Permutace

Jakub Löwit

Abstrakt. Jak v olympiádní, tak ve vysokoškolské matetamice se nám často stane, že mám někdo něco zamíchá nebo přeuspořádá. Všechny takové příklady ale spojuje jeden algebraicko-kombinatorický princip - permutace. V přednášce si ukážeme jejich základní vlastnosti, které posléze použijeme k řešení mnoha různorodých příkladů. Na závěr si blíže ukážeme sílu permutací v teorii čísel.

Permutace!

Permutace je jedním ze základních algebraických a kombinatorických objektů. Jde zkrátka o přečíslování či zamíchání nějaké množiny objektů. Přesto nás ale často může překvapit. Je dobré mít na paměti, že permutace jsou snad ty nejsymetričtější objekty, co si můžeme představit.

Definice 1. (Permutace) *Permutace* σ na množině X je zobrazení, které každému prvku X přiřadí nějaký (ne nutně jiný) prvek X. Přitom obrazy různých prvků musí být různé a každý prvek má nějaký vzor.

Definice 2.

(1) Skutečnost, že σ je permutace na množině X, často značíme $\sigma \in S_X$.
(2) Permutaci, která zobrazuje všechny prvky z X na sebe samotné nazýváme *identita*.
(3) Ke každé permutaci σ existuje právě jedna *inverzní* permutace σ^{-1}, která přiřazuje obrazům jejich vzory.
(4) Složením permutací σ, π myslíme zobrazení, které vznikne provedením postupně zobrazení σ a následně π. Toto zobrazení je opět permutace a značíme jej $\pi \circ \sigma$.
(5) Řádem permutace σ myslíme nejmenší $n \in \mathbb{N}_0$ takové, že pokud složíme σ samu se sebou k-krát, dostaneme identickou permutaci.

Lemma 3. *Existuje přesně* $n! = n \cdot (n-1) \dots 3 \cdot 2 \cdot 1$ *permutací* n*-prvkové množiny.*

Lemma 4. *Každé přirozené číslo lze jednoznačně zapsat jako* $a_1 \cdot 1! + a_2 \cdot 2! + a_3 \cdot 3! + \dots$, *kde* $0 \leq a_i \leq i$.

Definice. *Cyklus* je permutace, která cyklicky posouvá nějakých k prvků, přičemž ostatní nechává na místě.

Lemma 5. *Každou permutaci na konečné množině lze (až na pořadí) jednoznačně rozložit na součin disjunktních cyklů.*

Definice. *Transpozice* je permutace, která prohazuje pouze dva prvky (a všechny ostatní nechává na místě).

Lemma 6. *Každou permutaci na konečné množině lze získat jako složení několika transpozic.*

Lemma 7. *Každá permutace má nějaký řád (tedy existuje přirozené k takové, že složení této permutace k-krát je identická permutace).*

Na úvod...

Úloha 8. Kolika způsoby lze na šachovnici 8×8 rozmístit 8 věží tak, aby se žádné dvě neohrožovaly?

Úloha 9. Do tabulky $n \times n$ napíšeme čísla $1, 2, \ldots, n^2$ popořadě tak, že nejprve vyplníme zleva doprava první řádek, potom druhý atd. Nyní v tabulce vybereme n políček tak, abychom z každého řádku i každého sloupce vybrali právě jedno, a čísla na vybraných pozicích sečteme. Jaké výsledky můžeme dostat?

Nahlížíme

Jak už se nám doneslo, počet permutací n-prvkové množiny je $n!$. Když se proto někde faktoriál objeví, permutace určitě nejsou daleko a často se k řešení úlohy přímo vybízí vhodná kombinatorická interpretace.

Úloha 10. Pro přirozená k, n nahlédněte rovnost

$$\frac{(kn)!}{(k!)^n} = \binom{k}{k} \cdot \binom{2k}{k} \cdots \binom{nk}{k}.$$

Úloha 11. Je dáno přirozené k a $n \geq k$. Uvažme náhodnou permutaci na $1, 2, \ldots, n$. Nahlédněte, že pravděpodobnost, že prvky $1, \ldots, k$ leží v jednom cyklu, nezávisí na volbě n.

