Diskrétní matematika (MA0002)

—

Kombinatorika: Základní kombinatorická pravidla.

—

Odvození kombinatorických vzorců:
Permutace, variace, kombinace bez opakování a s opakováním.

—

Faktoriály a kombinační čísla. Binomická věta.
Princip inkluze a exkluze a další kombinatorické lahůdky.

—

Konečné součty.

—

Dělitelnost celých čísel. Základní věta aritmetiky.

—

Dělitelnost polynomů. Hledání kořenů polynomu.
Dělení polynomu polynomem. Euklidův algoritmus.

—

Základy teorie grafů.

—

Studijní text PdF MU - verze ze dne 10. října 2023

Helena Durnová

Pracovní verze

Obsah

Předmluva

Motto:

„Nevyučuj toho, kdo není připraven, aby byl vyučován.“

(Jan Ámos Komenský)

Matematika provází všechny děti po celou základní školní docházku od 70. let 20. století pod tímto jménem a pod jmény jinými (počty a měřictví, či aritmetika a geometrie) ještě déle. Některé děti matematika prostě baví, některé ne, ale přesto se jí musí učit všechny, stejně jako třeba češtině či tělocviku.

V dnešní době se stalo módou chlubit se neznalostí matematiky, začněme tedy kacířskou otázkou: co by se stalo, kdybychom děti, které matematické poznatky přirozeně nechápou, povinnosti učit se matematiku zprostili? Odpovědět na ni dokážeme teprve tehdy, když si uvědomíme, jaké učitele matematiky jsme zažili a co od nás matematika vyžadovala.

Matematika se dá — s velkou nadsázkou — přirovnat ke sportu. Ani ve sportu není talent všechno; skoro u každého je potřeba trénink. Tak je tomu i s matematikou: během školní docházky se v matematice učíme postupům, které nám procvičováním přejdou do krve. A tak si při při písemném sčítání „sloupečků“ i v dospělosti pomáháme prsty. Pravda, příležitostí k využití této dovednosti máme díky přítomnosti kalkulačky ve všudypřítomných mobilních telefonech pramálo, ale když bylo vynalezeno auto, také jsme nepřestali chodit pěšky a jezdit na kole.

Ve výuce matematiky se často klade důraz na správný zápis, na to, aby byl výsledek dvakrát podtržen, na to, aby znaménko rovnosti bylo v úrovni hlavní zlomkové čáry složeného zlomku. Všechny tyto věci se zvenčí mohou zdát podružnými a nepodstatnými, ale právě tyto návyky nás učí odlišovat podstatné od nepodstatného: vezměme si jako příklad pomocné výpočty psané tužkou na okraj sešitu nebo dokonce na šmírák. Podobně důraz na úpravu a dodržování pravidel není samoúčelný, nýbrž nám samotným později ve složitějších výpočtech usnadní orientaci. Během hodin matematiky se tak cvičíme v disciplíně; například samotné numerické počítání asi baví málokoho, přesto je bezchybný numerický výpočet nutný pro dosažení správné odpovědi na otázku, kterou jsme si položili.

Význam matematiky pro studující bývá často přirovnáván k latině. V knize „Nebezpečí jednotné školy“ použil Rudolf Mertlík slova Zdeňka Nejedlého:

> Netajím se přesvědčením, že latina je velmi důležitý výchovný předmět. Vzpomínám-li na své vzdělání, které z předmětů mi

> vlastně co daly, byla to matematika (ačkoliv jsem historik) a latina. To jsou předměty, které jsou takovou dresurou přesného myšlení. Jen ten, kdo nezná latinský jazyk, může tvrdit, že je ho možno nahradit jiným živým jazykem. Žádná francčtina, angličtina ani jiná řeč nenahradí latinský jazyk. Není jazyka, který by měl takovou logickou konstrukci, jako má klasická latina.

Latina už se dnes povinně učí na málokterém gymnáziu. Roli pomyslného biče tak převzala matematika: všimněte si, že Nejedlý mluvil o „tréninku přesného myšlení“. Samozřejmě, že i v matematice můžeme být kreativní, ale současně musíme dodržovat jistá pravidla; podobně jako při hře v šachy. Přesnost, kterou skrze matematiku pěstujeme, však netkví v počtu desetinných míst výsledku.

Na závěr dovolte několik vět k předkládanému textu. Je věnován některým partiím z tzv. diskrétní matematiky, zde konkrétně z teorie čísel, kombinatoriky a teorie grafů a je koncipován spíše jako vodítko k Vaší orientaci. Všechny partie zde probírané byly již popsány v řadě knih, na něž se v textu odkazujeme. Nepochopíte-li vše hned, nezoufejte a mějte na paměti, že vše lze pochopit, vyvinete-li dostatečné úsilí. Matematika je také práce.

Část I

Spíše teoretická část

Značení a úmluvy

Matematická komunikace je založena na konvencích. (Henri Poincaré) Proto bude dobré, když si pro začátek některé pojmy a jejich značení sjednotíme. Pro úspěšné zvládnutí předmětu není vždy bezpodmínečně nutné veškeré zde uvedené konvence dodržet, ale můžete se sem vracet, bude-li v textu použito značení, kterému z jakéhokoliv důvodu nebudete rozumět.

Číselné obory

$\mathbb{N}$	přirozená čísla	$(1, 2, 3, \ldots$; nulu za přirozené číslo nepovažujeme)
$\mathbb{Z}$	celá čísla	$(\ldots$, -2, -1, 0, 1, 2, $\ldots)$
$\mathbb{Q}$	racionální čísla	čísla tvaru $\frac{p}{q}$, kde $p \in \mathbb{Z}$ a $q \in \mathbb{N}$
$\mathbb{R}$	reálná čísla	„lze vyjádřit jako délku úsečky“
$\mathbb{C}$	komplexní čísla	čísla tvaru $a + bi$, kde $a, b \in \mathbb{R}$ a pro i platí: $i^2 = -1$

Jak přistupovat k domácím úkolům

- Každý samostatný pokus o vyřešení úlohy je cenný.
- Pokud úlohu nedokážete vyřešit, zkuste pro sebe formulovat podobnou úlohu, kterou vyřešit dokážete.
- U důkazových úloh typu “dokažte, že pro všechna přirozená čísla platí $\ldots$” je vhodné zkusit, zda tvrzení platí pro nějaká malá přirozená čísla. Při dosazování konkrétních čísel příslušnou obecnou zákonitost často odhalíte.
- Všeobecně platí tato korelace: úprava výpočtů je přímo úměrná úrovni porozumění. To není překvapivé, neboť při řešení příkladů je třeba určité disciplíny. Zejména je třeba oddělovat, co je dáno, co je (všeobecně) známo a co je výsledek výpočtu.

Jak psát řešení příkladů

- čitelně (není třeba krasopisně) a tak, abyste po pěti letech sami věděli, jak jste příklad řešili;

- opticky oddělujme stěžejní a pomocné výpočty; pomocné výpočty můžeme např. psát tužkou, za okraj, atp.;
- zejména v kombinatorice svůj postup alespoň stručně, avšak výstižně, komentujeme;
- u kombinatorických příkladů lze výsledek ponechat ve tvaru faktoriálů či kombinačních čísel, není třeba dopočítávat na kalkulačce
- u důkazových úloh klademe důraz na přehlednost;
- Odpověď je nedílnou součástí řešení příkladu.

Důkaz jako prostředek komunikace v matematice

Dohodneme-li se na značení, shodneme-li se na definicích, dospějeme v matematice k těm samým výsledkům. V tomto procesu je důkaz prostředkem k přesvědčování druhých, avšak nikoli ve smyslu nátlaku. Důkaz nás nutí dělat menší krůčky, a proto nám může pomoci, chceme-li druhým ukazát to, co vidíme my.

František Kuřina: Matematika jako umění vidět
Pro inspiraci doporučuji texty Františka Kuřiny.

Některé detaily

- hvězdička (*) označuje náročnější příklad
- upozornění na překlepy (v textu i v zadání příkladů) vítám
- dotazy na správnost výsledků jednotlivých příkladů a cvičení také vítám.

Kapitola 1

Kombinatorika

Řada knih zabývajících se kombinatorikou a jejími počátky poukazuje na zálibu lidí v přeskupování a vytváření vzorů. Například Athanasius Kircher (1602–1680) v ní viděl největší umění a svou knihu věnovanou kombinatorice nazval „Ars Magna Sciendi, Sive Combinatoria (Velké umění vědy, čili kombinatorika)“. Kombinatorické úlohy jsou pro malé počty prvků zábavné a snadno řešitelné vypsáním všech možností. Při větším počtu však působí spíše magickým dojmem, protože není v našich silách představit si všechny možnosti, pročež musíme více důvěřovat korektnosti naší úvahy.

V moderním množinovém vyjádření můžeme stručně a jasně psát:

Věta 1.1 (Pravidlo součtu) Nechť A, B jsou disjunktní množiny (tj. množiny, které nemají žádný společný prvek, což symbolicky zapisujeme jako: $A \cap B = \emptyset$), počet prvků množiny A je $|A|$ a počet prvků množiny B je $|B|$. Pak $|A \cup B| = |A| + |B|$.

Příklad 1.2 Na otázku „kolika způsoby lze na šachovnici postavit pěšáka?“ lze odpovědět také rozdělením šachovnice na černá a bílá políčka. Pro variantu, jak postavit pěšáka na bílé políčko, máme 32 možností; pro variantu, kdy pěšák stojí na černém políčku, máme také 32 možností. Celkem je možností $64 = 32 + 32$ (stojí-li pěšák na černém políčku, nestojí na bílém, a naopak).

Věta 1.3 (Pravidlo součinu) Nechť A, B jsou neprázdné množiny, počet prvků množiny A označujeme $|A|$ a analogicky počet prvků množiny B je $|B|$. Pak $|A \times B| = |A| \cdot |B|$.

Příklad 1.4 Ptáme-li se, kolika způsoby můžeme postavit na šachovnici černou a bílou dámu tak, aby černá dáma stála na černém políčku a bílá na bílém, odpověď určíme jako $32 \cdot 32 = 1\ 024$

V následujícím příkladu zkombinujeme pravidlo součtu a součinu:

Příklad 1.5 Kolik různých slov lze získat přeházením písmen ve slově KOLENA tak, že se v nich samohlásky a souhlásky střídají a souhlásky jsou seřazeny abecedně?

Pokud jsou souhlásky na sudých pozicích a samohlásky na lichých, můžeme takto získat 6 slov ($6 = 3! = 3 \cdot 2 \cdot 1$) a stejně slov získáme i tehdy,

jsou-li souhlásky na lichých pozicích a samohlásky na sudých. V této části naší úvahy jsme použili jsme pravidlo součinu.

