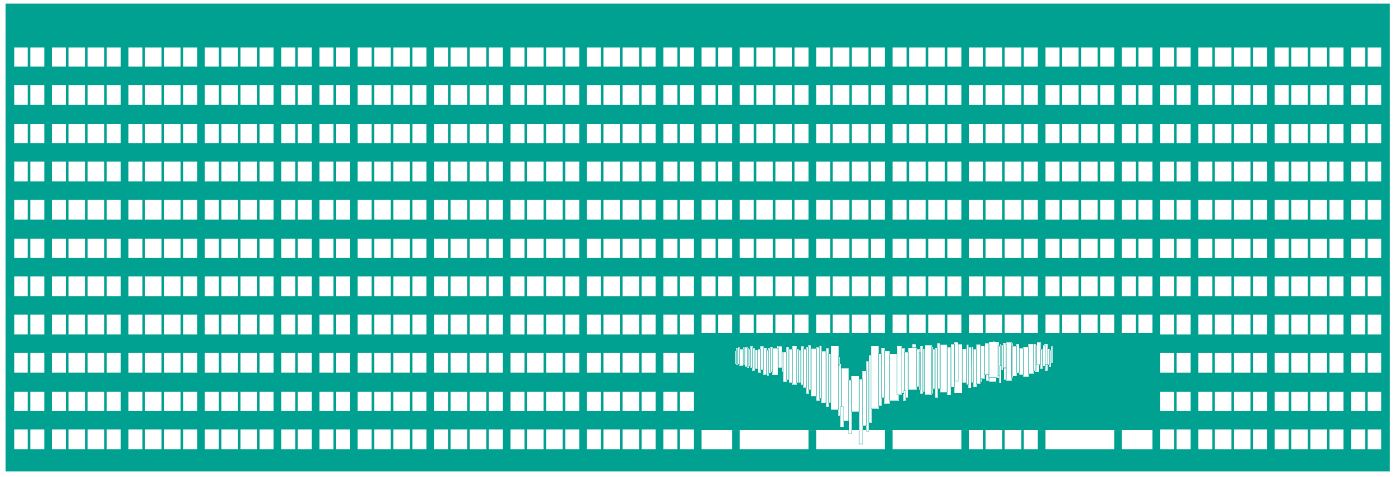
VŠB TECHNICKÁ UNIVERZITA OSTRAVA

VSB TECHNICAL UNIVERSITY OF OSTRAVA



www.vsb.cz

Kretní trik

Petr Kovář
Tereza Kovářová

VŠB – Technická Univerzita Ostrava

petr.kovar@vsb.cz

ŠKOMAM 5.2. 2021, Ostrava

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY | KATEDRA APLIKOVANÉ MATEMATIKY

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | IT4INNOVATIONS NÁRODNÍ SUPERPOČÍTAČOVÉ CENTRUM

Jak trik probíhá

Kouzelník má balíček 124 karet. Karty mají čísla 1, 2, 3, . . . , 124

Jak trik probíhá

Kouzelník má balíček 124 karet. Karty mají čísla 1, 2, 3, . . . , 124

- asistentka nechá diváka vybrat 5 karet,

Jak trik probíhá

Kouzelník má balíček 124 karet. Karty mají čísla 1, 2, 3, . . . , 124

- asistentka nechá diváka vybrat 5 karet,
- asistentka z nich jednu kartu vybere a vrátí ji divákovi

Jak trik probíhá

Kouzelník má balíček 124 karet. Karty mají čísla 1, 2, 3, . . . , 124

- asistentka nechá diváka vybrat 5 karet,
- asistentka z nich jednu kartu vybere a vrátí ji divákovi
- asistentka zbývající karty seřadí do úhledného balíčku a předá kouzelníkovi,
  (položí do řady na stůl, napíše na tabuli, . . .)

Jak trik probíhá

Kouzelník má balíček 124 karet. Karty mají čísla 1, 2, 3, . . . , 124

- asistentka nechá diváka vybrat 5 karet,
- asistentka z nich jednu kartu vybere a vrátí ji divákovi
- asistentka zbývající karty seřadí do úhledného balíčku a předá kouzelníkovi,
  (položí do řady na stůl, napíše na tabuli, . . .)
- kouzelník se na karty podívá a pozná divákovu kartu.

Jak trik probíhá

Kouzelník má balíček 124 karet. Karty mají čísla 1, 2, 3, . . . , 124

- asistentka nechá diváka vybrat 5 karet,
- asistentka z nich jednu kartu vybere a vrátí ji divákovi
- asistentka zbývající karty seřadí do úhledného balíčku a předá kouzelníkovi,
  (položí do řady na stůl, napíše na tabuli, . . .)
- kouzelník se na karty podívá a pozná divákovu kartu.

Veškerá informace jen v předávaných kartách.

Jak trik probíhá

Kouzelník má balíček 124 karet. Karty mají čísla 1, 2, 3, . . . , 124

- asistentka nechá diváka vybrat 5 karet,
- asistentka z nich jednu kartu vybere a vrátí ji divákovi
- asistentka zbývající karty seřadí do úhledného balíčku a předá kouzelníkovi,
  (položí do řady na stůl, napíše na tabuli, . . .)
- kouzelník se na karty podívá a pozná divákovu kartu.

Veškerá informace jen v předávaných kartách.

. . . Vyzkoušejme to!

Videa

Příklad 1 – video

Příklad 2 – video

Teoretické maximum

Karet v balíčku je 124 karet.
Aby popsaný proces vždy fungoval, nemůže jich být ani o jednu více!

- asistentka vybere jednu kartu z pěti $\binom{5}{1} = 5$

Teoretické maximum

Karet v balíčku je 124 karet.
Aby popsaný proces vždy fungoval, nemůže jich být ani o jednu více!

- asistentka vybere jednu kartu z pěti $\binom{5}{1} = 5$
- pořadí čtyř karet $4! = 24$

Teoretické maximum

Karet v balíčku je 124 karet.
Aby popsaný proces vždy fungoval, nemůže jich být ani o jednu více!

- asistentka vybere jednu kartu z pěti $\binom{5}{1} = 5$
- pořadí čtyř karet $4! = 24$
- jistě to není žádná ze 4 předaných karet

Teoretické maximum

Karet v balíčku je 124 karet.
Aby popsaný proces vždy fungoval, nemůže jich být ani o jednu více!

- asistentka vybere jednu kartu z pěti $\binom{5}{1} = 5$
- pořadí čtyř karet $4! = 24$
- jistě to není žádná ze 4 předaných karet

Celkem $5 \cdot 24 + 4 = 124$ karet.