Úloha 12. Uvažme nějakou permutaci α množiny $1, 2, \ldots, n$. Postupně za sebe napišme všechny prvky $\alpha(1)$, $\alpha(2)$, ..., $\alpha(n)$. Jejich čtením zleva doprava získáme postupně $f(\alpha)$ rostoucích úseků. Jaká je průměrná hodnota $f(\alpha)$ přes všechny permutace zadané množiny?

Úloha 13. Permutacím σ na množině $1, 2, \ldots, 2n$, pro něž existuje $1 \leq i < 2n$ takové, že $|\sigma(i) - \sigma(i+1)| = n$, říkejme dobré. Ostatní nazývejme špatné. Nahlédněte, že dobrých permutací je víc, než špatných.

(IMO 1989)

Úloha 14. Je dáno $n \geq 2$ bodů očíslovaných $1, 2, \ldots, n$, přičemž mezi každými dvěma vede šipka směrem od nižšího čísla k vyššímu. Obarvení šipek červenou a modrou nazveme *jednobarevné*, jestliže mezi žádnými dvěma vrcholy nevede zároveň červená a modrá cesta. Uvědomte si, že počet *jednobarevných* obarvení je $n!$.

(ARO 2005)

Úloha 15. Označme $D(n)$ počet permutací na n prvcích, které nenechávají na místě ani jeden prvek. Nahlédněte, že

$$D(n) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)!.$$

Úloha 16. Jako *plné* n-tici přirozených čísel budeme označovat ty, ve kterých pro každé číslo $i \geq 2$, jež se v n-tici vyskytuje, platí, že číslo $i-1$ se v ní vyskytuje také, přičemž první výskyt $i-1$ je před posledním výskytem i. Nahlédněte, že *plných* n-tic je $n!$.

(IMO Shortlist 2002)

Úloha 17. Pro přirozená $n \geq 1$ dokažte identitu

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

.

Hrajeme si...

Nejčastěji je zkrátka potřeba si s úlohou chvíli hrát a pochopit, jak funguje. Občas nám sice nějaká znalost navíc může pomoct, cesta k řešení je ale většinou o dost zajímavější.

Úloha 18. Kolik existuje permutací π množiny $1, 2, \ldots, n$, které splňují

$$1 \cdot \pi(1) \leq 2 \cdot \pi(2) \leq \cdots \leq n \cdot \pi(n)?$$

Úloha 19. Na slavnostní večeři je n účastníků. Někteří z nich jsou přitom přátelé. Před každým účastníkem leží jedno jídlo, přičemž na stole nejsou žádná dvě jídla stejná. Každý z účastníků ale má chuť na něco jiného. Pokud se dva lidé přátelí, mohou si vyměnit svá jídla. Kolik dvojic účastníků musí být přátelé, aby každý mohl dostat své vysněné jídlo?

Úloha 20. Ve vězení sedí 100 vězňů. Ředitel věznice se rozhodl, že jim dá šanci na svobodu. Do 100 očíslovaných šuplíků ve své kanceláři proto náhodně umístil jména vězňů, do každého šuplíku právě jedno. Vězni budou jeden po druhém chodit do kanceláře. Každý z nich se může postupně podívat do 50-ti šuplíků. Pokud se všem vězňům povede nalézt svá jména, jsou propuštěni, jinak je ředitel nechá popravit.

Před začátkem hry se navíc mohou domluvit. Vymyslete pro vězně takovou strategii, aby jejich šance na propuštění byla alespoň $1 - (\frac{1}{51} + \frac{1}{52} + \cdots + \frac{1}{100}) > \frac{3}{10}$.

(folklor)

Úloha 21. Uvažme strom na n vrcholech označených čísly 1, 2, ..., n. Postupně zvolíme všechny hrany (každou právě jednou), přičemž vždy prohodíme čísla na koncích zvolené hrany. Tím dostaneme nějakou permutaci čísel ve vrcholech. Kolik cyklů může tato permutace obsahovat?

(Irán TST 2014)

Úloha 22. Na severní straně ulice je $n \geq 2$ domů. Ze západu k východu, domy nají čísla postupně od 1 do n, přičemž na každém domě visí jeho číslo. Jednou si obyvatelé chtěli vystřelit z pošťáka. Během jednoho dne tak postupně prohodili čísla všem $n - 1$ dvojicím sousedních domů. Kolik různých posloupností čísel může být večer v na domech v ulici?