Celkem je možností $12 = 6 + 6$, neboť pokud jsou souhlásky na sudých místech, nejsou na lichých místech a naopak. Chceme-li formálně popsat tutot druhou úvahu, můžeme říkat, že jsme použili jsme pravidlo součtu.

Věta 1.6 (Přihrádkový, též zvaný Dirichletův, princip) Máme-li rozdělit $n + 1$ předmětů do n přihrádek, pak při libovolném rozdělení budou v alespoň jedné přihrádce alespoň dva předměty.

Příklad 1.7 V zásuvce je 12 párů červených a 12 párů modrých ponožek. Pokud bereme ponožky z přihrádky poslepu, kolik ponožek musíme vzít, abychom měli alespoň dvě ponožky téže barvy?

[Stačí vytáhnout tři ponožky.]

Všechny kombinatorické vzorce, které znáte ze střední školy, se dají odvodit pomocí pravidla součtu a pravidla součinu. Přihrádkový (Dirichletův) princip lze s výhodou použít při řešení některých příkladů.

Několik postřehů z historie kombinatoriky. Kombinatorická pravidla jsou tak jednoduchá a samozřejmá, že těžko můžeme očekávat, že bychom v historických pramenech našli zmínky o jejich přesné formulaci.[1] Zmínky o úlohách, které bychom dnes klasifikovali jako kombinatorické, nacházíme především v indických a čínských textech. První zmínky se však objevují již ve starověkém Egyptě, jak dokládá následující úloha z Rhindova papyru s poměrně nejasným zadáním. Obsahuje sloupec (viz též Obr. 1.1)

domy	7
kočky	49
myši	343
pšenice	2401
hekaty	6807
	19607

Podobné počty najdeme i u Fibonnacciho (Liber abaci, 1202) ve formě říkanky o sedmi starých ženách, které jdou do Říma:

Sedm starých žen šlo do Říma
každá nesla.....
Kolik....

Tyto počty se dochovaly i v dětské říkance „Když jsem šel do St. Ives“:

As I was going to St. Ives,
I met a man with seven wives.
Each wife had seven sacks.
In each sack there were seven cats.
Each cat had seven kits.
Kits, cats, sacks, and wives,
How many were going to St. Ives?

[1] Biggs, N. 1979. ‘Roots of combinatorics’. Historia Mathematica **6**:109-136.

R79

Majetek:

		domy	7
		kočky	49
1	2 801	myši	343
2	5 602	pšenice	2 301[sic]
4	11 204	ječmen	16 807
celkem	19 607	celkem	19 607

Obrázek 1.1: Úloha o majetku z Rhindova papyru. Převzato z knihy Vymazalová, Hana. Hieratické texty.

Možná byly doby, kdy takové počítání patřilo spíše k zábavě, ale i ta patří k matematice. Traduje se, že kombinatorické myšlení bylo pěstováno spíše v Indii než v Evropě. Známá je úloha o počtu možných kombinací z pětii chutí: slaná, sladká, hořká, pálivá a trpká. Výčtem všech možností dojdeme k počtu 31:

5 chutí - 1 možnost
4 chutě - 5 možností (vždy se jedna vynechá)
3 chutě - 10 možností (kombinace 3 z 5)
2 chutě - 10 možností (kombinace 2 z 5)
1 chuť - 5 možností
(buď sladká, nebo slaná, nebo hořká, nebo pálivá, nebo trpká)

Na této úloze může být zajímavé si povšimnout, že možnost „bez chuti“ se nepočítá; jinak se vlastně jedná o počet podmnožin pětiprvkové množiny, kterých je $2^5 = 32$. Vzhledem k tomu, že prázdná množina je jen jedna, skutečně stačí odečíst 1.

V Evropě se dostala kombinatorika do obecného povědomí nejpozději v 17. století v souvislosti s výpočtem počtu možností při hazardních hrách. Klasifikaci typů kombinatorických úloh na permutace, variace a kombinace v podstatě formuloval už švýcarský matematik Jacob Bernoulli (1654–1708).

1.1 Faktoriály a kombinační čísla. Kombinatorické identity.

V tomto oddíle stručně shrneme některé poznatky o faktoriálech a kombinačních číslech tak, abychom s nimi v dalším mohli počítat bez dalšího vysvětlování. Funkci faktoriál pro naše potřeby stačí definovat pouze pro přirozená čísla a nulu.

Definice 1.8 (Faktoriál přirozeného čísla) Pro libovolné $n \in \mathbb{N}$ klademe $n! = 1 \cdot 2 \cdot \cdots \cdot n$ (čteme: „n faktoriál“).

Dále klademe $0! = 1$.

Na okraj uveďme, že pojem faktoriálu lze rozšířit i mimo obor přirozených čísel.

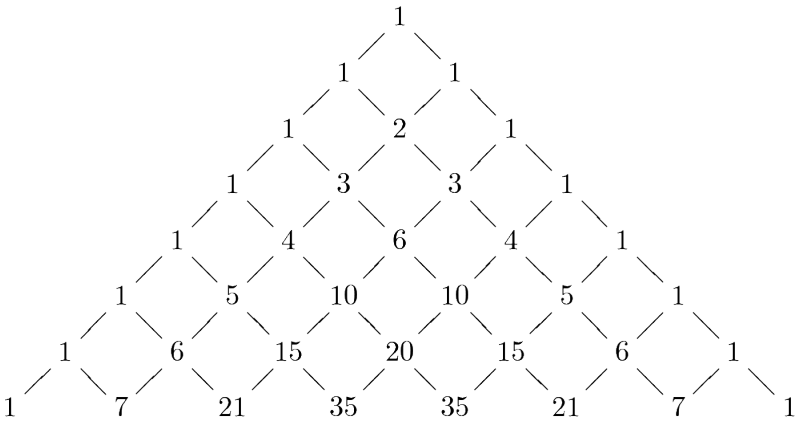
Tabulka hodnot faktoriálů pro $n = 1 \dots 10$**,** z níž je patrné, jak rychle tato funkce roste:

$0!$	1
$1!$	1
$2!$	2
$3!$	6
$4!$	24
$5!$	120
$6!$	720
$7!$	5 040
$8!$	40 320
$9!$	362 880
$10!$	3 628 800

Definice 1.9 (Kombinační číslo) Pro libovolná $k, n \in \mathbb{N}$ definujeme kombinační číslo (čteme: „n nad k“) takto:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Podobně jako pojem faktorál lze i i pojem kombinačního čísla rozšířit mimo obor přirozených čísel; v kombinatorice však vystačíme s kombinačními čísly, v nichž n i k budou přirozená čísla, pro něž navíc platí $0 \leq k\ n$. Hodnoty kombinačních čísel lze elegantně zapsat do trojúhelníku, v němž na obou ramenech jsou čísla 1 (n nad nulou stejně jako n nad n je vždy jedna) a v ostatních případech můžeme kombinační číslo určit jako součet dvou čísel, která leží na odpovídajících místech v o řádek výš, jak je naznačeno na Obr. 1.2.[2]



Obrázek 1.2: Řádky aritmetického trojúhelníka pro $n = 0 \dots 7$.

[2]Courtesy `artofproblemsolving.com`.

Počítání s faktoriály a kombinačními čísly: Jednodušší příklady lze řešit rozepsáním faktoriálů. Kombinační číslo $\binom{n}{k}$ představuje vlastně stručný zápis zlomku $\frac{n!}{k!(n-k)!}$, platí tedy: $\binom{n}{k} = \binom{n}{n-k}$.

Kombinatorické identity: pro kombinační čísla platí řada tzv. kombinatorických identit. Lze je dokázat jednak rozepsáním jednotlivých kombinačních čísel, jednak kombinatorickou úvahou. Nejznámější z nich je tato:

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Lze ji jednoduše ověřit rozepsáním kombinačních čísel. Také si můžeme uvědomit, že vybíráme-li např. tři osoby ze sedmi, je z početního hlediska jedno zda počítáme trojice těch, kteří nás budou reprezentovat, nebo naopak čtveřice těch, kteří "zůstanou doma".

Uveďme některé další typy jednoduchých příkladů na toto téma::

(a) Dokažte: $n! + (n-1)!n^2 = (n+1)!$ (Stačí na levé straně vytknout $n!$).

(b) Sečtěte: $\frac{(n+2)!}{n!} - 2\frac{(n+1)!}{(n-1)!} + \frac{n!}{(n-2)!}$ (Jednoduchých roznásobením dostáváme výsledek: 2).

(c) Vyjádřete jedním kombinačním číslem: $\binom{9}{4} + \binom{9}{6}$ $[=\binom{10}{6}]$; $\binom{11}{2} + \binom{11}{8}$ $[=\binom{12}{3}]$; $\binom{12}{5} + \binom{12}{6}$ $[=\binom{13}{6}]$.

Dále platí tyto jednoduché kombinatorické identity:

(i) $\binom{n}{k} = \binom{n}{n-k}$

(ii) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

(iii) $2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n}$

(iv) $0 = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^{n-1}\binom{n}{n-1} + (-1)^n\binom{n}{n}$

(v) $\binom{n-1}{0} + \binom{n}{1} + \binom{n+1}{2} + \cdots + \binom{n+m-1}{m} = +\binom{n+m}{m}$

(vi) $\binom{n}{n} + \binom{n+1}{n} + \binom{n+2}{n} + \cdots + \binom{n+m-1}{n} = +\binom{n+m}{m}$

(vii) $1 + 2 + \cdots + m = \frac{m(m+1)}{2}$

Jednoduchou úvahou z platnosti identity (iii) vyplývá platnost následujících identit pro sudé n:

(iii-a) $2^{n-1} = \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots + \binom{n}{n}$

(iii-b) $2^{n-1} = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots + \binom{n}{n-1}$

a analogicky pro liché n:

(iii-c) $2^{n-1} = \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots + \binom{n}{n-1}$

(iii-d) $2^{n-1} = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots + \binom{n}{n}$

Dále platí například:

(*viii) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + m \cdot (m+1) = \frac{m(m+1)(m+2)}{3}$

(*ix) $1 \cdot 2 \cdot 2 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 5 + \cdots + m \cdot (m+1) \cdot (m+2) = \frac{m(m+1)(m+2)(m+3)}{4}$

(*x) $\binom{n}{0}\binom{n}{m} - \binom{n}{1}\binom{n-1}{m-1} + \binom{n}{2}\binom{n-2}{m-2} + \cdots + (-1)^n \binom{m}{m}\binom{n-m}{0} = 0$

(*xi) $4^n = \binom{2n+1}{0} + \binom{2n+1}{1} + \binom{2n+1}{2} + \binom{2n+1}{3} + \cdots + \binom{2n+1}{n}$

Řada vztahů mezi kombinačními čísly je patrná z tzv. aritmetiického (Pascalova) trojúhelníka (viz Obr. 1.2). Například lze v aritmetickém trojúhelníku vidět, že je-li součet druhého řádku roven 4 (=1+2+1), pak součet třetího řádku je dvojnásobný, neboť každý sčítanec ze druhého řádku vstupuje do součtů na třetím řádku dvakrát. Z toho lze lehce odvodit, že součet čísel v daném řádku je 2^n, kde n je druhé číslo na daném řádku. Pro pořádek dodejme, že horní řádek má jediný prvek, totiž 1, což odpovídá 2^0.