Teoretické maximum

Karet v balíčku je 124 karet.
Aby popsaný proces vždy fungoval, nemůže jich být ani o jednu více!

- asistentka vybere jednu kartu z pěti $\binom{5}{1} = 5$
- pořadí čtyř karet $4! = 24$
- jistě to není žádná ze 4 předaných karet

Celkem $5 \cdot 24 + 4 = 124$ karet.

Tohoto maxima lze dosáhnout!

V našem balíčku jsou karty 1, 2, . . . , 124.

Existence řešení

Všech pětic z $n = 124$ karet je

$$p = \binom{124}{5} = \frac{124 \cdot 123 \cdot 122 \cdot 121 \cdot 120}{120}$$

Existence řešení

Všech pětic z $n = 124$ karet je

$$p = \binom{124}{5} = \frac{124 \cdot 123 \cdot 122 \cdot 121 \cdot 120}{120} = 225\ 150\ 024.$$

Existence řešení

Všech pětic z $n = 124$ karet je

$$p = \binom{124}{5} = \frac{124 \cdot 123 \cdot 122 \cdot 121 \cdot 120}{120} = 225\ 150\ 024.$$

Všech čtveřic z $n = 124$ karet je

$$c = \binom{124}{4} = \frac{124 \cdot 123 \cdot 122 \cdot 121}{24} = \frac{p}{24}.$$

Existence řešení

Všech pětic z $n = 124$ karet je

$$p = \binom{124}{5} = \frac{124 \cdot 123 \cdot 122 \cdot 121 \cdot 120}{120} = 225\ 150\ 024.$$

Všech čtveřic z $n = 124$ karet je

$$c = \binom{124}{4} = \frac{124 \cdot 123 \cdot 122 \cdot 121}{24} = \frac{p}{24}.$$

Různých pořadí čtyř karet je právě 24!

Existence řešení

Všech pětic z $n = 124$ karet je

$$p = \binom{124}{5} = \frac{124 \cdot 123 \cdot 122 \cdot 121 \cdot 120}{120} = 225\ 150\ 024.$$

Všech čtveřic z $n = 124$ karet je

$$c = \binom{124}{4} = \frac{124 \cdot 123 \cdot 122 \cdot 121}{24} = \frac{p}{24}.$$

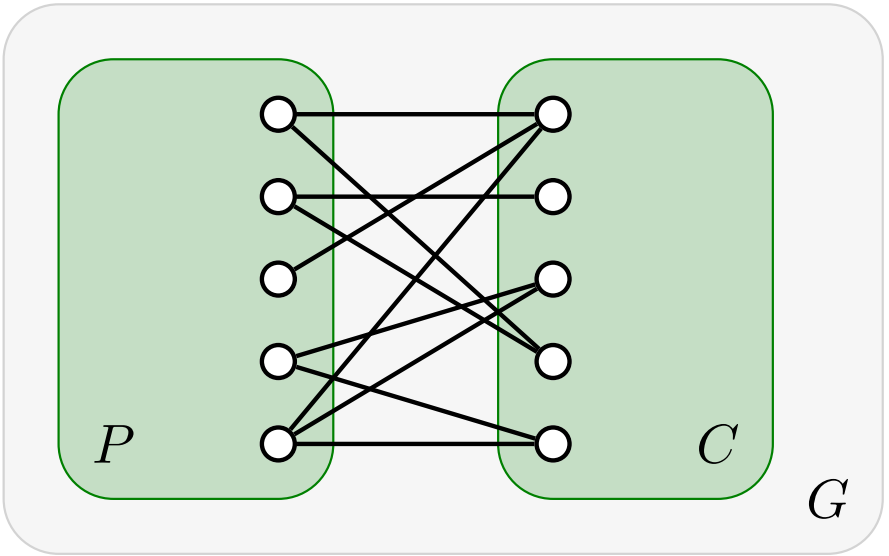
Různých pořadí čtyř karet je právě 24!

Stačí každé **uspořádané** čtveřici (a_1, a_2, a_3, a_4) jednoznačně přiřadit některou **neuspořádanou** pětici $\{a_1, a_2, a_3, a_4, x\}$ (a naopak).

Existence řešení

Hallova věta

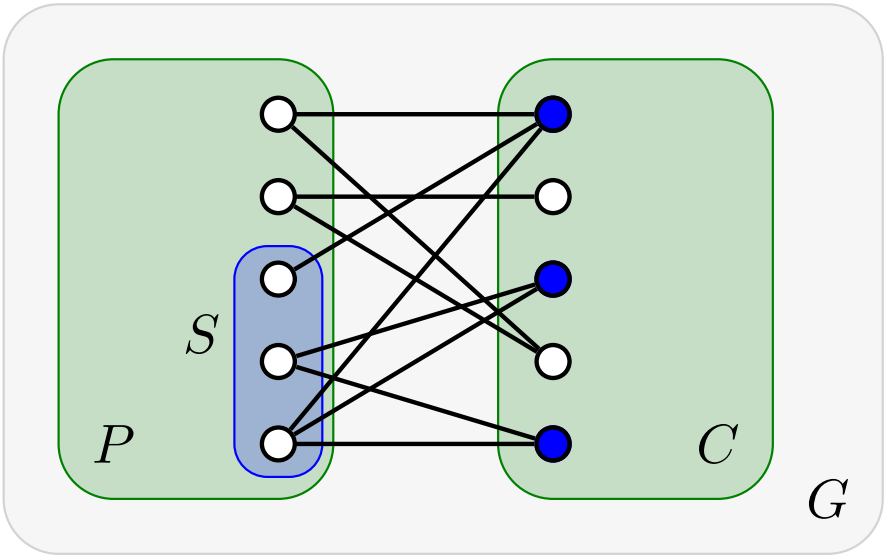
Nechť G je bipartitní graf s partitami P a C. Graf G má párování M, které saturuje všechny vrcholy množiny P právě tehdy, když $|S| \leq |N(S)|$ pro každou podmnožinu $S \subseteq P$.