(MEMO 2013)

Úloha 23. Je dáno n přirozené. Určete (v závislosti na n) počet permutací p na množině $1, \ldots, n$, pro něž $p \cdot p$ obrací pořadí čísel (tj. posílá číslo i na $n + 1 - i$ pro všechna $1 \leq i \leq n$).

Úloha 24. V řadě stojí n studentů. Když se učitel nedívá, někteří změní svá místa. Pokud student změnil pozici v řadě z i na j, pohnul se o $|j-i|$ míst. Určete maximální součet míst, o která se mohli pohnout všichni studenti dohromady.

(MEMO 2015)

Úloha 25. Stroj na vyměňování myslí funguje tak, že vždy vymění mysl zvolené dvojici lidí. Tato dvojice těl si už ale nikdy znovu nemůže pomocí stroje znovu vyměnit mysli. Jednoho dne si n lidí hrálo se strojem. Nyní by každý rád získal zpět své tělo. Dokažte, že pokud si na pomoc seženou alespoň dva další kamarády (kteří ještě stroj nikdy nezkoušeli), tak se jim to podaří.

(Futurama)

Úloha 26. Pro sudé $n \geq 4$ mějme tabulku $n \times n$ vyplněnou čísly 1, 2, ..., $\frac{n^2}{2}$, přičemž každé je použito právě dvakrát. Dokažte, že lze vybrat n políček takovým způsobem, aby bylo zvoleno právě jedno políčko z každého řádku i sloupce, a navíc žádná dvě vybraná políčka neobsahovala stejné číslo.

Úloha 27. O Velikonocích hrálo n hráčů turnaj. Každý hrál s každým a nenastaly žádné remízy. Permutací n hráčů je *pomlázková*, pokud se poráželi cyklicky dokola. Dokažte, že se mohlo hrát tak, aby vzniklo alespoň $\frac{n!}{2^n}$ pomlázkových permutací.

Úloha 28. Dokažte, že každý konvexní mnohostěn P v $\mathbb{R}^d$ lze získat jako projekci nějakého k rozměrného simplexu v $\mathbb{R}^n$ pro vhodné n, k (k-rozměrný simplex je mnohostěn, který má $k + 1$ vrcholů, jejichž vzájemné vzdálenosti jsou stejné).

Úloha 29. Dokažte rovnost polynomů

$$\sum_{\pi \in S_n} x^{I(\pi)} = 1 \cdot (1+x) \cdot (1+x+x^2) \dots (1+x+\dots+x^{n-1}),$$

kde $I(\pi)$ značí počet inverzí v pemutaci π, tedy dvojic $1 \leq i < j \leq n$, pro která je $\pi(i) > \pi(j)$.

Nejsou čísla jako čísla...

Většina úloh o permutacích moc nezávisí na tom, jak velkou množinu vlastně permutujeme. Občas je ale potřeba využít i její velikosti, popřípadě se zajímat i o jiné teoriečíselné vlastnosti, které po nás vyžaduje zadání.

Úloha 30. Při večeři sedí $2n$ lidí kolem otočného stolu. Každý si objednal jiné jídlo, ale zmatený číšník rozdal jídla náhodně. Dokažte, že lze stůl otočit tak, aby alespoň dva lidé měli jídlo, které si objednali.

(Brkos)

Úloha 31. Máme balíček $2n$ karet. Zamíchání balíčku změní pořadí karet z a_1, a_2, $\dots$, a_n, b_1, b_2, $\dots$, b_n na a_1, b_1, a_2, b_2, $\dots$, a_n, b_n. Určete všechna n taková, že po 8 zamícháních má balíček karet původní pořadí.

(VJIMC 2014)

Úloha 32. Nechť $p > 2$ je prvočíslo. Pro každou permutaci $\pi = (\pi(1), \pi(2), ..., \pi(p))$ prvků množiny $S = 1, 2, ..., p$ nechť $f(\pi)$ značí počet všech násobků prvočísla p, které se vyskytují mezi následujícími p čísly: $\pi(1), \pi(1) + \pi(2), ..., \pi(1) + \pi(2) + ... + \pi(p)$. Určete průměrnou hodnotu $f(\pi)$ uvažovanou pro všechny permutace π prvků množiny S. (MEMO 2012)

Úloha 33. Pro $n \geq 2$ označíme permutaci σ množiny $1, 2, \dots, n$ jako *kvadratickou* (respektive *kubickou*), jestliže jsou čísla $\sigma_i \cdot \sigma_{i+1} + 1$ druhé (respektive třetí) mocniny přirozených čísel pro všechna i od 1 do $n-1$. Dokažte, že pro nekonečně mnoho n existuje kvadratické permutace, ale pro žádné n neexistuje kubická.