Podobně se dá odvodit vztah $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ tak, že máme-li všechny k-prvkové kombinace z n prvků, můžeme je rozdělit na dvě (disjunktní) skupiny: prvky, které daný pevně zvolený prvek neobsahují (těch je $\binom{n-1}{k}$) a na ty, které jej obsahují (těch je $\binom{n-1}{k-1}$).

Rovnice s kombinačními čísly

Cvičení 1.10 Najděte všechna x, pro něž platí:

$$\binom{x-1}{x-3} + \binom{x-2}{x-4} = 9$$

[5]

Cvičení 1.11 Určete m, n, víte-li, že platí:

$$\binom{n+1}{m+1} = \binom{n+1}{m} = \frac{5}{3}\binom{m+1}{m-1}$$

$[n = 6, m = 3]$

1.2 Variace, permutace, kombinace.

V následujícím odvodíme pomocí pravidla součtu a součinu vzorce, které znáte ze střední školy pod názvy variace, permutace a kombinace (bez opakování a s opakováním). Postup vysvětlíme vždy na nějakém příkladu.

Variace bez opakování:

Příklad 1.12 Kolika způsoby lze na šachovnici rozestavit dámu, krále a věž?
Řešení: Opakovaným použitím pravidla součinu: $64 \cdot 63 \cdot 62 = 249\ 984$

Obecně pokud vybíráme k předmětů z celkového počtu n předmětů, přičemž $k, n \in \mathbb{N}$ a $k \leq n$, možností je

$$n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

Permutace bez opakování jsou zvláštním případem variací pro $n = k$. Někdy mluvíme také o „pořadí“.

Příklad 1.13 Kolika způsoby lze sestavit devítimístné číslo z cifer 1 až 9 takové, že se v něm cifry neopakují?

Řešení: Opakovaným použitím pravidla součinu: $9 \cdot 8 \cdot \cdots \cdot 1 = 362\ 880$

Obecně je počet pořadí n prvků roven $n!$ ($n \in \mathbb{N}$)

Příklad 1.14 Určete součet všech čtyřciferných čísel sestavených z cifer $1, 2, 3, 4$.

Řešení: $640 + 6400 + 64000 + 640000$ (číslice se mohou opakovat); $60 + 600 + 6000 + 60000$ (číslice se nemohou opakovat).

Kombinace bez opakování: uvědomíme si, že množství stejně početných variací a kombinací bez opakování prvků vybíraných ze stejně velké množiny spolu úzce souvisí. V podstatě stačí počet variací vhodným číslem vydělit; tímto vhodným číslem je faktoriál počtu vybíraných prvků; tj.

$$\frac{n!}{(n-k)!k!}$$

To je právě kombinační číslo:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Příklad 1.15 Kolika způsoby lze na šachovnici rozestavit tři bílé pěšáky?

Řešení: Vyjdeme z příkladu, kdy jsme na šachovnici měli postavit krále, dámu a věž; možností bylo $64 \cdot 63 \cdot 62 = 249\ 984$, Je zřejmé, že pokud na tři daná políčka postavíme tři pěšáky, je možnost jediná (pěšáci jsou stejní), zatímco krále, dámu a věž na tatáž políčka postavíme $3 \cdot 2 \cdot 1 = 6$ způsoby.

U variant „s opakováním“ začneme s odvozováním vzorců také u variací.

Variace s opakováním

Příklad 1.16 Do restaurace přijde 12 hostí. Na jídelním lístku jsou 4 jídla. Kolika způsoby si mohou objednat?

Řešení: Každý z hostů má 4 možnosti, tedy $4{\cdot}4{\cdot}4{\cdot}4{\cdot}4{\cdot}4{\cdot}4{\cdot}4{\cdot}4{\cdot}4{\cdot}4{\cdot}4 = 4^{12}$ možností.

Podobným způsobem lze odvodit počet podmnožin množiny A o n prvcích:

$$2^{|A|} = 2^n$$

Permutace s opakováním tentokrát nejsou zvláštním případem variací.

Příklad 1.17 Kolika způsoby můžeme přeskládat písmena slova

(a) TATA

(b) POPOCATEPETL

Řešení:

(a) Vypíšeme možnosti dle abecedy: AATT, ATTA, ATAT, TAAT, TATA, TTAA. To odpovídá permutacím všech čtyř písmen vyděleným permutacemi opakujících se písmen, tj. $\frac{4!}{2!2!}$

(b) Analogicky slovo POPOCATEPETL má 3 P, 2 O, 2 T, 2 E, 1 A, 1 C 1 L, tj. dohromady 12 písmen a možností přeházení je tedy $\frac{12!}{3!2!2!2!1!1!1!}$

Kombinace s opakováním vyžadují zvláštní přístup. Začneme „kódovat" a sestrojovat bijekce (vzájemně jednoznačná zobrazení) mezi objekty, jejichž počet máme spočítat, a objekty, jejichž počet budeme umět spočítat.

Příklad 1.18 Do restaurace přijde 12 hostí. Na jídelním lístku jsou 4 jídla. Kolika může být objednávek z hlediska kuchaře?

Řešení: Kuchaři je jedno, kdo si objednal které jídlo, zajímá ho pouze, kolik má připravit porcí jídla č. 1 až 4. Možností je $\binom{12+4-1}{4-1} = \binom{12+4-1}{12}$

Příklad 1.19 Kolika způsoby mohu vybrat deset mincí v hodnotě 5, 10 a 20 Kč? (Máme dostatečný počet mincí každé hodnoty.)

Řešení: Možností je $\binom{10+3-1}{3-1} = \binom{10+3-1}{10} = 66$

Oba výše uvedené případy můžeme „zakódovat" pomocí nul a jedniček. V příkladě s mincemi si například můžeme představit, že mince uspořádáme podle hodnoty: nejprve dvacetikoruny, pak desetikoruny a nakonec pětikoruny. Místo dvacetikorun napíšeme do řádku příslušný počet jedniček; za ně napíšeme nulu. Pokračujeme tak, že zapíšeme tolik jedniček, kolik je desetikorun; za ně opět napíšeme nulu. Nakonec napíšeme tolik jedniček, kolik je pětikorun. Je zřejmé, že psát za nimi nulu je nadbytečné: pokud hromádka dvaceti-, deseti- a pětikorun splňuje zadání a obsahuje deset mincí, napsali jsme posud deset jedniček a dvě nuly. Je zřejmé, že mezi hromádkami mincí a permutacemi deseti jedniček a dvou nul existuje vzájemně jednoznačné zobrazení, neboli vyhovujících hromádek je právě tolik, kolik je permutací deseti jedniček a dvou nul. Ty však již umíme spočítat: jedná se o předchozí výsledek, který jsme nazvali permutace s opakováním (deseti jedniček a dvou nul).

Výše uvedené odvození můžeme zopakovat při řešení jednotlivých příkladů; je to spolehlivější než snaha dosazovat naslepo do vzorečku pro kombinace s opakováním, kdy vybíráme k prvků n druhů:

$$C_o(k,n) = \binom{k+n-1}{n-1} = \binom{k+n-1}{k}$$

Vzoreček pro kombinace s opakováním, v němž přehodíme značení pro druhy a počet prvků ,a tedy vybíráme n prvků k druhů, totiž na první pohled vypadá dost podobně.

1.3 Další úlohy

Nyní si ukážeme několik zajímavých příkladů, u kterých vhodně využijeme výše uvedené vzorce a pravidla. Jsou převzaty z jiných učebnic, zejména z výborných skript Antonína Vrby ([4]).

Příklad 1.20 Kolika způsoby lze přeskládat písmena slova LOKOMOTIVA tak, aby žádná dvě „O“ nestála vedle sebe?

Řešení: Nejprve určíme, kolika způsoby lze přeskládat písmena L, K, M, T, I, V, A. To lze provést 7! způsoby. Při libovolném z těchto rozložení máme posloupnost sedmi písmen. Abychom vyhověli podmínkám, můžeme O vložit před nebo za tuto posloupnost nebo do mezer mezi písmeny, přičemž na každé z těchto míst lze vložit nejvýše jedno O. Taková místa můžeme vybrat $\binom{8}{3}$ způsoby. Možností je tedy $7!\binom{8}{3}$.

Příklad 1.21 Krotitel má do arény přivést 4 tygry a 5 lvů tak, aby žádní dva tygři nešli za sebou. Kolika způsoby to lze provést?

Řešení: Nejrpve určíme počet seřazení tygrů a lvů bez ohledu na to, který tygr a který lev kde konkrétně bude. Symbolicky můžeme napsat, že hledáme permutace pěti L a čtyř T takových, že žádná dvě T nenásledují těsně za sebou; například LTLTLTLTL. Takových rozmístění je $\binom{6}{4}$ (mezi pěti L jsou čtyři mezery, jedno místo je před prvním L a jedno za posledním; podobně jako v předchozím příkladu vyberem z těchto šesti míst čtyři místa, na něž umístíme T). V dalším kroku pak „dáme lvům a tygrům jména“, což početně znamená, že například místo uvedené permutace bezejmenných tygrů LTLTLTLTL dostáváme $5! \cdot 4!$ Celkem je tedy možností $5!\binom{6}{4} \cdot 4!$

1.4 Binomická věta

Věta 1.22 Nechť a, b jsou proměnné, $n \in \mathbb{N}$. Platí následující vztahy:

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b^1 + \cdots + \binom{n}{n-1}a^1b^{n-1} + \binom{n}{n}b^n$$

a analogicky

$$(a-b)^n = \binom{n}{0}a^n - \binom{n}{1}a^{n-1}b^1 + \cdots + (-1)^{n-1}\binom{n}{n}b^n$$

Příklad 1.23 Speciálními přiklady binomické věty jsou známé vzorce:

$$(a+b)^2 = \binom{2}{0}a^2 + \binom{2}{1}ab + \binom{2}{2}b^2$$

$$(a-b)^2 = \binom{2}{0}a^2 - \binom{2}{1}ab + \binom{2}{2}b^2$$

$$(a+b)^3 = \binom{3}{0}a^3 + \binom{3}{1}a^2b + \binom{3}{2}ab^2 + \binom{3}{3}b^3$$

$$(a-b)^3 = \binom{3}{0}a^3 - \binom{3}{1}a^2b + \binom{3}{2}ab^2 - \binom{3}{3}b^3$$

Se vzorci, které se opticky podobají binomické větě, se setkáte např. i v matematické analýze.

