$  med farver fra en mængde med  $k$  farver ved at permutere koordinaterne. Banerne svarer til  $k$ -sæt af antal,  $(a_1, \dots, a_k)$ , hvor  $a_j$  er antallet af koordinater af den  $j$ 'te farve. Vis, at Polya's tælleformel er følgende formel:

$$\binom{n+k-1}{n} = \frac{1}{n!} \sum_r \left[ \begin{matrix} n \\ r \end{matrix} \right] k^r.$$

Hvilken ligning mellem polynomier udledes af formelen?

[Vink: begge formlens sider kræver en overvejelse. Venstresiden er antallet af heltalsløsninger til  $a_1 + \dots + a_k = n$  med  $a_j \geq 0$ , og på højresiden er koefficienten til  $k^r$  lig med antallet af permutationer i  $S_n$  med  $r$  baner.]

**46.** I en *partition*  $n = \lambda_1 + \dots + \lambda_k$ , hvor  $\lambda_i \in \mathbb{N}$ , skelner man ikke rækkefølgen af leddene, og partitionen kan enten angives ved følgen af addender *altid ordnet aftagende*,  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k > 0$ , eller ved *typen*  $1^{m_1} 2^{m_2} 3^{m_3} \dots$ , hvor  $m_1$  er antallet af 1-taller blandt  $\lambda_i$ 'erne,  $m_2$  er antallet af 2-taller osv. Fx kan partitionen  $18 = 1 + 1 + 3 + 3 + 3 + 3 + 4$  angives som  $(4, 3, 3, 3, 3, 1, 1)$  eller som  $1^2 3^4 4^1$  (det er et „formelt“ produkt, som *ikke* skal regnes ud).

For en klassedeling af en mængde  $X$  med  $n$  elementer i  $k$  klasser udgør klassernes elementantal en partition  $(\lambda_1, \dots, \lambda_k)$ , som kaldes klassedelings type. Bemærk, at antallet af klassedeling af en given type  $(\lambda_1, \dots, \lambda_k)$  *ikke* er givet ved multinomialkoefficienten,

$$\binom{n}{\lambda_1, \dots, \lambda_k} = \frac{n!}{\lambda_1! \cdots \lambda_k!}.$$

Multinomialkoefficienten ovenfor angiver nemlig antallet af opdelinger af  $X$  i *nummerede* delmængder  $X_1, \dots, X_k$  med  $|X_i| = \lambda_i$ ; hvis vi, som her, antager at  $\lambda_i \geq 1$  for alle  $i$ , så fås de nummerede opdelinger blot ved at nummerere klasserne i en klassedeling (under kravet  $|X_i| = \lambda_i$ ). Slut heraf, at det søgte antal klassedeling af en given type  $(\lambda_1, \dots, \lambda_k)$

er bestemt at dividere multinomialkoefficienten med  $m_1!m_2!\cdots$ . Vis herved: Antallet af klassedeling af den givne type er bestemt som tallet

$$\frac{n!}{m_1!m_2!\cdots\lambda_1!\cdots\lambda_k!} = \frac{n!}{m_1!m_2!\cdots(1!)^{m_1}(2!)^{m_2}\cdots},$$

og antallet af permutationer i  $S_n$  af denne type er bestemt som tallet

$$\frac{n!}{m_1!m_2!\cdots\lambda_1\cdots\lambda_k} = \frac{n!}{m_1!m_2!\cdots 1^{m_1}2^{m_2}\cdots}.$$

**47.** I en klassedeling af  $X = \{1, \dots, n\}$  med  $k$  klasser kan man nummerere klasserne  $X_i$  sådan, at når  $h_m$  er det mindste tal i  $X_m$ , så er  $h_1 < h_2 < \cdots < h_k$ . Øjensynlig er så  $h_1 = 1$ , og  $h_k \leq n$ . Følgen  $h_1, \dots, h_k$  kan alternativt bestemmes ud fra følgen  $m_1, \dots, m_k$ , hvor  $m_\nu$  er antallet af tal  $h$  som opfylder  $h_\nu < h < h_{\nu+1}$  (hvor  $h_{k+1} := n + 1$ ). Overvej nu:

de  $m_1$  tal  $h$  med  $h_1 < h < h_2$  ligger alle i  $X_1$ ;

de  $m_2$  tal  $h$  med  $h_2 < h < h_3$  ligger i  $X_1$  eller i  $X_2$ ;

de  $m_3$  tal  $h$  med  $h_3 < h < h_4$  ligger i  $X_1$  eller i  $X_2$  eller i  $X_3$ ; osv.

Slut heraf, at for en given følge  $m_1, \dots, m_k$  er der  $1^{m_1}2^{m_2}\cdots k^{m_k}$  muligheder for klassedelingen. Vis herved, at

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \sum_{m_1+\cdots+m_k=n-k} 1^{m_1}2^{m_2}\cdots k^{m_k} = \sum_{1 \leq j_1 \leq j_2 \leq \cdots \leq j_{n-k} \leq k} j_1 j_2 \cdots j_{n-k}.$$