(Irán TST 2014)

Úloha 34. Permutaci $(a_1, a_2, ..., a_n)$ množiny $(1, 2, ..., n)$ nazveme *čtvercovou*, pokud je mezi čísly a_1, $a_1 + a_2$, $\dots$, $a_1 + a_2 + ... + a_n$ alespoň jedna druhá mocnina přirozeného čísla. Najděte všechna přirozená n taková, že jsou všechny permutace množiny $(1, 2, ..., n)$ čtvercové.

(Irán TST 2002)

Parita!

Nyní si ukážeme trikový invariant, který je zachováván při různých zápisech nějaké permutace, zvaný parita permutace. Hezké na něm je to, že jde zjistit hned několika různými způsoby. Tato na první pohled hravá tvrzení mají poměrně hluboké důsledky.

Lemma 35. (Parita transpozic) *Mějme pevnou permutaci σ rozepsanou jako složení n transpozic. Potom parita n nezávisí na konkrétním rozepsání.*

Definice. (Znaménko) Pro permutaci σ uvažme její libovolný rozklad na n transpozic. Pak definujeme její *znaménko* (neboli *paritu*) jako $\operatorname{sgn}(\sigma) = (-1)^n$.

Lemma 36. *Pro libovolné permutace σ, π na stejné množině platí*

$$\operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\pi) = \operatorname{sgn}(\sigma \circ \pi).$$

Lemma 37. *Pro permutaci σ uvažme její rozklad na disjunktní cykly, dále označme k počet těchto cyklů, které mají sudou délku. Potom $\operatorname{sgn}(\sigma) = (-1)^k$.*

Lemma 38. *Inverzí v permutaci σ na množině $1, 2, \ldots, n$ označíme libovolnou dvojici prvků této množiny i, j, které splňují $i < j$ a zároveň $\sigma(i) > \sigma(j)$. Počet různých inverzí v permutaci σ označme l. Potom $\operatorname{sgn}(\sigma) = (-1)^l$.*

Lemma 39. *Uvažme funkci f, které každé permutaci z S_X přiřadí 1 nebo -1. Navíc pro libovolnou dvojici takových permutací σ, τ platí $f(\sigma \circ \tau) = f(\sigma) \cdot f(\tau)$. Potom buď f je konstantně 1, nebo $f = \operatorname{sgn}$.*

Úloha 40. Pro přirozené $n \geq 2$ spočtěte počet sudých permutací n-prvkové množiny.

Úloha 41. Je dán čtverečkovaný hrací plán 4×4. Na čtvercích plánu jsou náhodně rozmístěna čísla $1, 2, \ldots, 15$, každé právě jednou. Poslední pole je volné. V každém tahu můžeme zvolit jedno z polí, která sousedí stranou s volným polem a přesunout číslo, které obsahuje, do volného pole. Hru vyhrajeme právě tehdy, když se nám po konečném počtu kroků povede seřadit všechna čísla postupně po řádcích (a pravý dolní čtvereček zůstane prázdný). Rozhodněte, zda vždy umíme vyhrát.

Úloha 42. Jaká je pravděpodobnost, že hru z předešlého příkladu umíme vyhrát, dostaneme-li na začátku náhodné rozmístění čísel 1, 2, ..., 15?

Úloha 43. Pro přirozené číslo n uvažme množinu S všech permutací na n prvcích. Elsa a Anna hrají následující hru. Každá z nich ve svém tahu vybere jednu permutaci z S, která doteď nebyla zvolena. Pokud lze pomocí skládání a invertování vybraných permutací vyrobit všechny permutace z S, hra končí a hráč, který hrál poslední, prohrává. Elsa přitom hraje první. Pro která n má Elsa vyhrávající strategii?