Binomické věty lze s výhodou užít například při těchto výpočtech:

(a) $101^5 = (100+1)^5 = 100^5 + 5\cdot 100^4 + 10\cdot 100^3 + 10\cdot 100^2 + 5\cdot 100 + 1$

(b) $99^5 = (100-1)^5 = 100^5 - 5\cdot 100^4 + 10\cdot 100^3 - 10\cdot 100^2 + 5\cdot 100 - 1$

V obou výše uvedených případech je výpočet jednodušší než přímo umocňovat 101 a 99.

Podobně lze umocňovat i komplexní čísla v algebraickém tvaru. Pro to, abychom mohli podobné příklady počítat, vystačíme se znalostí faktu, že každé komplexní číslo lze zapsat ve tvaru $a + bi$, přičemž platí $i^2 = -1$.[3]

Cvičení a úkoly k zamyšlení: binomická věta

Cvičení 1.24 Dokažte binomickou větu metodou matematické indukce.

Cvičení 1.25 Určete, který sčítanec je v binomickém rozvoji $\sqrt{2} + \sqrt{3}^{50}$ největší.

$[\binom{50}{22}\sqrt{2}^{22}\sqrt{3}^{28}]$

Jak na kombinatorické úlohy, pro které nelze přímo použít žádný ze šesti vzorců pro kombinace, variace a permutace bez opakování a s opakováním si ukážeme v následujících příkladech.

Příklad 1.26 Kolika způsoby lze ze šesti hochů a čtyř dívek vybrat šestičlenné družstvo na volejbal tak, aby v něm byla aspoň jedna dívka?
Řešení (a): Rozdělíme si možnosti podle toho, kolik dívek bude ve vybraném volejbalovém družstvu. Je zřejmé, že družstvo, ve kterém bude jedna dívka, nemůže být nikdy započítáno mezi družstvy, v nichž jsou dvě, tři nebo čtyři dívky. Využijeme tedy pravidla součtu a počty možností pro tyto čtyři případy spočítáme zvlášť.

Družstev s jednou dívkou je $\binom{4}{1}\cdot\binom{6}{5} = 4\cdot 6 = 24$
Družstev se dvěma dívkami je $\binom{4}{2}\cdot\binom{6}{4} = 6\cdot 15 = 90$
Družstev se třemi dívkami je $\binom{4}{3}\cdot\binom{6}{3} = 4\cdot 20 = 80$
Družstev se čtyřmi dívkami je $\binom{4}{4}\cdot\binom{6}{2} = 1\cdot 15 = 15$

Dohromady tedy $24 + 90 + 80 + 15 = 209$
Řešení (b): Jinou možností je spočítat všechny možnosti výběru družsva bez ohledu na počet dívek a potom odečíst počet družstev, v nichž není žádná dívka. Takové družstvo je jen jedno, tedy dostáváme
$\binom{10}{6} - \binom{6}{6} = 210 - 1 = 209$

V některých kombinatorických úlohách se výsledku dobereme tak, že nejprve vezmeme počet možností, který umíme dobře spočítat, i když víme, že tak zahrneme možností příliš mnoho; poté počet upravíme například odečtením nepříznivých případů nebo vydělením. Tyto postupy jsme už použili pro odvození vzorců pro kombinace (podělením příslušného počtu variací), pro permutace s opakováním (podělením celkového počtu permutací počty

[3] Pro ty, kteří se s komplexními čísly dosud nesetkali, lze doporučit např. knihu Emila Caldy Komplexní čísla z řady Matematika pro gymnázia nakladatelství Prometheus.

permutací opakujících se písmen), a tedy i pro odvození vzorce pro výpočet kombinací s opakováním. Ukažme si tuto strategii řešení na některých dalších příkladech.

Příklad 1.27 úprava výsledku dělením - př. č. 2

Příklad 1.28 úprava výsledku odečtením - př. č. 1

Příklad 1.29 úprava výsledku odečtením - př. č. 2

Příklad 1.30 úprava výsledku odečtením - př. č. 3

1.5 Princip inkluze a exkluze.

Někdy nedokážeme určit výsledek pouze pomocí jediné operace (přičtení, vynásobení, odečtení, vydělení). a například odečtení některých možností musíme opět nějaké možnosti přičíst, neboť víme, že jsme jich odečetli mnoho. Odečtení pak musíme opět dorovnat přičtením a tak dále, dokud je to potřeba. Systematickému použití přičítání a odečítání říkáme „princip inkuze a exkluze“. Nejjednodušším použitím principu inkluze a exkluze je vztah pro určení počtu prvků sjednocení dvou konečných množin:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Pro odvození vztahu pro určení počtu prvů sjednocení tří množin můžeme použít například Vennovy diagramy (viz Základy matematiky). Snadno nahlédneme, že

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|;$$

pro čtyři množiny:

$$\begin{gathered}|A \cup B \cup C \cup D| = \\ |A| + |B| + |C| + |D| \\ -|A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D| \\ +|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D|;\end{gathered}$$

pro pět množin:

$$\begin{gathered}|A \cup B \cup C \cup D \cup E| = \\ |A| + |B| + |C| + |D| + |E| \\ -|A \cap B| - |A \cap C| - |A \cap D| - |A \cap E| - |B \cap C| - |B \cap D| - |B \cap E| - |C \cap D| - |C \cap E| - |D \cap E| \\ +|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| \\ -|A \cap B \cap C \cap D| - |A \cap B \cap C \cap E| - |A \cap C \cap D \cap E| - |B \cap C \cap D \cap E| \\ +|A \cap B \cap C \cap D \cap E|\end{gathered}$$

atd., a tedy pro n množin lze formulovat

Obecný princip inkluze a exkluze:

$$|M_1 \cup M_2 \cup \cdots \cup M_n| =$$

$$|M_1| + |M_2| + \cdots + |M_n|$$
$$-|M_1 \cap M_2| - |M_1 \cap M_3| - \cdots - |M_1 \cap M_n|$$
$$-|M_2 \cap M_3| - \cdots - |M_2 \cap M_n| - |M_3 \cap M_4| - \cdot - |M_{n-1} \cap M_n|$$
$$+|M_1 \cap M_2 \cap M_3| + \cdots |M_{n-2} \cap M_{n-1} \cap M_n|$$
$$- \cdots + \cdots + (-1)^n |M_1 \cap M_2 \cap \cdots \cap M_n|$$

Příklad 1.31 (Eratosthenovo síto) Kolik je prvočísel mezi čísly od 1 do 100.

Můžeme si představit, že budeme postupovat jako prý postupoval Eratoshenes ve starověkém Řecku: na voskovou tabulku napíšeme čísla od 1 do 100 a horkou jehlou „propichujeme“ místa označená násobky prvočísel, tj. násobky 2: 4, 6, 8, 10, ... atd., násobky 3: 6, 9, 12, ... atd., násobky 5: 10, 15, 20, 25, ... atd. a násobky 7: 14, 21, ... atd.

Snadno nahlédneme, že některá čísla vypichujeme vícekrát, například 6, 10, 15, 30, ... atd. toho níže využijeme. Dále využijeme skutečnosti, že při zkoumání toho, zda je dané číslo n prvočíslo, stačí vyzkoušet dělitelnost prvočísly do hodnoty $\sqrt{n}$ (včetně). V našem případě hledáme prvočísla do 100, tedy stačí zkoumat děliletnost prvočísly 2, 3, 5 a 7.

Víme, že 1 není prvočíslo, tedy můžeme počítat s 99 čísly. Nejprve od 99 odečteme počet všech násobků 2, 3, 5 a 7 s výjimkou těchto prvočísel:

$$99 - 49 - 32 - 19 - 13 = 50 - 51 - 13 = -14$$

Výsledkem je záporné číslo, neboť např. číslo 6 jsme odečetli dvakrát: jednou jako násobek dvou, jednou jako násobek tří. Všechna tato nedopatření se pokusíme napravit naráz tím, že přičteme zpět násobky 6, 10, 14, 15, 21 a 35:

$$99 - 49 - 32 - 19 - 13 + 16 + 10 + 7 + 6 + 4 + 2 = 31$$

Teď již nemáme varování v podobě záporného výsledku, ale snadno nahlédneme, že jsme například 30 přičetli třikrát: v prvním kroku jsme 30 třikrát odečetli (jako násobek 2, 3 a 5) a nyní jsme je třikrát přičetli (jako násobek 6, 10 a 15). Číslo 30 ale není prvočíslo, je tedy třeba je (a jemu podobná čísla, např. 70) odečíst. Dalším pokusem o nápravu je tedy odečtení násobků trojic prvočísel, tj. 30, 42, 70 a 105:

$$99 - 49 - 32 - 19 - 13 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 = 25$$

Naši snahu by mohlo zhatit číslo, které by bylo dělitelné všemi čtyřmi prvočísly; nejmenší takové číslo však je 210, a tedy bychom přičetli 0 (tolik je mezi čísly od 1 do 100 násobků 210).

(Jen pro úplnost: v prvním kroku bychom je čtyřikrát odečetli, následně šestkrát přičetli a nakonec čtyřikrát odečetli; v součtu bychom je tedy odečetli dvakrát, přičemž jsme je chtěli odečíst pouze jedenkrát; to bychom napravili tím, že bychom je nyní ještě jedenkrát přičetli; nic takového však

dělat nemusíme, protože číslo 210 vůbec do hry nevstoupilo: počítali jsme stále pouze s přirozenými čísly menšími nebo rovnými 100.)

Pro pořádek odpověď: mezi čísly 1 až 100 je 25 prvočísel.

Příklad 1.32 (jazyky) V oddělení pracuje nekolik osob, z nichž každá zná alespoň jeden z těchto jazyků: ruština, španělština, italština. Rusky mluví šest osob, španělsky také šest osob, italsky sedm osob. Někteří hovoří více jazyky, konkrétně rusky a španělsky mluví čtyři osoby, španělsky a italsky tři osoby, rusky a italsky dvě osoby,. Jedna osoba dokonce ovládá všechny tři uvedené jazyky. Na základě těchto informací odpovězte na následující otázky:

(a) Kolik osob pracuje v oddělení?

(b) Kolik z nich mluví rusky, avšak ne španělsky ani italsky?

(c) Kolik z nich mluví španělsky, avšak ne rusky ani italsky?

