Závěr 19. století: 2 události typické pro naše téma

8. 8. 1900 Hilbertova přednáška Matematické problémy

David HILBERT (1862 – 1943)

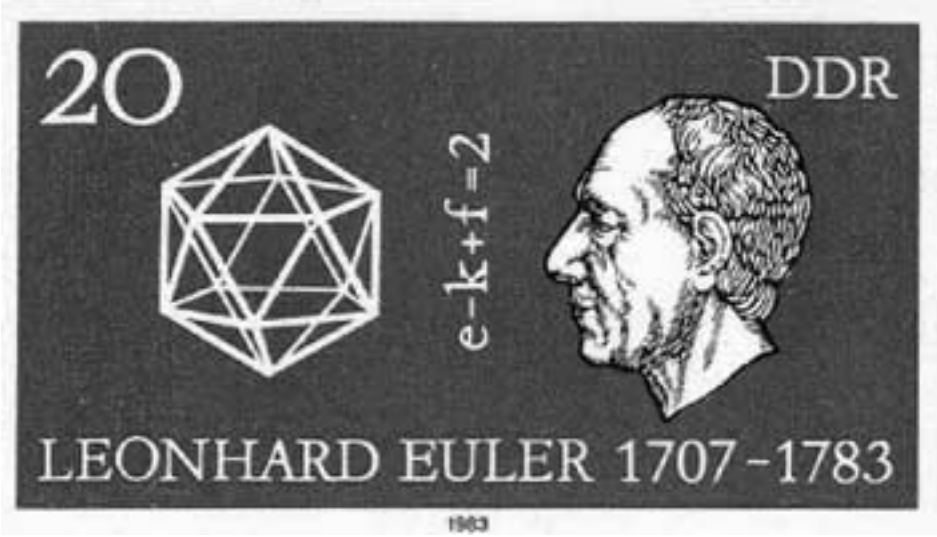
Gaston Tarry (1843 -- 1913) dokázal, že neexistují ortogonální latinské čtverce 6. řádu. Tím pro n = 6 potvrdil Eulerovu domněnku.

VĚTA: *Latinských čtverců řádu n je minimálně*

n! . (n-1)! . (n-2)! ... 1!

Pro n = 6 je tedy latinských čtverců nejméně

6! 5! 4! 3! 2! 1! = 24 883 200



Leonhard EULER (1707 – 1783)

Problematika moderní diskrétní matematiky

1. **Existuje konfigurace daného typu?**
   (ortogonální latinské čtverce 6. řádu, konečná rovina 10. řádu, graf s danými vlastnostmi, …)

2. **Sestrojit konfiguraci daného typu.**

3. Kolik je všech konfigurací daného typu?

4. Vygenerovat všechny konfigurace daného typu.

5. Najít v nějakém smyslu „optimální“ konfiguraci (nejkratší cestu, nejlevnější kostru, největší tok, …).

Které konfigurace jsou nejběžnější?

Grafy
Bloková schémata
Konečné geometrie
Uspořádané množiny
Rozklady čísel a množin ….

ALGORITMY

Dnešní pojetí pojmu:

- **algoritmus je zformulován v nějakém jazyku; jazyk je množina slov v zadané abecedě**
- **problém je řešen na základě vstupních dat**
- **algoritmus je procedura, která probíhá postupně po jednotlivých krocích**
- **každý krok je jednoznačně popsán algoritmem, vstupními daty a výsledky předcházejících kroků**
- **možné odpovědí – výstupy jsou jednoznačně předepsány**
- **při jakýchkoliv vstupních datech algoritmus končí po konečném počtu kroků**

Kořeny: Leibniz, Babbage, Boole, Frege, Peano.

V 90. letech 19. století – Hilbert: axiomatická výstavba, odvozování tvrzení z axiómů, problematika bezespornosti.

1904: na 3. mezinárodním matematickém kongresu v Heidelbergu Hilbert popisuje, jak lze axiómy a věty reprezentovat konečnými posloupnostmi symbolů a prověřování důkazů lze popsat „mechanickými pravidly“.