Existence řešení

Hallova věta

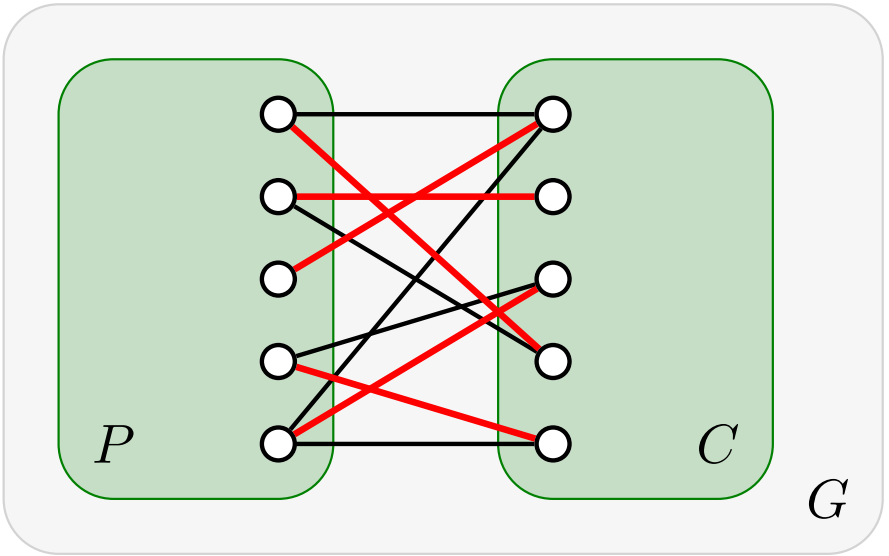
Nechť G je bipartitní graf s partitami P a C. Graf G má párování M, které saturuje všechny vrcholy množiny P právě tehdy, když $|S| \leq |N(S)|$ pro každou podmnožinu $S \subseteq P$.



Existence řešení

Hallova věta

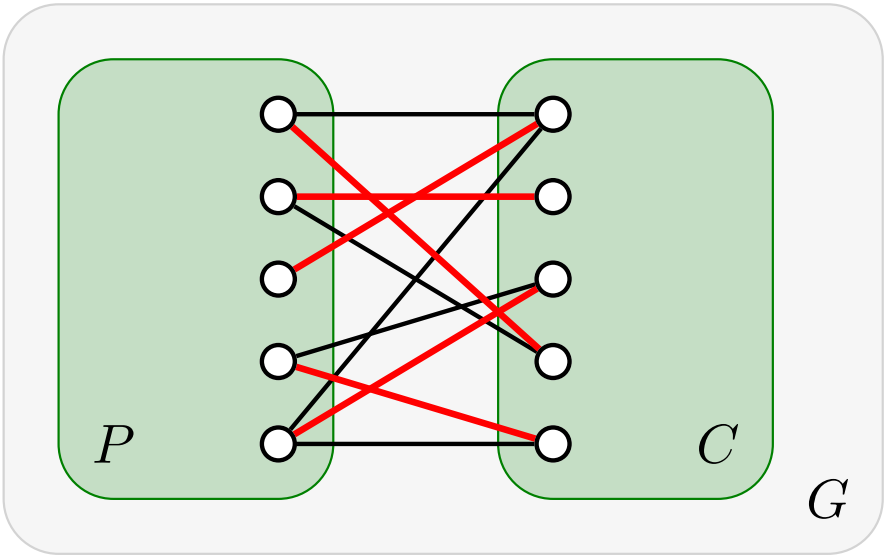
Nechť G je bipartitní graf s partitami P a C. Graf G má párování M, které saturuje všechny vrcholy množiny P právě tehdy, když $|S| \leq |N(S)|$ pro každou podmnožinu $S \subseteq P$.



Existence řešení

Hallova věta

Nechť G je bipartitní graf s partitami P a C. Graf G má párování M, které saturuje všechny vrcholy množiny P právě tehdy, když $|S| \leq |N(S)|$ pro každou podmnožinu $S \subseteq P$.



Důsledek

Každý pravidelný bipartitní graf s alespoň jednou hranou má úplné párování.

Existence z (důsledku) Hallovy věty

Sestavíme bipartitní graf $G = (P \cup C, E)$:

Existence z (důsledku) Hallovy věty

Sestavíme bipartitní graf $G = (P \cup C, E)$:
Partita P – všechny *neuspořádané* pětice karet.
Partita C – všechny *uspořádané* čtveřice karet.

Existence z (důsledku) Hallovy věty

Sestavíme bipartitní graf $G = (P \cup C, E)$:
Partita P – všechny *neuspořádané* pětice karet.
Partita C – všechny *uspořádané* čtveřice karet.

Každá partita má $124 \cdot 123 \cdot 122 \cdot 121 = 225\ 150\ 024$ vrcholů.

Existence z (důsledku) Hallovy věty

Sestavíme bipartitní graf $G = (P \cup C, E)$:
Partita P – všechny *neuspořádané* pětice karet.
Partita C – všechny *uspořádané* čtveřice karet.

Každá partita má $124 \cdot 123 \cdot 122 \cdot 121 = 225\ 150\ 024$ vrcholů.

Každá čtveřice spojena se 120 pěticemi
(ve kterých se čtveřice vyskytuje) a pátá karta je pak jednoznačně určena.

Existence z (důsledku) Hallovy věty

Sestavíme bipartitní graf $G = (P \cup C, E)$:
Partita P – všechny *neuspořádané* pětice karet.
Partita C – všechny *uspořádané* čtveřice karet.

Každá partita má $124 \cdot 123 \cdot 122 \cdot 121 = 225\ 150\ 024$ vrcholů.

Každá čtveřice spojena se 120 pěticemi
(ve kterých se čtveřice vyskytuje) a pátá karta je pak jednoznačně určena.

Současně je každá pětice spojena se 120 čtveřicemi
celkem $\binom{5}{4} = 5$ čtveřic, každá v některém z $P(4) = 24$ pořadí.

Existence z (důsledku) Hallovy věty

Sestavíme bipartitní graf $G = (P \cup C, E)$:
Partita P – všechny *neuspořádané* pětice karet.
Partita C – všechny *uspořádané* čtveřice karet.

Každá partita má $124 \cdot 123 \cdot 122 \cdot 121 = 225\ 150\ 024$ vrcholů.

Každá čtveřice spojena se 120 pěticemi
(ve kterých se čtveřice vyskytuje) a pátá karta je pak jednoznačně určena.

Současně je každá pětice spojena se 120 čtveřicemi
celkem $\binom{5}{4} = 5$ čtveřic, každá v některém z $P(4) = 24$ pořadí.

G je 120-pravidelný bipartitní graf a podle (důsledku) Hallovy věty v něm existuje úplné párování M.
Stačí si zapamatovat $|M| = 225\ 150\ 024$ hran párování.

Bipartitní graf G s partitami P a C.

Bipartitní graf G s partitami P a C.

Pohár ŠKOMAMu

Kdybychom graf nakreslili na papír tak, aby na každý vrchol připadal $1\mathrm{cm}^2$ (120 incidentních hran), jak velký bude papír?
Kolik čtverečních metrů bude mít?