[(a) 11; (b) 1; (c) 0]

Definujeme-li jednotlivé množiny pomocí vlastností, pak množina M_1 obsahuje prvky s vlastností 1, množina M_n prvky s vlastností i, analogicky $M_i \cap M_j$ prvky s vlastnostmi i a současně j, atd. Pak lze např. odvodit, že prvků, které nemají žádnou z požadovaných vlastností (přičemž prvky, které nemají vlastnost i označíme $M_1{}'$ a množinu obsahující všechny uvažované prvky označíme M), je

$$
\begin{aligned}
&|M_1{}' \cap M_2{}' \cap \cdots \cap M_n{}'| = \\
&|M| - |M_1| - |M_2| - \cdots - |M_n| \\
&+|M_1 \cap M_2| + |M_1 \cap M_3| + \cdots + |M_1 \cap M_n| \\
&+|M_2 \cap M_3| + \cdots + |M_2 \cap M_n| + |M_3 \cap M_4| + \cdot + |M_{n-1} \cap M_n| \\
&-|M_1 \cap M_2 \cap M_3| - \cdots |M_{n-2} \cap M_{n-1} \cap M_n| \\
&+ \cdots - \cdots + (-1)^n |M_1 \cap M_2 \cap \cdots \cap M_n|
\end{aligned}
$$

```
příklady:
lednička, auto, chata
znalost jazyků
kroužky
```

1.6 Speciální princip inkluze a exkluze

Úlohy, jejichž výpočet vede na tzv. speciální princip inkluze a exkluze, lze formulovat jako „problém šatnářky“ nebo „problém roztržité sekretářky“. Naším úkolem je určit, v kolika případech nedostane žádný pán svůj klobouk nebo v kolika případech se nedostane žádný dopis ke svému adresátovi. Počet možností zde nezávisí na konkrétní osobě, ale pouze na počtu osob, které nedostanou svůj klobouk nebo dopis.

Pro 4 osoby tedy dostáváme 9 možností:

$$4! - \binom{4}{1} \cdot 3! + \binom{4}{2} \cdot 2! - \binom{4}{3} \cdots 1! + \binom{4}{4} \cdot 0! = 24 - 24 + 12 - 4 + 1 = 9$$

Pro 5 osob pak 44 možností:

$$5! - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdots 2! + \binom{5}{4} \cdot 1! - \binom{5}{5} \cdot 0! = 120 - 120 + 60 - 20 + 5 - 1 = 44$$

Na speciální případ inkluze a exkluze pro pět vlastností vede následující úloha:

Příklad 1.33 Máme pět obálek s adresami (pro pět různých lidí) a pět dopisů. Kolika způsoby můžeme vložit dopisy do obálek tak, aby ani jeden dopis nebyl ve správné obálce?

Obecně: lze počet možností pro n vlastností podle speciálního principu inkluze a a exkluze spočítat takto:

$$n! - \binom{n}{1} \cdot (n-1)! + \binom{n}{2} \cdot (n-2)! - \cdots + (-1]^{n-1} \binom{n}{n-1} \cdot 1! - + (-1]^n \binom{n}{n} \cdot 0!$$

Cvičení 1.34 Na třídní schůzce informoval učitel rodiče takto:

„Naše třída má 30 žáků. Mohou chodit do 4 zájmových kroužků, z nichž každý probíhá jednou týdně. Pondělní kroužek navštěvuje 29 žáků, úterní 13, středeční 18 a čtvrteční 11. Žádný žák nenavštěvuje více než dva kroužky a žádné dva kroužky nemají více než 5 společných žáků. “

Určete, zda učitel mluvil pravdu

[Ne. Návod: použijte princip inkluze a exkluze a selský rozum.]

Cvičení 1.35 Kolika způsoby lze na šachovnici $n \times n$ rozestavit n věží tak, aby každé neobsazené pole šachovnice bylo ohrožováno nějakou věží?

[$2n^n - n!$ Návod: zkuste pro šachovnice o rozměrech $2 \times 2, 3 \times 3$, atd.]

1.7 Kompozice a rozklady.

Další kombinatorické kategorie. Kromě variací, permutací a kombinací známe další typické kombinatorické kategorie. Z nich si nyní představíme dva typy, a to počítání, kolika způsoby lze přirozené číslo zapsat ve tvaru sčítanců–přirozených čísel, a dále počítání, kolika způsoby můžeme věci (rozlišitelné nebo nerozlišitelné) rozdělit do přihrádek (rozlišitelných nebo nerozlišitelných)-

Úmluva: Pro účely tohoto textu rozumíme přirozenými čísly (a značíme $\mathbb{N}$) čísla $!1, 2, 3, \ldots$; jinými slovy, nulu za přirozené číslo nepovažujeme

S rozklady (přirozeného) čísla na (přirozené) sčítance se setkávají děti již v 1. třídě, kdy si ujasňují, že např. $5 = 4+1 = 2+3$. Pokud bychom vyjádření čísla 5 jako $1+4$ a jako $4+1$ považovali za navzájem různá, mluvili bychom z kombinatorického hlediska o „kompozicích“ (čísla 5 ze dvou sčítanců); pokud by pro nás tato vyjádření byla totožná, jednalo by se z kombinatorického hlediska o „rozklady“. Vdalším textu budeme o kompozicích a rozkladech mluvit ve smyslu níže uvedených definic. Ty nám říkají, že zatímco u rozkladů nezáleží na pořadí sčítanců, zatímco u kompozic ano. Rozdíl v počtu kompozic a rozkladů si můžeme ukázat na počtu rozkladů a kompozic čísla 4:

Rozkladů čísla 4 je 5:
$4 = 4 = 2 + 2 = 3 + 1 = 2 + 1 + 1 = 1 + 1 + 1 + 1$

Kompozic čísla 4 je 8:
$4 = 4 = 2 + 2 = 3 + 1 = 1 + 3 =$
$= 2 + 1 + 1 = 1 + 2 + 1 = 1 + 1 + 2 = 1 + 1 + 1 + 1$

Definice 1.36 (Kompozice) Kompozicí přirozeného čísla n z k sčítanců rozumíme každou uspořádanou k-tici přirozených čísel, pro niž platí ásledující vztah:

$$n = a_1 + a_2 + \ldots + a_k$$

Na základě předchozí definice formulujeme kombinatorickou úlohu: kolik je možných kompozic čísla n z k sčítanců?

Definice 1.37 (Rozklad) Rozkladem přirozeného čísla n na k sčítanců rozumíme každou nuspořádanou k-tici přirozených čísel, pro niž platí ásledující vztah:

$$n = a_1 + a_2 + \ldots + a_k$$

Analogicky jako u předchozího příkladu můžeme formulovat kombinatorickou úlohu: kolik je rozkladů čísla n na k sčítanců? Navíc se můžeme ptát, kolik je všech rozkladů — bez ohledu a počet sčítanců. Je zřejmé, že sčítanců může být nejméně 1 a nejvýše n.

Uveďmě jako příklad všechny rozklady čísla 10 na dva sčítance:
$10 = 5 + 5$
$10 = 4 + 6$
$10 = 3 + 7$
$10 = 2 + 8$
$10 = 1 + 9$

Zajímavosti k rozkladům a kompozicím
Ferrersovy diagramy
Adjungovaný rozklad
Samoadjungovaný rozklad
Uspořádání rozkladů

Cvičení 1.38 Vypište všechny kompozice čísla 10 ze čtyř sčítanců.

Cvičení 1.39 Vypište všechny kompozice čísla 10 z nejvíše 4 sčítanců.

Cvičení 1.40 Vypište všechny rozklady čísla 12 na 5 sčítanců.

Cvičení 1.41 Vypočtěte počty kompozic a rozkladů uvedených v přechozích příkladech pomocí vzorce pro výpočet počtu kompozic a rekurentního vzorce pro výpočet počtu rozkladů.

Cvičení 1.42 Vypište všechny rozklady čísla 12 na 3 sčítance takové, že každý ze sčítanců je roven nejvýše 6.

1.8 Rozdělování do přihrádek.

Část kombinatorických úloh se dá vhodně přeformulovat jako tzv. rozdělování předmětů (věcí) do přihrádek. Toto převedení si částečně ukážeme při odvozování příslušných vztahů;ty lze brátch prostě jako další nástroje k uchopení kombinatorické problematiky. U jednotlivých případů tedy budeme ptát, zda jsou přihrádky rozlišitelné (např. různě barevné krabice) nebo nerozlišitelné (např. stejné krabice) a zda jsou předměty rozlišitelné (např. různé knihy) nebo nerozlišitelné (stejné knihy). Na základě toho dostáváme čtyři situace, které si popíšeme níže. Ještě předtím si stručně připomeneme jednoduchý, ale účinný

Dirichletův (přihrádkový) princip: Při každém rozdělení n předmětů do k přihrádek, kde $k < n$, existuje alespoň jedna přihrádka obsahující alespoň dva předměty.

Příklad: Dokažte, že vyberem-li v obdélníku 6 cm $\times$ 4 cm libovolných 25 bodů, budou mezi nimi nejméně dva, jejichž vzdálenost je menší než $1,5$ cm.

Návod: Uvažujme body, jejichž souřadnice jsou celočíselné,

Příklad: Dokažte, že mezi sedmi různými přirozenými čísly jsou alespoň dvě taková, jejichž součet nebo rozdíl je dělitelný 10.

Návod: Rozdělte čísla do tříd podle dělitelnosti 10.

Rozdělování rozlišitelných předmětů do rozlišitelných přihrádek Nechť n, k jsou libovolná přirozená čísla. Pak lze n rozlišitelných předmětů rozdělit do k rozlišitelných přihrádek rozdělit právě k^n způsoby.

Rozdělování rozlišitelných předmětů do rozlišitelných přihrádek, přičemž žádná přihrádka nezůstane prázdná Nechť n, k jsou libovolná přirozená čísla, $n \geq k$. Pak lze n rozlišitelných předmětů do k rozlišitelných přihrádek tak, aby žádná přihrádka nezůstala prázdná, rozmístit právě

$$k!S(n,k) = \Sigma_{i=0}^{k}(-1)^i \binom{k}{i}(k-i)^n$$

způsoby.

Rozdělování nerozlišitelných předmětů do rozlišitelných přihrádek Nechť n, k jsou libovolná přirozená čísla,. Pak lze n nerozlišitelných předmětů do k rozlišitelných přihrádek rozdělit právě

$$\binom{n+k-1}{k-1}$$

způsoby.

Rozdělování nerozlišitelných předmětů do nerozlišitelných přihrádek, přičemž žádná přihrádka nezůstane prázdná Nechť n, k jsou libovolná přirozená 4ísla,. Pak lze n nerozlišitelných předmětů do k rozlišitelných přihrádek tak, aby v každé přihrádce bylo aspoň r předmetů, rozdělit právě

$$\binom{n-kr+k-1}{k-1}$$

způsoby; pro $r = 1$ je tento počet zřejmě

$$\binom{n-1}{k-1}.$$

Rozdělování rozlišitelných předmětů do nerozlišitelných přihrádek Nechť n, k jsou libovolná přirozená čísla,. Pak lze n rozlišitelných předmětů do k nerozlišitelných přihrádek rozdělit právě

$$S(n,1) + S(n,2) + \cdots + S(n,k)$$

způsoby. ($S(n,k)$ jsou tzv. Stirlingova čísla.)