1922: Hilbert zpřesňuje popsané úvahy a formuluje „rozhodovací problém“ – proceduru, která po jednotlivých krocích testuje, zda lze formální výraz odvodit z daných axiómů

1928 Hilbert popisuje studium těchto formálních systémů ve společné práci s Wilhelmem Ackermannem (1896 – 1962). V témže roce Hilbert formuluje program, jak má být matematika budována.

1930 – 31 Gödel – věta o neúplnosti

Kurt GÖDEL (1906 – 1978)

Gödel při důkazu věty zavedl tzv. rekurzivní funkce, které v r. 1934 ještě zobecnil. Jeho práce inspirovaly Churche, Kleeneho, Turinga a Posta.

Alonzo CHURCH (1903 – 1995)

Alan Mattison TURING (1912 – 1954)

Emil Leon POST (1897 – 1954)

Stephen Cole KLEENE (1909 – 1994)

Turingův stroj

Churchova téze: Efektivně vyčíslitelné funkce jsou právě všechny rekurzivní funkce.

Vznik teorie algoritmů.

1970 Stephen A. Cook z University Toronto: klasifikace problémů (publikoval 1971) – třída P, NP, úplné-NP

V následující tabulce je přibližná doba k provedení algoritmu o složitosti f(n) na stroji, který provádí 1 milión operací za sekundu

		n		
		10	**100**	**1000**
f(n)	**25**	25×10^{-6} s	25×10^{-6}	25×10^{-6}
	$\log_2 n$	$3{,}3 \times 10^{-6}$ s	$6{,}6 \times 10^{-6}$ s	$1{,}2 \times 10^{-6}$ s
	n	10^{-5} s	10^{-4} s	5×10^{-3} s
	$n \log_2 n$	$3{,}3 \times 10^{-5}$ s	$6{,}6 \times 10^{-6}$ s	$6{,}1 \times 10^{-2}$ s
	n^2	10^{-4} s	0,01 s	25 s
	$2n^2+5n$	$3{,}5 \times 10^{-4}$ s	0,21 s	50 s
	$n^3/100$	10^{-5} s	0,01 s	21 min.
	2^n	10^{-3} s	4×10^{16} roků	$4{,}5 \times 10^{1491}$ r.

Příklady polynomiálních algoritmů:

- **nejkratší cesta mezi dvěma body**
- **úloha čínského pošťáka**
- **maximální tok v síti**
- **telefonní síť minimální délky**

Příklady nepolynomiálních algoritmů:

- **problém obchodního cestujícího**
- **zjištění isomorfismu dvou konfigurací**
- **problém dvou loupežníků**

Klíčové postavení Borůvkova problému:

Všechny algoritmy mají společné jádro. Začínají od izolovaných uzlů („triviální“ fragmenty). V každém kroku se k již sestrojeným fragmentům připojí další hrana nebo hrany.

Algoritmus
DVA NEJBLIŽŠÍ FRAGMENTY

Autor: J.B. KRUSKAL (1956)

1. Uspořádej hrany do posloupnosti tak, že
$$f(h_1) \leq f(h_2) \leq \ldots \leq f(h_n).$$

2. Utvoř graf (U,∅).

3. Přidávej postupně ty hrany $h_1, h_2, \ldots, h_n$, které neuzavřou kružnici.

Nejvhodnější strukturu dat pro implementaci popsali

J.E. Hopcroft, J.D. Ullman (1972)

Jejich algoritmus pracuje v čase O(e.log v), kde e je počet uzlů, v počet hran.

Algoritmus
VŠECHNY NEJBLIŽŠÍ FRAGMENTY

Autor: O. Borůvka (1926)

Nejstarší a historicky nejzajímavější. V průběhu let byl mnohokrát objeven.

Na jaře 1927 Borůvka o algoritmu přednášel v Paříži na semináři u Élie Cartana. Ten však na to zřejmě zapomněl, neboť v r. 1938 doporučil k publikaci práci

G. Choquet, Comptes Rendus 1938

v níž je Borůvkův algoritmus bez citace zopakován.