(IMC 2012)

Úloha 44. Dokažte, že pro libovolnou n-tici reálných čísel $a_1, a_2, \ldots, a_n$ platí identita

$$\sum_{\pi \in S_n} sgn(\pi) \prod_{i=1}^{n} a_{\pi(i)}^{i-1} = \prod_{1 \le i < j \le n} (a_j - a_i).$$

A co na to teorie čísel?

Pojďme si na závěr jště lépe demonstrovat sílu permutací v teorii čísel. Od snadných tvrzení se kouzelně dostaneme až k samotné reciprocitě.

Lemma 45. (Malá Fermatova věta) *Pro prvočíslo p a číslo a, které není dělitelné p, platí $a^{p-1} \equiv 1 \pmod{p}$.*

Lemma 46. (Eulerova věta) *Pro přirozené n označme $\varphi(n)$ počet přirozených čísel $m \le n$, která jsou s ním nesoudělná. Potom pro libovolné a, která je nesoudělné s n, platí $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Lemma 47. (Čínská zbytková věta) *Pro n-tici po dvou nesoudělných čísel $a_1, a_2, \ldots, a_k$ a libovolná celá $b_1, b_2, \ldots, b_k$ existuje právě jedno číslo $0 \le x < a_1 a_2 \ldots a_k$, které dává po dělení číslem a_i zbytek b_i pro všechna $i \in 1, 2, \ldots, k$.*

Definice. (Legendreův symbol) Ať p je prvočíslo, a celé číslo. Potom definujeme Legendreův symbol jako

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{pokud } p \mid a, \\ 1, & \text{pokud a je kvadratický zbytek modulo p,} \\ -1, & \text{pokud a je kvadratický nezbytek modulo p.} \end{cases}$$

Nyní si ještě rozmyslíme jedno lemma bez použití permutací, potom už permutace budou všude.

Lemma 48. (Eulerovo kritérium) *Pro prvočíslo $p \ge 3$ a a celé platí $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.*

Lemma 49. (Gaussovo lemma) *Mějme prvočíslo $p \ge 3$ a a libovolné celé. Označme m počet čísel $a, 2a, \ldots, \frac{p-1}{2}a$, jejichž zbytek modulo p je ostře větší než $\frac{p-1}{2}$. Potom $\left(\frac{a}{p}\right) = (-1)^m$.*

Lemma 50. (Zolotarevovo lemma) *Pro prvočíslo $p \ge 3$ a a nesoudělné s p platí $\left(\frac{a}{p}\right) = \operatorname{sgn}(\pi_a)$, kde π_a značí permutaci indukovanou na zbytcích modulo p násobením číslem a.*

Lemma 51. (Kvadratická reciprocita) *Pro prvočísla $p, q \ge 3$ platí vztah*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Návody

3. První prvek lze vybrat n způsoby, druhý $n-1$ způsoby atd., až poslední jedním způsobem.

4. Indukcí podle počtu členů je to zřejmé.

5. Vyjděte na procházku z nějakého prvku, časem se nutně musíte vrátit. Tím jste našli jeden cyklus.

6. Rozmyslete si, že libovolný cyklus umíte zapsat jako složení transpozic.

7. Stačí vzít nejmenší společný násobek délek všech jejích cyklů.

8. Přesně 8! způsoby, protože pozice věží postupně ve sloupcích zleva doprava odpovídají permutaci osmiprvkové množiny.

9. Rozepište si čísla na součet řádkové a sloupcové části, každou z nich můžete nasčítat zvlášť.

10. Mějme kn různých míčků k barev a n tvarů. Kolik různých posloupností všech míčků můžeme vytvořit, pokud nás zajímají pouze jejich tvary?

11. Sestrojte všechny permutace na n prvcích takovým způsobem, aby pravděpodobnost skutečně nezávisela na k. Co třeba přidávat čísla postupně?

12. Je to $\frac{n+1}{n}$. Spárujte permutace do dvojic podle směru čtení.

13. Permutace si představujte jako posloupnosti kuliček n barev, přičemž každá barva je použita dvakrát. Dvě kuličky stejné bary vedle sebe lze splácnout do jedné. Špatných posloupností je stejně jako dobrých, ve kterých došlo k jednomu splácnutí.