Rozdělování nerozlišitelných předmětů do nerozlišitelných přihrádek Nechť n, k jsou libovolná přirozená čísla,. Pak lze n nerozlišitelných předmětů do k nerozlišitelných přihrádek rozdělit právě

$$p(n,1) + p(n,2) + \cdots + p(n,k)$$

způsoby; chceme-li, aby všechny přihrádky byly neprázdné, je tento počet

$$p(n,k).$$

1.9 Závěrem ke kombinatorice.

Dosud představené kombinatorické úlohy jsou samozřejmě pouhou „ochutnávkou“. Vůbec jsme se nedotkli problematiky magických či latinských čtverců, neformulovali jsme Kirkmanův problém 15 dívek, nedefinovali jsme Bellova či Stirlingova čísla. To je obsahem pokročilejších kurzů diskrétní matematiky. Zde probíraná látka představuje — kromě procvičení logického uvažování atp. — průpravu pro teorii pravděpodobnosti.

Kapitola 2

Rekurentní vztahy. Konečné součty.

Některé příklady nedokážeme vyřešit pomocí pravidla součtu a součinu – nedokážeme určit vzorec, do něhož bychom dosadili, a místo toho určujeme počet řešení na základě znalosti počtu řešení pro menší hodnoty parametru nebo parametrů. S tímto postupem jsme se již seznámili při určování počtu rozkladů čísel na sčítance. Ukážeme si ho také na následujícím příkladě:

Příklad 2.1 Kolika způsoby lze vyjít 10 schodů, děláme-li kroky po 1, 2, nebo 3 schodech?

Řešení: Poslední krok můžeme udělat ze 7., 8. nebo 9. schodu; tj.

$$S_{10} = S_9 + S_8 + S_7.$$

Obecně můžeme psát:

$$S_n = S_{n-1} + S_{n-2} + S_{n-3}.$$

Lehce ověříme, že

$$S_1 = 1, S_2 = 2, S_3 = 4,$$

a podle vzorce tedy dopočítáme

$$S_4 = 7 (= 1 + 2 + 4)$$

a analogicky

$$S_5 = 13, S_6 = 24, S_7 = 44, S_8 = 81, S_9 = 149,$$

a tedy

$$S_{10} = S_9 + S_8 + S_7 = 149 + 81 + 44 = 274.$$

Rekurentně lze definovat například funkci faktoriál: známe-li $n!$, pak $(n+1)!$ určíme jako $(n+1)!$ jako $(n+1)$ násobek předchozí hodnoty, tj. $n!$.

S rekurentní vztahy jste se mohli setkat na střední škole při studiu aritmetických a geometrických posloupností. Shrňme si, co o těchto posloupnostech víme.

Aritmetická posloupnost. Posloupnost daná rekurentním vztahem $a_n = a_{n-1} + d$ (a prvním členem), kde d nazýváme diferencí. U této posloupnosti umíme sečíst prvních n členů; vzorec:

$$S_n = (a_1 + a_n)\frac{n}{2} = \frac{n(2a_1 + (n-1)d)}{2}$$

Traduje se, že jednu z variant této úlohy vyřešil Karl Friedrich Gauss (1777–1855), když jako školák dostal za úkol sečíst čísla od 1 do 50 (někdy se tvrdí, že od 1 do 100). Všiml si, že součet 1 a 50 je stejný jako součet 2 a 49 a tak dále, tedy dvojnásobek hledaného součtu je $51 \cdot 50$.

Příklad 2.2 Určete součet:

$$S = 2n - 4 + 2n - 2 + 2n + \cdots + 4n.$$

Řešení: Jedná se o aritmetickou posloupnost s diferencí 2; její první člen je v našem částečném součtu $2n - 4$, poslední $4n$, diference 2. Abychom mohli použít výše uvedený vzorec, potřebujeme znát počet sčítanců, který však není n. Pro určení tohoto počtu můžeme použít úvahu: n sčítanců by bylo v součtu

$$S_n = (2n - 4) + (2n - 2) + (2n) + \cdots + (4n - 6),$$

čili scházejí tři sčítance, neboť

$$S - S_n = (4n - 4) + (4n - 2) + (4n)$$

Dosazením do výše uvedeného vzorce získáváme

$$S = (2n - 4 + 4n)\frac{n+3}{2} = (n-1)(n+3).$$

Rozmyslete si, že výsledkem zlomku bude pro posloupnost s celočíselnými členy vždy celé číslo.

Geometrická posloupnost. Posloupnost daná rekurentním vztahem $a_n = a_{n-1}q$ (a prvním členem), kde q nazýváme kvocientem. U této posloupnosti umíme sečíst prvních n členů; vzorec:

$$S_n = a_1\frac{1 - q^n}{1 - q} = a_1(1 + q + q^2 + \cdots + q^{n-1})$$

Je tedy vidět, že posloupnost je určena svým prvním členem a rekurentním vztahem.

Obecně platí, že každá rekurentní posloupnost je určena rekurentním vztahem a prvními několika členy — tolika, kolik jich explicitně nebo implicitně vystupuje v rekurentním vztahu.

Fibonacciho posloupnost patří mezi zajímavé posloupnosti Platí v ní, že každý další člen lze určit jako součet dvou členů předchozích. Zpr: $f_1 = 1, f_2 = 1, f_n = f_{n-1} + f_{n-2}$; první členy: $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$. Z rekurentního vztahu umíme v některých případech určit i tzv. vzorec pro n-tý člen, tj. návod, jak vypočítat f_n jen pomocí n.

Kapitola 3

Základy elementární teorie čísel

Elementární teorie čísel se zabývá dělitelností v oboru celých čísel ($\mathbb{Z}$) nebo v oboru přirozených čísel ($\mathbb{N}$). Základními pojmy jsou prvočíslo, číslo složené„ společný dělitel a společný násobek. Můžeme sem také zařadit také pojmy jako sudé a liché číslo (slovensky ‘párne a nepárne), trojúhelníkové číslo, čtvercové číslo, číslo dokonalé, spřátelená čísla, prvočíselná dvojčata a podobně.

`Co se tím myslí?`

`OBRÁZKY`

Jakýmsi základním problémem je nalezení řešení rovnice $ax = b$ v oboru celých čísel, tzn. zajímají nás pouze celočíselná řešení. Celočíselným řešením rovnice $2x = 3$ není (pochopitelně) číslo $1,5$; tedy daná rovnice nemá řešení v boru celých čísel, ale v oboru racionálních (reálných, komplexních ...) čísel samozřejmě ano.

V zápalu řešení rovnici někdy zapomínáme, v jakém oboru jsme ji měli řešit. Proč vůbec omezovat výsledky dělení na celočíselné, když si např. dokážeme představit, že koláč lze rozdělit na sedm dílů? Například proto, že praktické provedení (rozkrájení koláče na sedm stejných nebo dokonce i jen stejně velkých kousků) není úplně jednoduché.Podobně asi nelze dost dobře rozdělit na sedminy plod lesní jahody nebo třeba knihy. Rozlišujme tedy mezi dělitelností, která se týká výhradně celých čísel, a operací dělení, která probíhá v tom oboru, který si zvolíme. Formální definice dělitelnosti vypadá následovně:

Definice 3.1 *Nechť a, b jsou celá čísla. Říkáme, že číslo a je dělitelné číslem b právě tehdy, když existuje celé číslo q takové, že platí $a = bq$. Číslo a nazýváme q-násobkem (nebo jen násobkem) čísla b.*

Lehce nahlédneme, že platí následující tvrzení:

Věta 3.2 (Základní postřehy) Pro libovolná $a, b, c \in \mathbb{Z}$ platí:

(a) Pokud a dělí b a současně b dělí c, pak také a dělí c.

(b) Pokud a dělí b a současně a dělí c, pak a dělí rozdíl $b - c$.

(c) Pro nenulová c platí: a dělí b právě tehdy když ac dělí bc.

(d) Pokud a dělí b a b je kladné, pak a je menší nebo rovno b.

Tato tvrzení lze dokázat například tak, že si zapíšeme b jako k-násobek a a analogicky c zapíšeme jako m-násobek b, kde k a m jsou vhodná celá čísla. Tvrzení (b) je základem postupu zvaného „Eukleidův algoritmus“ (viz dále).

Dále platí věta:

Věta 3.3 (O dělení se zbytkem) Pro libovolné celé číslo a a přirozené číslo m existují právě jedno celé číslo q a právě jedno číslo r z množiny čísel $\{0, 1, ...(m-1)\}$ taková, že platí: $a = mq + r$.

Zápis čísla pomocí věty o dělení se zbytkem. Předchozí větu lze dobře využít k tomu, abychom mohli odpovědět na otázky:

- Jaký zbytek po dělení dávají mocniny čísla, které po dělení šesti dává zbytek 1?
- Jaký zbytek po dělení dávají mocniny čísla, které po dělení šesti dává zbytek 5?
- Ukažte, že součin tří po sobě jdoucích čísel je vždy dělitelný třemi.
- ...

3.1 Znaky dělitelnosti (známe často ze ZŠ)

Všechna pravidla uváděná ve školské matematice jsou založena na zápisu čísel v desítkové soustavě poziční soustavě. Tento způsob zápisu čísel se dnes děti učí v první třídě ZŠ. Používáme při něm deset cifer (0, ..., 9) a jejich význam souvisí s místem, které v číselném zápisu zaujímají: tak 910 je jiné číslo než např. 109. Jednotlivé cifry stojí na místě (zprava doleva) jednotek, desítek, stovek, tisíců atd.

Zápis čísla v poziční desítkové soustavě. Čísla můžeme zapisovat různými způsoby. Podíváme-li se do historie, najdeme tzv. pozicční i tzv. nepoziční systémy, systémy se základem 10 (starověký Egypt), 20 (Mayové) nebo 60 (Mezopotámie), systémy, které k vyjádření číslic používají písmena (starověké Řecko), číslice .

`formální zápis:`

```
a(n)-a(n-1)-\ldots - a(1) - a(0) =
a x (10 na n) + \ldots + a(1) x 10 + a(0)
```

Shrňme nyní některé poznatky o dělitelnosti, které znáte ze základní a střední školy:

- **dělitelnost 10, 5, 2** určíme podle poslední cifry.
- **dělitelnost 4, resp. 8** určíme podle toho, zda je poslední dvojčíslí dělitelné 4, resp. poslední trojčíslí 8.
- **dělitelnost 3 a 9** určíme pomocí ciferného součtu.