Pohár ŠKOMAMu

Kdybychom graf nakreslili na papír tak, aby na každý vrchol připadal $1\mathrm{cm}^2$ (120 incidentních hran), jak velký bude papír?
Kolik čtverečních metrů bude mít?

$$124 \cdot 123 \cdot 122 \cdot 121 \cdot 2 \ \mathrm{cm}^2 \quad = \quad 450\ 300\ 048 \ \mathrm{cm}^2 = 45\ 030,0048 \ \mathrm{m}^2$$

Pohár ŠKOMAMu

Kdybychom graf nakreslili na papír tak, aby na každý vrchol připadal $1\mathrm{cm}^2$ (120 incidentních hran), jak velký bude papír?
Kolik čtverečních metrů bude mít?

$$\begin{aligned} 124 \cdot 123 \cdot 122 \cdot 121 \cdot 2 \ \mathrm{cm}^2 &= 450\ 300\ 048 \ \mathrm{cm}^2 = 45\ 030,0048 \ \mathrm{m}^2 \\ &\doteq 4,5 \ \text{hektaru.} \end{aligned}$$

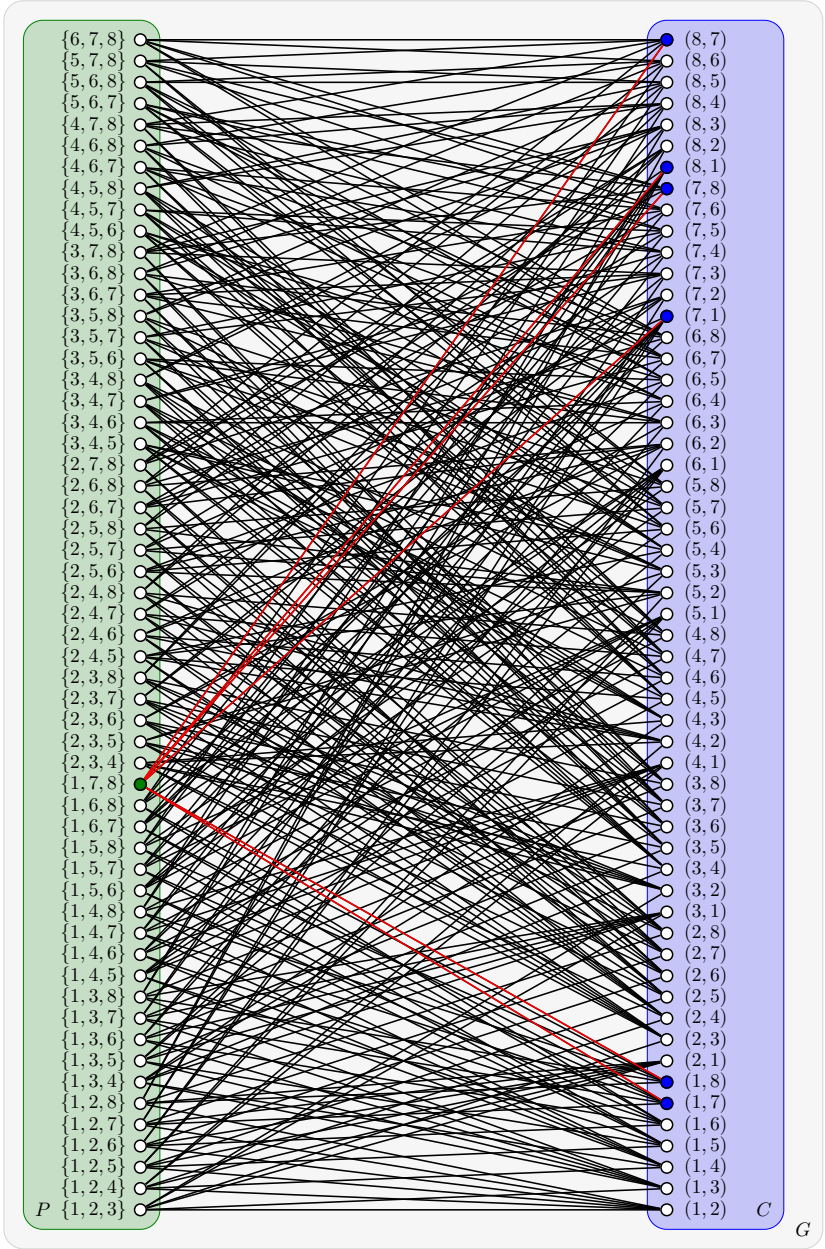
Pohár ŠKOMAMu

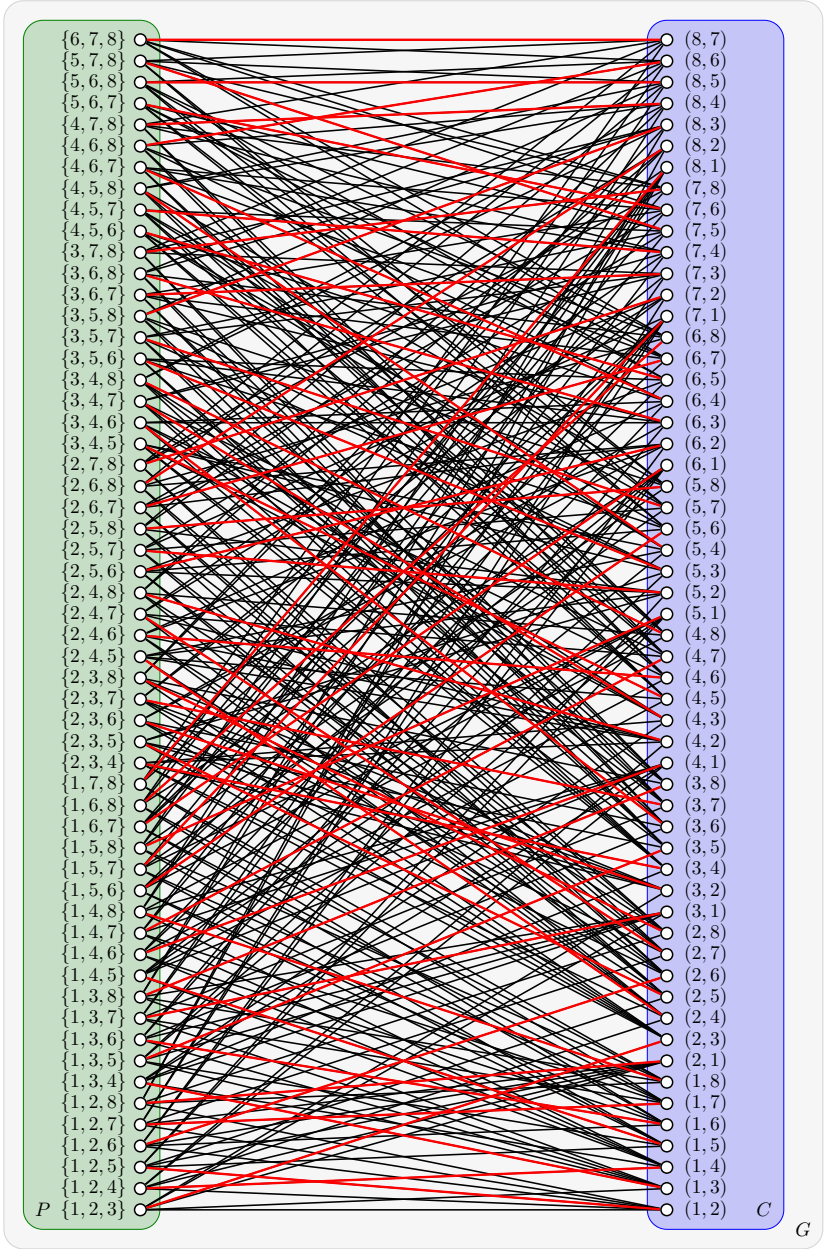
Kdybychom graf nakreslili na papír tak, aby na každý vrchol připadal $1\mathrm{cm}^2$ (120 incidentních hran), jak velký bude papír?
Kolik čtverečních metrů bude mít?