14. Rozmyslete si, že každé takové obarvení odpovídá nějakému seřazení čísel 1, 2, ..., n, které jednoznačně určuje barvy šipek a naopak. Barvy jsou směry.

15. Použijte princip inkluze a exkluze podle počtu.

16. $(2,1,2,1,2,1,3,3) \equiv (6,3,5,2,4,1,8,7)$

17. Použije princip inkluze a exkluze, i-tý člen odpovídá počtu možností, jak udělat nepermutaci pouze s využitím i prvků z n-prvkové množiny.

18. Induktivně dokažte, že takové permutace mohou nanejvýš prohazovat některá sousedící čísla. Posléze si uvědomte, jak se množí králíci.

19. Stačí vzít $n-1$ transpozic vedlejších účastníků. Ukažte, že z nich už lze vygenerovat všechny transpozice, méně triviálně nestačí.

20. Vězni si mohou označit šuplíky svými jmény. Jména v šuplících jsou permutací jmen na nich. Vězeň se vždy otevře ten šuplík, na který ukazuje jméno z předchozího. Rozmyslete si, že neuspějí právě tehdy, když zmíněná permutace obsahuje cyklus délky alespoň $n+1$. pravděpodobnost takového jevu je ale celkem malá.

21. Takové permutace musí mít jeden cyklus délky n. Nějakým prohozením se začít musí, dál už stačí indukce.

22. Vezměte to indukcí ze správného konce, vyjde 2^{n-1}.

23. Rozmyslete si, jakým způsobem se permutace mohou skládat na jednotlivých prvcích. Posléze si permutaci rozložte na nezávislé cykly a v závislosti na n modulo 4 dopočtěte, jak to dopadne.

24. Dokažte, že optimum nastává, třeba když se pořadí studentů otočí. Vhodným přepojování cyklů stačí ukázat, že se při optimální konstrukci prohodil první a poslední student (popř. můžete sumu přepsat s užitím minim původních a nových pozic).

25. Postupujte po cyklech, rozmyslete si, jak přejdete z jednoho na jiný a jak ten poslední dokončíte. Prohození dvou nových lidí si šetřete na konec.

26. Každá taková volba odpovídá nějaké permutaci. Odhadněte shora počet permutací, které obsahují nějaká dvě políčka se stejnými čísla a ukažte, že je ostře menší než $n!$.

27. Vezměte všechny takové turnaje a shora odhadněte počet nepomlázkových permutací ve všech dohromady. Z toho vyplyne, že pomlázkových je v průměru alespoň tolik, jako zadaný zlomek.

28. Dívejte se na souřadnice bodů. Prvních d složek vyplňte souřadnicemi vrcholů P (P pak bude nutně projekcí našeho simplexu). Zbývá přidat libovolný konečný počet souřadnic tak, aby byly vzdálenosti všech vrcholů stejné. Co je na světě nejsymetričtější? Permutace!

29. Postupně přidávejte čísla 1, 2, ..., n. U i-tého máte i možností, ty přidají nějaký pořet inverzí.

30. Předpokládejte, že každé jídlo je posunuté o jiný počet míst ve zvoleném směru modulo $2n$. Dojděte ke sporu porovnáním součtu pozic míst a jídel modulo $2n$.

31. Očíslujte si všechny karty kromě poslední čísly modulo $2n-1$ a lépe popište definované zobrazování.

32. Sčítejte počet vyhovujících k-tic přes k. Pro $k \neq p$ si permutace rozdělte do vhodných skupinek po p permutacích tak, aby v každé skupince vyhovovala právě jedna. Znalost Čínské zbytkové věty výhodou.

33. Pro kvadratické permutace stačí využít identitu $(i-1)\times(i+1) = i^2-1$ a zkonstruovat je. Pro kubické uvažujte největší mocninu dvojky menší rovnou n, ta by musela dělit x^3-1 pro nějaké x, rozkladem polynomu a snadnými odhady dojděte ke sporu s existencí dostatečně malého souseda.

34. Řešením jsou vskutku pouze ta špatná n, pro které je $\frac{n(n+1)}{2}$ čtverec. Pro ostatní čísla si posloupnost $(1, 2, ..., n)$ rozstříhejte na úseky mezi špatnými čísly a vymyslete, jak je na rozstříhnutých místech pozměnit.