Důkaz pravidla dělitelnosti 3 a 9 (v desítkové poziční soustavě):

V desítkové soustavě zapíšeme číslo obecně takto:

$$a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0$$

Je zřejmé, že $10a_1 = 9a_{n-1}1a_{n-1}$, kde $9a_{n-1}$ je dělitelné 9, zatímco o a_1 to nevíme. Analogicky se dají rozepsat ostatní členy na násobky devíti a dané cifry, např. $10^2 a_2 = 99a_2 + a_2$. Potom tedy každé číslo můžeme rozepsat takto:

$$a_n \cdot 99\ldots9 + a_{n-1} \cdot 99\ldots9 + \cdots + a_2 \cdot 99 + a_1 \cdot 9 + a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0$$

Odtud je přímo vidět, že

$$a_n \cdot 99\ldots9 + a_{n-1} \cdot 99\ldots9 + \cdots + a_2 \cdot 99 + a_1 \cdot 9$$

a o dělitelnosti 3, resp. 9, rozhoduje dělitelnost ciferného součtu 3, resp. 9. Abychom zjistili, zda je dané číslo dělitelné třemi nebo devíti, stačí zkoumat dělitelnost příslušného ciferného součtu.

$$a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0.$$

Tento postup můžeme opakovat, dokud nedostaneme číslo, o jehož dělitelnosti třemi či devíti dokážeme rozhodnout na základě znalosti násobilky. Nejpozději může proces skončit v okamžiku, kdy dostaneme jednociferný výsledek.

Jako cvičení dokažte pravidla o dělitelnosti výše uvedená (10, 5, 2, 4 a 8)

Pro zajímavost uvedeme pravidla pro určení toho, zda je dané číslo dělitelné 7 nebo 11.

Dělitelnost 7 lze určit např. takto: (Eva Davidová, Wichterlovo g., Ostrava-Poruba)

(a) rozdíl součtu čísel vzniklých ze „sudých“ a „lichých“ trojic cifer je dělítelný 7;

(b) je-li 7 dělitelný součet násobků číslic daného čísla „odzadu“ postupně čísly 1, 2, 3, 4, 5, 6, 1, 2, ... (atd., periodicky se opakuje), pak je číslo dělitelné 7.

(c) rozdíl dvou čísel, z nichž první je tvořeno číslicemi daného čísla vyjma poslední a druhé je dvojnásobkem poslední číslice, je dělitelný 7 (periodicky opakujeme, podobně jako když používáme kritérium pro dělitelnost 3 a 9).

```
Používá se pro čísla letenek nebo čísla zakázek, odhalí 94 procent nesrovnalostí
k tomu slouží teorie kódování --- na konci čísla zakázky nebo letenky bývá
tzv. kontrolní číslice --- rozmyslete si, že stačí jedna číslice.
```

Proč to platí?

```
např. (c)
n=10a +b
je-li a - 2b dělitelné 7, pak
existuje m přirozené: a-2b=7m
Pak a = 7m + 2b, tedy 10a=70m+20b

jelikož n = 10a+b (předpoklad), pak 10a=n-b
ale je-li a-2b=7m, pak také 10a= 70m +20b

dohromady: n-b=70m+20b, tedy n=70m+21b = 7(10m+3b)
tedy n je dělitelné 7
```

Po přečtení výše uvedených pravidel vzniká otázka, zda není rychlejší dané číslo sedmi vydělit. U dělitelnosti 11 vypadají pravidla na první pohled schůdněji:

Dělitelnost 11 lze určit třemi způsoby:

(a) rozdíl součtu číslic na sudých a lichých místech je dělitelný 11;

(b) součet jednotlivých dvojčíslí je dělitelný 11;

(c) rozklad trojčíslí na sudých a lichých místech dělitelný 11.

```
K zamyšlení:
Rozmyslete si, odkud se počítají trojčíslí, ev. dvojčíslí.
Nebo je to jedno?
```

Kontrola dělitelnosti 11 se používá jako kontrolní znak pro rodná čísla nebo čísla účtů. U rodných čísel je prvních šest cifer určeno pohlavím a datem narození, další dvě číslice bývaly kódem pro místo narození a poslední dvě číslice byly kontrolní — byly doplněny tak, aby výsledek byl dělitelný 11.

Je evidentní, že výše uvedená pravidla nelze používat, pracujeme-li se zápisem čísla v jiné než naší běžné, tedy desítkové poziční, soustavě.

Dělitelnost 6, 15, a dalšími složenými čísly můžeme zkoumat na základě dělitelnosti nesoudělnými čísly.

3.2 Prvočísla a čísla složená. Základní věta aritmetiky.

Pojmy prvočíslo a číslo složené znáte patrně již ze základní školy. Pro naše účely budeme používat následující definici, která může, ale nemusí, odpovídat domu, jak jste si prvočísla definovali na základní či střední škole. Budeme se držet dohody (konvence), že číslo 1 není prvočíslem (ale ani číslem složeným).

Definice 3.4 (Prvočíslo) Nechť p je přirozené číslo. Říkáme, že p je prvočíslo, právě tehdy, když má p dva různé přirozené dělitele.

```
číslo složené - více než dva různí kladní dělitelé
zvláštní případ - číslo 1

Samozřejmě pokud a dělí b, pak také a dělí -b; -a dělí b; -a dělí -b
triviální dělitelé: čísla 1 a -1

0 má nekonečně mnoho děliteů
ale nulou nelze dělit

říkat, že nula dělí pouze nulu může být matoucí,
ale podle definice je to tak:
pokud 0=km,
pak je  k = 0 nebo je m=0

(Poznámka: spojka "nebo" je zde využita tak, jak jste
se s ní seznámili ve výrokové logice, např. v předmětu
Základy matematiky: může nastat i situace, kdy k=0=m)

Tohoto tvrzení využíváme např. hledáme-li body na ose x,
v nichž daná funkce vyjádřená polynomem nabývá hodnoty 0
```

Přinejmenším intuitivně znáte následující tvrzení:[1]

Věta 3.5 (Základní věta aritmetiky) Každé přirození číslo lze jednoznačně vyjádřit ve tvaru součinu mocnin prvočísel.

Definice 3.6 (Největší společný dělitel) Nechť a, b jsou celá čísla. Celé číslo m, pro něž platí, že m dělí a i že m dělí b, se nazývá společným dělitelem těchto dvou čísel. Kladný společný dělitel čísel a, b, který je dělitelný libovolným společným dělitelem těchto dvou čísel, se nazývá jejich největším společným dělitelem.

Analogicky lze definovat nejmenší společný násobek dvou čísel:

Definice 3.7 (Nejmenší společný násobek) Nechť a, b jsou celá čísla. Celé číslo m, pro něž platí, že m je násobkem a i že m je násobkem b, se nazývá společným násobkem těchto dvou čísel. Kladný společný násobek čísel a, b, který je dělitelem libovolného společného násobku těchto dvou čísel, se nazývá jejich nejmenším společným násobkem.

Známe-li největšího společného dělitele, můžeme nejmenšího společného dělitele určit pomocí následující vět:

Věta 3.8 (Nejmenší společný násobek) `PODMÍNKY`

$$nsn(a,b) = \frac{(axb)}{NSD(a,b)}$$

[1] Je-li základní vět aritmetiky formulována takto, potřebujeme, aby 1 nebylo prvočíslo. Na druhou stranu, kdyby 1 byla považována za prvočíslo, jistě bychom si s definicí poradili; například tak, že bychom do ní zahrnuli podmínku, že žádně z prvočísel použitých v rozkladu nesmí být rovno 1. Jinými slovy, to, že 1 nepovažujeme za prvočíslo, je „konvence.“

Nesoudělná čísla

```
Dvě čísla jsou nesoudělná, pokud
jejich největším společným dělitelem je 1.
NSD (a, b) = 1

Největší společný násobek dvou
nesoudělných čísel je jejich součin, tj.
nsn (a, b) = a x b
```

3.3 Kongruence

Věta o dělení se zbytkem nám dává tušit, že je možné rozdělit všechny celá čísla podle toho, jaký zbytek dávají po dělení jistým číslem m. Toto je speciální případ relace zvané ekvivalence, která je na dané množině reflexivní, symetrická a tranzitivní. Taková relace indukuje na množině tzv. rozklad na tzv. třídy; v našem případě se bude jednat o zbytkové třídy (modulo m).

Uveďme jako příklad zbytokové třídy modulo 5:

(0) ..., - 10, -5, 0, 5, 10, ...

(1) ..., -9, -4, 1, 6, 11, ...

(2) ..., -8, -3, 2, 7, 12, ...

(3) ..., -7, -2, 3, 8, 13, ...

(4) ..., -6, -1, 4, 9, 14, ...

* * * * *

Uveďme (zatím bez důkazu) následující tvrzení:

Věta 3.9 (Bezoutova) Pro libovolná celá čísla a, b existují celá čísla x, y taková, že $NSD(a, b) = ax + by$.

Pak také platí, jakékoliv celé číslo tvaru $ax + by$ je násobkem d.

Než Bezoutovu větu dokážeme, uvedem si postup známý jako „Eukleidův algoritmus“.

```
x x x x
```

3.4 Diofantické rovnice a Eukleidův algoritmus

Obecně jsou jako diofantické (diofantovské) rovnice označovány všechny rovnice (libovolného stupně a s libovolným počtem neznámých), které mají celočíselné koeficienty a pro které mají význam jen celočíselná řešení. Takovou rovnicí je tak i Pythagorova věta

$$x^2 + y^2 = z^2,$$

pokud hledáme pouze celočíselná řešení. Takovými řešeními jsou například pythagorejské trojice$x = 3, y = 4, z = 5$ nebo $x = 5, y = 12, z = 13$.

Diofantické rovnice lze nalézt v různých starších sbírkách úloh, např. v této úloze ze sbírky „Úlohy k bystření mladíků“ Alcuina z Yorku, tj. z doby kolem roku 800 našeho letopočtu:

Úloha o kupci kupujícím sto zvířat (Alcuin, Propositiones, č. 38): Nějaký muž chtěl koupit sto zvířat za sto zlatých, přičemž kůň se kupuje za třii zlaté, kráva za jeden zlatý a 24 ovcí za jeden zlatý. Řekni, kdo jsi s to, kolik bylo koní, kolik krav a kolik ovcí.
Řešení: sestavíme dvě rovnice o třech neznámých, v nichž x bude představovat počet koní, y počet krav a z počet ovcí.

$$\begin{aligned} x + y + z &= 100 \\ 3x + y + \frac{z}{24} &= 100 \end{aligned}$$

Druhou rovnici vynásobíme 24 a první číslem -1

$$\begin{aligned} -x - y - z &= -100 \\ 72x + 24y + z &= 2400 \end{aligned}$$

Obě rovnice sečteme a dostáváme rovnici

$$71x + 23y = 2300,$$

z níž po vydělení číslem 23 získáváme rovnici

$$\frac{71}{23}x + y = 100,$$

která bude mít celočíselné řešení pouze tehdy, bude-li x násobkem 23. Pak zřejmě $y = 100 - \frac{71}{23}x$. Dosadíme-li $x = 23$, vypočtem $y = 29$; odtud $z = 48$. Dosaddíme-li za x další násobek 23, tedy 46, vyjde y záporné, což nevyhovuje zadání příkladu. Jedinou možností nákupu zvířat je tedy koupě 23 koní (69 zlatých), 29 krav (29 zlatých) a 48 ovcí (2 zlaté).