$$\begin{aligned} 124 \cdot 123 \cdot 122 \cdot 121 \cdot 2\ \mathrm{cm}^2 &= 450\ 300\ 048\ \mathrm{cm}^2 = 45\ 030,0048\ \mathrm{m}^2 \\ &\doteq 4,5\ \text{hektaru.} \end{aligned}$$

. . . více než 6 fotbalových hřišť.

Bipartitní graf G s partitami P a C.


{6, 7, 8}
{5, 7, 8}
{5, 6, 8}
{5, 6, 7}
{4, 7, 8}
{4, 6, 8}
{4, 6, 7}
{4, 5, 8}
{4, 5, 7}
{4, 5, 6}
{3, 7, 8}
{3, 6, 8}
{3, 6, 7}
{3, 5, 8}
{3, 5, 7}
{3, 5, 6}
{3, 4, 8}
{3, 4, 7}
{3, 4, 6}
{3, 4, 5}
{2, 7, 8}
{2, 6, 8}
{2, 6, 7}
{2, 5, 8}
{2, 5, 7}
{2, 5, 6}
{2, 4, 8}
{2, 4, 7}
{2, 4, 6}
{2, 4, 5}
{2, 3, 8}
{2, 3, 7}
{2, 3, 6}
{2, 3, 5}
{2, 3, 4}
{1, 7, 8}
{1, 6, 8}
{1, 6, 7}
{1, 5, 8}
{1, 5, 7}
{1, 5, 6}
{1, 4, 8}
{1, 4, 7}
{1, 4, 6}
{1, 4, 5}
{1, 3, 8}
{1, 3, 7}
{1, 3, 6}
{1, 3, 5}
{1, 3, 4}
{1, 2, 8}
{1, 2, 7}
{1, 2, 6}
{1, 2, 5}
{1, 2, 4}
P {1, 2, 3}
(8, 7)
(8, 6)
(8, 5)
(8, 4)
(8, 3)
(8, 2)
(8, 1)
(7, 8)
(7, 6)
(7, 5)
(7, 4)
(7, 3)
(7, 2)
(7, 1)
(6, 8)
(6, 7)
(6, 5)
(6, 4)
(6, 3)
(6, 2)
(6, 1)
(5, 8)
(5, 7)
(5, 6)
(5, 4)
(5, 3)
(5, 2)
(5, 1)
(4, 8)
(4, 7)
(4, 6)
(4, 5)
(4, 3)
(4, 2)
(4, 1)
(3, 8)
(3, 7)
(3, 6)
(3, 5)
(3, 4)
(3, 2)
(3, 1)
(2, 8)
(2, 7)
(2, 6)
(2, 5)
(2, 4)
(2, 3)
(2, 1)
(1, 8)
(1, 7)
(1, 6)
(1, 5)
(1, 4)
(1, 3)
(1, 2) C
G


{6, 7, 8}
{5, 7, 8}
{5, 6, 8}
{5, 6, 7}
{4, 7, 8}
{4, 6, 8}
{4, 6, 7}
{4, 5, 8}
{4, 5, 7}
{4, 5, 6}
{3, 7, 8}
{3, 6, 8}
{3, 6, 7}
{3, 5, 8}
{3, 5, 7}
{3, 5, 6}
{3, 4, 8}
{3, 4, 7}
{3, 4, 6}
{3, 4, 5}
{2, 7, 8}
{2, 6, 8}
{2, 6, 7}
{2, 5, 8}
{2, 5, 7}
{2, 5, 6}
{2, 4, 8}
{2, 4, 7}
{2, 4, 6}
{2, 4, 5}
{2, 3, 8}
{2, 3, 7}
{2, 3, 6}
{2, 3, 5}
{2, 3, 4}
{1, 7, 8}
{1, 6, 8}
{1, 6, 7}
{1, 5, 8}
{1, 5, 7}
{1, 5, 6}
{1, 4, 8}
{1, 4, 7}
{1, 4, 6}
{1, 4, 5}
{1, 3, 8}
{1, 3, 7}
{1, 3, 6}
{1, 3, 5}
{1, 3, 4}
{1, 2, 8}
{1, 2, 7}
{1, 2, 6}
{1, 2, 5}
{1, 2, 4}
P {1, 2, 3}
(8, 7)
(8, 6)
(8, 5)
(8, 4)
(8, 3)
(8, 2)
(8, 1)
(7, 8)
(7, 6)
(7, 5)
(7, 4)
(7, 3)
(7, 2)
(7, 1)
(6, 8)
(6, 7)
(6, 5)
(6, 4)
(6, 3)
(6, 2)
(6, 1)
(5, 8)
(5, 7)
(5, 6)
(5, 4)
(5, 3)
(5, 2)
(5, 1)
(4, 8)
(4, 7)
(4, 6)
(4, 5)
(4, 3)
(4, 2)
(4, 1)
(3, 8)
(3, 7)
(3, 6)
(3, 5)
(3, 4)
(3, 2)
(3, 1)
(2, 8)
(2, 7)
(2, 6)
(2, 5)
(2, 4)
(2, 3)
(2, 1)
(1, 8)
(1, 7)
(1, 6)
(1, 5)
(1, 4)
(1, 3)
(1, 2) C
G

Řešení hrubou (výpočetní) silou

Pro velký graf s

$$2 \cdot 225\ 150\ 024 = 450\ 300\ 048 \text{ vrcholy}$$

není problém najít párování na počítači.
(hodiny strojového času)

Řešení hrubou (výpočetní) silou

Pro velký graf s

$$2 \cdot 225\ 150\ 024 = 450\ 300\ 048 \text{ vrcholy}$$

není problém najít párování na počítači.
(hodiny strojového času)

Párování jsme našli,

Řešení hrubou (výpočetní) silou

Pro velký graf s

$$2 \cdot 225\ 150\ 024 = 450\ 300\ 048 \text{ vrcholy}$$

není problém najít párování na počítači.
(hodiny strojového času)

Párování jsme našli, pak jsme si 225 150 024 dvojic zapamatovali . . .