35. Jak se změní počet cyklů permutace, vynásobíme-li ji libovolnou permutací?

36. Počet transpozic se sčítá, stejně jako parita.

37. Rozmyslete si, jak rozložit cyklus délky n na $n-1$ transpozic.

38. Každou permutaci na $1, 2, \ldots, n$ jde rozepsat jako složení transpozic sousedních prvků. Parita počtu prohození dvou konkrétních čísel odpovídá tomu, jaké je potom jejich vzájemné pořadí.

39. Ukažte, že f je jednoznačně určena hodnotou na jediné transpozici π. Rozmyslete si tedy, jak napsat libovolnou jinou transpozici tak, aby její znaménko záviselo pouze $\operatorname{sgn}(\pi)$. Je nutné rozebrat dva případy podle toho, kolik má hledaná transpozice společného s π.

40. Je jich přesně polovina. Stačí popárovat sudé a liché permutace do dvojic, třeba složením s pevnou transpozicí.

41. Neumíme. Každému stavu hry odpovídá jedna permutace 16-prvkové množiny. Obarvěte plán šachovnicově a dívejte se, jak souvisí barva volného políčka s paritou permutace.

42. Opravdu je to $\frac{1}{2}$, ale je to mírně technické. Nakreslete přes hrací plán hada, permutace posuzujte podle pořadí neprázdných polí na něm (pohyb prázdného políčka po hadovi toto pořadí nemění). Zbývá dokázat, že všechny pohyby prázdného políčka mimo směr hada už nagenerují všechny sudé permutace.

43. Případy $n \in 2, 3$ rozeberte zvlášť. Pro $n \geq 4$ vhodně použijte paritu a symetrii, které hrají ve prospěch Anně. Je opravdu nutné dávat pozor, abyste nenagenerovali celou S moc brzy.

44. Suma na levé straně je determinant vhodné matice a platí pro něj hodně pěkných vztahů. Pro přehlednost je dobré napsat si do n řádků šachovnice $n \times n$ vzestupně mocniny jednotlivých čísel a_i.

45. Vynásobením všech nenulových zbytků jedním (pevným) dostaneme jejich permutaci. Okamžitě proto $(p-1)! \equiv a^{p-1}(p-1)!$ modulo p.

46. Udělejte to samé, jako při důkazu Malé Fermatovy věty, uvažujte ale pouze zbytky nesoudělné s n.

47. Tvrzení stačí dokázat pro dvě nesoudělná čísla a_1, a_2. Násobení čísel modulo a_1 číslem a_2 je pouze propermutuje. Vezměte správný zbytek modulo a_1 a zkuste k němu násobky a_1 přičítat.

48. Pro kvadratické zbytky tvrzen plyne z Malé Fermatovy věty. Pro nezbytky se zamyslete, kolik nejvýše kořenů může mít polynom stupně $\frac{p-1}{2}$ nad zbytky modulo p.

49. Násobení a zbytky permutuje, převeďte problém na Eulerovo kritérium.

50. Rozmyslete si, že obě funkce dávají pro pevné p oba výsledky -1, 1 a navíc jsou obě multiplikativní. Že pro každé p dává permutace indukovaná nějakým $a$výsledek -1 plyne z existence primitivního prvku. S pomocí primitivního prvku si snadno rozmyslíme, že jsou obě funkce stejné.

51. Uvažujte tabulku $m \times n$ a permutaci odpovídající rozdání karet po řádcích a jejich následné sesbírání po sloupcích. Speciálně se dívejte na její znaménko (které odpovídá znaménku ze vztahu pro kvadratickou reciprocitu). Tuto permutaci lze

navíc z Čínské zbytkové věty elegantně rozložit na součin dvou permutací, jejichž znaménka budou odpovídat současně permutování prvků modulo m násobením n (a naopak). Dokončete Zolotarevovým lematem.

Literatura a zdroje

[1] *Art of Problem Solving*, https://artofproblemsolving.com/
[2] Mirek Olšák: *Kombinatorické nepočítáni*, iKS
[3] Matt Baker: *Zolotarev's magical proof of the Law of Quadratic Reciprocity*
[4] Matoušek, Nešetřil: *Kapitoly z diskrétní matematiky*

A další zdroje napříč internetem.