Nyní uvedeme postup řešení nejjednodušší netriviální diofantovské rovnice (jednodušší je jen lineární rovnice o jedné neznámé, tj. rovnice tvaru $ax = b$, u níž je podmínka řešitelnosti v oboru celých čísel zřejmá: číslo b musí být násobkem čísla a.

Lineární diofantovskou rovnicí o dvou neznámých nazveme rovnici tvaru $ax + by = c$, kde a, b, c jsou celá čísla a hledáme pouze celočíselná řešení ($x, z \in \mathbb{Z}$, ne nutně kladná). Zda má tato rovnice řešení lze zjistt pomocí následující věty:

Věta 3.10 Lineární diofantovská rovnice $ax + by = c$ ($a, b, c \in \mathbb{Z}$) má alespoň jedno (celočíselné) řešení právě tehdy, když c je násobkem největšího společného dělitele čísel a, b.

Poznámka: Předchozí věta má tvar ekvivalence $A \Leftrightarrow B$, můžeme tedy říci, že B je nutnou a také dostatečnou podmínkou pro A (tedy řešitelnost diofantovské rovnice). V předmětu Základy matematiky jste si řekli, že obecně v implikaci $A \Rightarrow B$ platí, že B je nutnou podmínkou pro A. Platnost této implikace („zleva doprava“) je zřejmá, totiž rovnice $ax + by = c$ nemůže mít řešení v oboru celých čísel, pokud pravá strana není násobkem největšího společného dělitele čísel a a b.

Pokud platí i opačná implikace, tj. $B \Rightarrow A$, tedy pokud z toho, že pravá strana rovnice je násobkem největšího společného dělitele čísel a a b, přímo plyne existence celočíselného řešení rovnice, nazýváme B podmínkou dostatečnou; dohromady potom jde o podmínku nutnou a dostatečnou.

Uveďme nyní příklad diofantovské rovnice a postupu nalezení jejích řešení.

Příklad 3.11 Řešte v oboru celých čísel rovnice

(a) $2x + 3y = 1$

(b) $x + 3y = 4$

(c) $3x + 11y = 28$

Řešení: Nějaké řešení dokážeme ve všech případech odhadnout:

(a) $x = -1,\ y = 1$ nebo $x = 2\ y = -1$

(b) $x = 1,\ y = 1$ nebo $x = 7\ y = -1$

(c) $x = 2\ y = 2$ nebo $x = 13\ y = -1$

Co mají tato řešení společného a jak najdeme všechna? To ukážeme za chvíli.

Poznámka: Důkaz následující věty podává návod, jak najít největšího společného dělitele dvou čísel.[2]

Větu 3.10 můžeme přeformulovat pro libovolný počet nesoudělných neznámých. Je-li totiž pravá i levá strana rovnice dělitelná největším společným dělitelem koeficientů na levé straně, pak můžeme tímto číslem vydělit pravou i levou stranu.

Věta 3.12 Lineární diofantovská rovnice

$$a_1x_1 + a_2x_2 + \cdots a_nx_n = c,$$

kde $a_i \in \mathbb{Z}$ a největší společný dělitel koeficientů a_i je roven 1, má vždy celočíselné řešení. Všechna celočíselná řešení této rovnice lze popsat pomocí $n - 1$ celočíselných parametrů.

`zopakujte si, co víte z kongruencích`
`z předmětu Základy matematiky`

[2]Pro zajímavost: **z hlediska filosofie matematiky** můžeme rozlišovat mezi důkazy existence a důkazy pomocí pomocí konstrukce daného objektu (v tomto případě jde o nalezení největšího společného dělitele). Eukleidův algoritmus dává návod, jak nalézt největšího společného dělitele, a tím dává i důkaz o jeho existenci pro ibovolná dvě celá čísla; naopak to neplatí: je-li nám známo, že jistý objekt existuje, neznamená to, že jej umíme najít.

Důkaz: K důkazu této věty využijeme vlastnostni zvané kongruence, tj. vyjádření, že dva výrazy dávají stejný zbytek po dělení daným číslem (tzv. modulem). Připomeňmě, že zápis $a \equiv b(\mod m)$ čteme „a je kongruentní s b modulo m“.

Při důkazu budeme postupovat matematickou indukcí vzhledem k počtu neznámých. Pro jednu neznámou dostáváme rovnici $a_1 x = 1$. Podmínka NSD(a) = 1 znamená, že a_1 může nabývat hodnot 1 nebo -1.Pro každou z těchto hodnot má rovnice jediné řešení, které nezavisí na žádném parametru (ve shodě s tvrzením věty, neboť (n-1)=(1-1)=0).

Předpokládáme tedy, že počet neznámých v rovnici je alespoň 2 ($n \geq 2$). Potom pro libovolné řešení musí platit:

$$a_1 x_1 + a_2 x_2 + \cdots a_n x_n \equiv c(\mod d),$$

kde d je největší společný dělitel koeficientů $a_1, a_2, \ldots, a_{n-1}$. Musí tedy platit také kongruence

$$a_n x_n \equiv c(\mod d)$$

(od levé strany kongruence jsme odečetli násobek čísla d, tedy zbytek po dělení pravé a levé strany číslem d se nezměnil). Podle předpokldau jsou čísla a_n a d nesoudělná, tedy platí:

$$x_n = k + d \cdot t,$$

kde k je vhodné celé číslo a t je libovolné celé číslo. Tím je důkaz hotov, neboť rovnice s $(n-1)$ neznámými má podle předpokladu řešení závislé na $(n-2)$ parametrech, a my jsme právě vyjádřili n-tou neznámou s pomocí parametru t, tedy máme všechna řešení dané rovnice vyjádřena pomocí $(n-1)$ parametrů.

Postup nyní ukážeme na konkrétním příkladu:

Příklad 3.13 Řešte v oboru celých čísel rovnici

(d) $3x + 7y = 2$

Řešení: Podle předchozí věty musí platit:

$$3x + 7y \equiv 2(\mod 3),$$

tedy $7y \equiv 2(\mod 3)$.
Dalšími úpravami získáváme: $y \equiv 2(\mod 3)$, a tedy $y = 2 + 3t$ (slovně vyjádříme: y dává po dělení třemi zbytek 2).
Dosadíme do původní rovnice:

$$3x + 7(2 + 3t) = 2$$

a odtud

$$3x = 2 - 14 - 21t = -12 - 21t,$$

tedy

$$x = 4 - 7t.$$

Řešením rovnice jsou všchny dvojice celých čísel tvaru $[4 - 7t; 2 + 3t]$, kde t je libovolné celé číslo.

Postup zvaný Eukleidův algoritmus se používá k hledání největšího společného dělitele dvou čísel. Využíváme při něm (zřejmého?!?) k tvrzení z předchozího odstavce:

(b) Pokud a dělí b a současně a dělí c, pak a dělí rozdíl b-c.

Je výpočetně jednodušší než hledání NSD pomocí rozkladu čísla na prvočísla, o jejichž existenci jsme se v rámci tohoto textu dosud nezmínili. Pro výpočet NSD pomocí Eukleidova algoritmu tento pojem ani nepotřebujeme.

xxx

3.5 Úlohy na zbytkové třídy (důkazy)

Cvičení 3.14 Dokažte: 2. mocnina lichého čísla dává po dělení 4 zbytek 1.

Cvičení 3.15 Dokažte: 2. mocnina násobku 3 dává po dělení 9 zbytek 0 nebo 3 nebo [6].

Cvičení 3.16 Nechť m je prvočíslo. Dokažte, že m nedělí $(m-1)!$.

Cvičení 3.17 Nechť m je číslo složené. Dokažte, že m dělí $(m-1)!$.

Kapitola 4

Dělitelnost polynomu. Hledání kořenů polynomu.

Během výuky na základní a střední škole jste se v matematice zabývali řešením rovnic. Jako absolventi střední školy umíte řešit zejména

- rovnice o jedné neznámé (lineární, ale i nelineární, např. kubické: $x^3 = 8$)
- soustavy lineárních rovnic (zejména soustavy dvou lineárních rovnic: metoda dosazovací a sčítací)
- kvadratické rovnice s reálnými koeficienty

Poměrně jednoduše (ač může být výpočet pracný a může trvat dlouho) se dají řešit

- soustavy lineárních rovnic (tzv. Gaussovou eliminační metodou, viz přednášky z lineární algebry)
- speciální typy rovnic jako např. bikvadracké rovnice pomocí substituce

V dalším se budeme zabývat rovnicemi, v nichž na jedné straně vystupuje polynom stupně n a na druhé straně číslo 0.

Definice 4.1 (polynom stupně n) Nechť a_i jsou reálná čísla pro i=0, ..., n a nechť dále $a_n \neq 0$. Pak výraz $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ nazýváme polynomem stupně n, čísla a_i koeficienty polynomu, číslo n stupněm polynomu. Koeficient a_n se nazývá vedoucí koeficient daného polynomu a koeficient a_0 nese název absolutní člen.

Definice 4.2 (kořen polynomu) Říkáme, že číslo k je kořenem polynomu, jestliže $a_n k^n + a_{n-1}k^{n-1} + \cdots + a_2 k^2 + a_1 k + a_0 = 0$. (Dosadíme-li za x hodnotu k, bude polynom mít hodnotu 0.)

```
opakování vzorců $(a+b)^2 = $ atp.
   --- je třeba umět ‘‘tam i zpět’’

dělení polynomu polynomem jako analogie
    písemného dělení čísel
```

!! JE TO JEDNODUŠŠÍ!!

Kvadratické rovnice:
--- řešení pomocí diskriminantu
--- Vietovy vztahy

Cardanovy vzorce
--- bez odvození, jen to, že existují

rovnice 4. stupně: umíme - bikvadratické,
dají se řešit tzv. analyticky
(analogie diskriminantu a Cardanových vzorců)

hledání celočíselných kořenů:
--- Hornerovo schéma ---- jak funguje
(určení hodnoty polynomu; vyjde-li nula, je to kořen;
navíc podíl: mnohočlen dělím dvojčlenem)

!!! Úprava ‘‘doplnění na čtverec’’ !!!

Kapitola 5

Základy teorie grafů

Literatura

[1] Apfelbeck, Alois.1968. Kongruence. Edice škola mladých matematiků, svazek 21

[2] Bulant, Michal. Elementární teorie čísel. El. text.

[3] Fuchs, Eduard.2001. Diskrétní matematika pro učitelel. Skriptum MU.

[4] Vrba, Antonín. 1980. Kombinatorika. Edice škola mladých matematiků, svazek 45.