Řešení hrubou (výpočetní) silou

Pro velký graf s

$$2 \cdot 225\ 150\ 024 = 450\ 300\ 048 \text{ vrcholy}$$

není problém najít párování na počítači.
(hodiny strojového času)

Párování jsme našli, pak jsme si 225 150 024 dvojic zapamatovali . . .

. . . a je to, můžeme trik předvádět!

Děkuji za pozornost.

Jednodušší řešení

Tak moment!

Nikdo se nebude učit $225\ 150\ 024$ dvojic zpaměti!

Jednodušší řešení

Tak moment!
Nikdo se nebude učit $225\ 150\ 024$ dvojic zpaměti!

Samozřejmě existuje elegantnější řešení.

"It keeps me from looking at my phone every two seconds."
Liam Walsh/The New Yorker

O kongruencích

Kongruentní čísla

Řekneme, že dvě celá čísla a, b jsou *kongruentní modulo* n, jestliže dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n. Číslo n nazýváme *modul*.

Píšeme $a \equiv b \pmod{n}$.

O kongruencích

Kongruentní čísla

Řekneme, že dvě celá čísla a, b jsou *kongruentní modulo* n, jestliže dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n. Číslo n nazýváme *modul*.

Píšeme $a \equiv b \pmod{n}$.

Příklady

- $52 \equiv 12 \pmod{10}$

O kongruencích

Kongruentní čísla

Řekneme, že dvě celá čísla a, b jsou *kongruentní modulo* n, jestliže dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n. Číslo n nazýváme *modul*.

Píšeme $a \equiv b \pmod{n}$.

Příklady

- $52 \equiv 12 \pmod{10}$
- $3 \not\equiv 15 \pmod{10}$

O kongruencích

Kongruentní čísla

Řekneme, že dvě celá čísla a, b jsou *kongruentní modulo* n, jestliže dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n. Číslo n nazýváme *modul*.

Píšeme $a \equiv b \pmod{n}$.

Příklady

- $52 \equiv 12 \pmod{10}$
- $3 \not\equiv 15 \pmod{10}$
- $3 \equiv 15 \pmod{12}$

O kongruencích

Kongruentní čísla

Řekneme, že dvě celá čísla a, b jsou *kongruentní modulo* n, jestliže dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n. Číslo n nazýváme *modul*.

Píšeme $a \equiv b \pmod{n}$.

Příklady

- $52 \equiv 12 \pmod{10}$
- $3 \not\equiv 15 \pmod{10}$
- $3 \equiv 15 \pmod{12}$
- $3 \not\equiv 15 \pmod{5}$

O kongruencích

Kongruentní čísla

Řekneme, že dvě celá čísla a, b jsou *kongruentní modulo* n, jestliže dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n. Číslo n nazýváme *modul*.

Píšeme $a \equiv b \pmod{n}$.

Příklady

- $52 \equiv 12 \pmod{10}$
- $3 \not\equiv 15 \pmod{10}$
- $3 \equiv 15 \pmod{12}$
- $3 \not\equiv 15 \pmod{5}$
- $13 \equiv 28 \pmod{5}$

O kongruencích

Kongruentní čísla

Řekneme, že dvě celá čísla a, b jsou *kongruentní modulo* n, jestliže dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n. Číslo n nazýváme *modul*.

Píšeme $a \equiv b \pmod{n}$.

Příklady

- $52 \equiv 12 \pmod{10}$
- $3 \not\equiv 15 \pmod{10}$
- $3 \equiv 15 \pmod{12}$
- $3 \not\equiv 15 \pmod{5}$
- $13 \equiv 28 \pmod{5}$
- $-1 \equiv 4 \pmod{5}$

Čísla a, b jsou kongruentní modulo n

Alternativně můžeme říci, že čísla a, b

- dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n,
- rozdíl $a - b$ je násobkem čísla n,
- číslo b dostaneme z čísla a přičtením násobku čísla n.

Čísla a, b jsou kongruentní modulo n

Alternativně můžeme říci, že čísla a, b

- dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n,
- rozdíl $a - b$ je násobkem čísla n,
- číslo b dostaneme z čísla a přičtením násobku čísla n.

Příklad na hodinách

- $3 \equiv 15 \pmod{12}$

Čísla a, b jsou kongruentní modulo n

Alternativně můžeme říci, že čísla a, b

- dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n,
- rozdíl $a - b$ je násobkem čísla n,
- číslo b dostaneme z čísla a přičtením násobku čísla n.

Příklad na hodinách

- $3 \equiv 15 \pmod{12}$
- rozdíl $15 - 3$ je (násobkem) čísla 12

Čísla a, b jsou kongruentní modulo n

Alternativně můžeme říci, že čísla a, b

- dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n,
- rozdíl $a - b$ je násobkem čísla n,
- číslo b dostaneme z čísla a přičtením násobku čísla n.

Příklad na hodinách

- $3 \equiv 15 \pmod{12}$
- rozdíl $15 - 3$ je (násobkem) čísla 12
- číslo 15 dostanu z čísla 3 přičtením (násobku) 12

Čísla a, b jsou kongruentní modulo n

Alternativně můžeme říci, že čísla a, b

- dávají stejný zbytek po (celočíselném) dělení přirozeným číslem n,
- rozdíl $a - b$ je násobkem čísla n,
- číslo b dostaneme z čísla a přičtením násobku čísla n.

Příklad na hodinách

- $3 \equiv 15 \pmod{12}$
- rozdíl $15 - 3$ je (násobkem) čísla 12
- číslo 15 dostanu z čísla 3 přičtením (násobku) 12

V některých situacích pak kongruentní čísla (případně výrazy) s výhodou považujeme za „ekvivalentní“ nebo „stejná“ vzhledem k celočíselnému dělení, přesněji vzhledem k celočíselným zbytkům.

Další využití modulární aritmetiky

- kontrolní součty: $23\ 536 + 47\ 461 \neq 19\ 272 + 51\ 626$

Další využití modulární aritmetiky

- kontrolní součty: $23\ 536 + 47\ 461 \neq 19\ 272 + 51\ 626$
- ISBN kódy
- čárové kódy

Další využití modulární aritmetiky

- kontrolní součty: $23\ 536 + 47\ 461 \neq 19\ 272 + 51\ 626$
- ISBN kódy
- čárové kódy
- rodná čísla
- čísla účtů

Další využití modulární aritmetiky

- kontrolní součty: $23\ 536 + 47\ 461 \neq 19\ 272 + 51\ 626$
- ISBN kódy
- čárové kódy
- rodná čísla
- čísla účtů
- šifrování
- záznam CD/DVD

Další využití modulární aritmetiky

- kontrolní součty: $23\ 536 + 47\ 461 \neq 19\ 272 + 51\ 626$
- ISBN kódy
- čárové kódy
- rodná čísla
- čísla účtů
- šifrování
- záznam CD/DVD
- digitální přenos dat

Karetní trik – popis konstruktivního řešení

Označme si vytažené karty $x_0 < x_1 < x_2 < x_3 < x_4$.

Karetní trik – popis konstruktivního řešení

Označme si vytažené karty $x_0 < x_1 < x_2 < x_3 < x_4$.

Asistentka (zpaměti) vypočítá zbytek i po dělení čísla $s = x_0 + x_1 + x_2 + x_3 + x_4$ číslem 5.

Karetní trik – popis konstruktivního řešení

Označme si vytažené karty $x_0 < x_1 < x_2 < x_3 < x_4$.

Asistentka (zpaměti) vypočítá zbytek i po dělení čísla $s = x_0 + x_1 + x_2 + x_3 + x_4$ číslem 5.

Označme $i \equiv s \pmod 5$, $i \in [0, 4]$.

Karetní trik – popis konstruktivního řešení

Označme si vytažené karty $x_0 < x_1 < x_2 < x_3 < x_4$.

Asistentka (zpaměti) vypočítá zbytek i po dělení čísla $s = x_0 + x_1 + x_2 + x_3 + x_4$ číslem 5.

Označme $i \equiv s \pmod 5$, $i \in [0, 4]$.

Asistentka zvolí kartu x_i.

Karetní trik – popis konstruktivního řešení

Označme si vytažené karty $x_0 < x_1 < x_2 < x_3 < x_4$.

Asistentka (zpaměti) vypočítá zbytek i po dělení čísla $s = x_0 + x_1 + x_2 + x_3 + x_4$ číslem 5.

Označme $i \equiv s \pmod 5$, $i \in [0, 4]$.

Asistentka zvolí kartu x_i.

Označíme $y = x_i - i$, kde $y \in [1, 120]$.

Číslo y je pořadí chybějící karty.

Popis konstruktivního řešení (pokračování)

Protože $y = x_i - i$, tak platí kongruence

$$\begin{aligned} x_i - y &\equiv i \pmod 5 \\ x_i - y &\equiv s \pmod 5. \end{aligned} \tag{1}$$

Popis konstruktivního řešení (pokračování)

Protože $y = x_i - i$, tak platí kongruence

$$\begin{aligned} x_i - y &\equiv i \pmod 5 \\ x_i - y &\equiv s \pmod 5. \end{aligned} \tag{1}$$

Součet zbývajících 4 karet $r = x_0 + x_1 + x_2 + x_3 + x_4 - x_i = s - x_i$.

$$x_i = s - r. \tag{2}$$

Popis konstruktivního řešení (pokračování)

Protože $y = x_i - i$, tak platí kongruence

$$\begin{aligned} x_i - y &\equiv i \pmod 5 \\ x_i - y &\equiv s \pmod 5. \end{aligned} \tag{1}$$

Součet zbývajících 4 karet $r = x_0 + x_1 + x_2 + x_3 + x_4 - x_i = s - x_i$.

$$x_i = s - r. \tag{2}$$

Dosazením (??) do (??) dostaneme kongruenci

$$\begin{aligned} s - r - y &\equiv s \pmod 5 \\ -r - y &\equiv 0 \pmod 5 \\ -r &\equiv y \pmod 5. \end{aligned} \tag{3}$$

Klíčové je, že pořadí y chybějící karty je kongruentní s číslem $-r$.

Popis konstruktivního řešení (pokračování)

Mezi 120 zbývajícími kartami je každé páté číslo, tedy $120/5 = 24$ čísel kongruentních s číslem $-r \pmod 5$.
Které z 24 možných čísel to je, se zakomponuje do posloupnosti čtyř předaných karet.

Popis konstruktivního řešení (pokračování)

Mezi 120 zbývajícími kartami je každé páté číslo, tedy $120/5 = 24$ čísel kongruentních s číslem $-r \pmod 5$.
Které z 24 možných čísel to je, se zakomponuje do posloupnosti čtyř předaných karet.

Pozor! Divák má kartu s číslem x_i (nikoliv y) a kouzelník nezná x_i, jen určí y.

Popis konstruktivního řešení (pokračování)

Mezi 120 zbývajícími kartami je každé páté číslo, tedy $120/5 = 24$ čísel kongruentních s číslem $-r \pmod 5$.
Které z 24 možných čísel to je, se zakomponuje do posloupnosti čtyř předaných karet.

Pozor! Divák má kartu s číslem x_i (nikoliv y) a kouzelník nezná x_i, jen určí y.

Podle domluvy divák dostane kartu x_i.
Jen díky úmluvě lze určit i (počet karet menších než y).
A proto kouzelník může vypočítat $x_i = y + i$.

Popis konstruktivního řešení (pokračování)

Mezi 120 zbývajícími kartami je každé páté číslo, tedy $120/5 = 24$ čísel kongruentních s číslem $-r \pmod 5$.
Které z 24 možných čísel to je, se zakomponuje do posloupnosti čtyř předaných karet.

Pozor! Divák má kartu s číslem x_i (nikoliv y) a kouzelník nezná x_i, jen určí y.

Podle domluvy divák dostane kartu x_i.
Jen díky úmluvě lze určit i (počet karet menších než y).
A proto kouzelník může vypočítat $x_i = y + i$.

Místo $225\ 150\ 024$ dvojic si zapamatujeme 24 permutací čtyř prvků, zbývající údaje lze dopočítat.

Příklad

Divák vybere $11, 37, 39, 90, 105$ (už seřazeno).

Příklad

Divák vybere $11, 37, 39, 90, 105$ (už seřazeno).

Asistentka vypočítá

$$\begin{aligned} s &= 11 + 37 + 39 + 90 + 105 \equiv \\ &\equiv 1 + 2 + 4 + 0 + 0 \equiv 2 \pmod 5 \\ i &= 2. \end{aligned}$$

Divákovi vrátí kartu $x_2 = 39$ a určí $y = 39 - i = 39 - 2 = 37$.

Příklad

Divák vybere $11, 37, 39, 90, 105$ (už seřazeno).

Asistentka vypočítá

$$\begin{aligned} s &= 11 + 37 + 39 + 90 + 105 \equiv \\ &\equiv 1 + 2 + 4 + 0 + 0 \equiv 2 \pmod 5 \\ i &= 2. \end{aligned}$$

Divákovi vrátí kartu $x_2 = 39$ a určí $y = 39 - i = 39 - 2 = 37$.

Nyní číslo 37 „jakoby“ vydělíme se zbytkem číslem 5.

$$y = 37 = 7 \cdot 5 + 2 = 8 \cdot 5 - 3$$

Proto nejbližší vyšší násobek čísla 5 je číslo $40 = 8 \cdot 5$ a platí $k = 8$.
Není to dělení se zbytkem, zbytek není záporný!

Příklad

Divák vybere $11, 37, 39, 90, 105$ (už seřazeno).

Asistentka vypočítá

$$\begin{aligned} s &= 11 + 37 + 39 + 90 + 105 \equiv \\ &\equiv 1 + 2 + 4 + 0 + 0 \equiv 2 \pmod 5 \\ i &= 2. \end{aligned}$$

Divákovi vrátí kartu $x_2 = 39$ a určí $y = 39 - i = 39 - 2 = 37$.

Nyní číslo 37 „jakoby“ vydělíme se zbytkem číslem 5.

$$y = 37 = 7 \cdot 5 + 2 = 8 \cdot 5 - 3$$

Proto nejbližší vyšší násobek čísla 5 je číslo $40 = 8 \cdot 5$ a platí $k = 8$.
Není to dělení se zbytkem, zbytek není záporný!

Předávaná posloupnost karet je $37, 11, 105, 90$.
(k-tá, tj. osmá posloupnost v tabulce, kterou hned ukážeme.)

24 permutací

k	permutace	k	permutace
1	1 2 3 4	13	3 1 2 4
2	1 2 4 3	14	3 1 4 2
3	1 3 2 4	15	3 2 1 4
4	1 3 4 2	16	3 2 4 1
5	1 4 2 3	17	3 4 1 2
6	1 4 3 2	18	3 4 2 1
7	2 1 3 4	19	4 1 2 3
8	2 1 4 3	20	4 1 3 2
9	2 3 1 4	21	4 2 1 3
10	2 3 4 1	22	4 2 3 1
11	2 4 1 3	23	4 3 1 2
12	2 4 3 1	24	4 3 2 1

Tabulka: Tabulka pořadí permutací čtyř prvků.

Příklad (pokračování)

Karty nyní dostane do ruky kouzelník.
Protože $r = 37 + 11 + 105 + 90 \equiv 2 + 1 + 0 + 0 = 3$,
tak ví, že $y \equiv -3 \pmod 5$.

Příklad (pokračování)

Karty nyní dostane do ruky kouzelník.
Protože $r = 37 + 11 + 105 + 90 \equiv 2 + 1 + 0 + 0 = 3$,
tak ví, že $y \equiv -3 \pmod 5$.

Protože permutace $37, 11, 105, 90$ určuje $k = 8$, tak již snadno určí

$$y = 5k - r = 5 \cdot 8 - 3 = 37.$$

Příklad (pokračování)

Karty nyní dostane do ruky kouzelník.
Protože $r = 37 + 11 + 105 + 90 \equiv 2 + 1 + 0 + 0 = 3$,
tak ví, že $y \equiv -3 \pmod 5$.

Protože permutace $37, 11, 105, 90$ určuje $k = 8$, tak již snadno určí

$$y = 5k - r = 5 \cdot 8 - 3 = 37.$$

Protože $11 \leq 37$ a $37 \leq 37 + 1$, tak třicátá sedmá chybějící karta je
$x = y + 2 = 37 + 2 = 39$.

Kouzelník nyní „uhodne“ (vypočítá) divákovu kartu 39.

Videa

Příklad 1 – vysvětlení

Příklad 2 – vysvětlení

Zobecnění

Co kdyby divák vybíral n karet (ne nutně 5)?

Zobecnění

Co kdyby divák vybíral n karet (ne nutně 5)?

n	karet nejvýše $n! + (n-1)$
2	3
3	8
4	27
5	124
6	725
7	5 046
8	40 327
9	362 888
10	3 628 809

Pozor!

Výpočty je nutno provádět v číselné soustavě $(\mathrm{mod}\ n)$.

Zatím jsme počítali modulo 5 což je snadné, počítat modulo 7 je těžší.

Zobecnění

Náměty na přemýšlení:
Jak se úloha změní, když

- kdybychom mohli rozlišit otočení karet?
  (u dvouhlavých karet není možné)

Zobecnění

Náměty na přemýšlení:
Jak se úloha změní, když

- kdybychom mohli rozlišit otočení karet?
  (u dvouhlavých karet není možné)
- Kdyby asistentka zbývající karty mohla vyložit postupně?
  (mohli bychom rozlišit pořadí, v jakém karty položí)

Zobecnění

Náměty na přemýšlení:
Jak se úloha změní, když

- kdybychom mohli rozlišit otočení karet?
  (u dvouhlavých karet není možné)
- Kdyby asistentka zbývající karty mohla vyložit postupně?
  (mohli bychom rozlišit pořadí, v jakém karty položí)
- Kdyby asistentka měla
  - dala vybrat nejprve pět karet jednomu divákovi
  - a z vybraných 5 karet si jednu vybere jiný divák?

Zobecnění

Náměty na přemýšlení:
Jak se úloha změní, když

- kdybychom mohli rozlišit otočení karet?
  (u dvouhlavých karet není možné)
- Kdyby asistentka zbývající karty mohla vyložit postupně?
  (mohli bychom rozlišit pořadí, v jakém karty položí)
- Kdyby asistentka měla
  - dala vybrat nejprve pět karet jednomu divákovi
  - a z vybraných 5 karet si jednu vybere jiný divák?
- kdyby asistentka divákovi vracela dvě karty?

Chcete to nyní vyzkoušet ještě jednou?

Chcete to nyní vyzkoušet ještě jednou?

Děkuji za pozornost.

(teď už doopravdy končím)