Další „objev“ téhož algoritmu provedl

G. Sollin (1961)

Rukopis však nepublikoval, ačkoliv práce byla již dokonce citována v knize
Berge – Ghoula-Houri: Programming Games and Transportation Networks, Wiley 1965

Borůvkův algoritmus:
1. **Spoj KAŽDÝ vrchol s nejbližším**
2. **Spoj KAŽDÝ fragment s nejbližším.**

Hladový algoritmus

Nechť S je konečná množina, F začátek v 2^S a w váhová funkce na S . Hledáme množinu $A \in F$ s největší vahou. Hladový algoritmus je následující:

1. Vyber $x_1 \in S$ tak, že $\{x_1\} \in F$ a $w(x_1)$ je maximální.
2. Když takové x neexistuje : KONEC

3. Zvol $x_2 \neq x_1$ tak, že $\{x_1, x_2\} \in \mathsf{F}$ a $w(x_2) \geq w(x)$ pro každé $x \neq x_1$, $\{x_1, x\} \in \mathsf{F}$
4. Když takové x neexistuje: KONEC
5. …….

Po konečném počtu kroků se algoritmus zastaví na nějaké množině X. Kdy je tento algoritmus správný při libovolné váhové funkci?

Věta: Hladový algoritmus řeší zadaný problém při libovolné váhové funkci právě tehdy, když je (S, F) matroid.

Lineární programování

Standardní simplexová metoda NENÍ polynomiálním algritmem.
Chačijan 1979: „elipsoidová metoda“ JE polynomiální algoritmus.

LATINSKÉ ČTVERCE

E. T. PARKER, Proc. AMS 10 (1959), 946 -949

Konstrukce ortogonálních latinských čtverců řádu 22.

Definitivní odpověď v r. 1960:

R. C. BOSE - S. S. SHRIKHANDE, Trans. AMS 95 (1960), 191 - 209

Ortogonální latinské čtverce existují pro každé přirozené $n > 2$ kromě $n = 6$.

Přitom je evidentní, že každá množina po dvou ortogonálních latinských čtverců řádu n má nejvýše $n-1$ prvků.

Příklad - ortogonální čtverce řádu 10

00	49	17	96	28	83	75	61	52	34
76	11	59	27	90	38	84	02	63	45
85	70	22	69	37	91	48	13	04	56
58	86	71	33	09	47	92	24	15	60
93	68	80	72	44	19	57	35	26	01
67	94	08	81	73	55	29	46	30	12
39	07	95	18	82	74	66	50	41	23
21	32	43	54	65	06	10	77	88	99
42	53	64	05	16	20	31	89	97	78
14	25	36	40	51	62	03	98	79	87

KONEČNÉ ROVINY

Definice: Buď A konečná neprázdná množina, $\mathfrak{R}$ nějaký systém jejích neprázdných podmnožin. Prvky množiny A v dalším nazýváme *body*, **prvky množiny $\mathfrak{R}$** *přímky.* **Dvojici (A, $\mathfrak{R}$) nazveme** *konečnou afinní rovinou*, **jestliže platí:**

I. **Každé dva různé body leží na právě jedné přímce.**
II. **Ke každému bodu $x \in A$ a každé přímce p , $x \notin p$ existuje právě jedna přímka q taková, že $x \in q$, $p \cap q = O$.**
III. **Existují tři navzájem různé body, které neleží na jedné přímce.**

Řád konečné roviny, rovnoběžky, směr.

Věta: Konečná afinní rovina řádu n má n^2 bodů a $n^2 + n$ přímek. Na každé přímce leží n bodů a každým bodem prochází n + 1 přímek. Všechny přímky lze rozdělit do n+1 směrů a každý směr obsahuje n rovnoběžek.

První směr	I	1	2	3	4
	II	5	7	6	8
	III	10	11	9	12
	IV	15	14	16	13
Druhý směr	V	13	1	5	9
	VI	14	10	2	6
	VII	11	15	7	3
	VIII	4	8	12	16
Třetí směr	IX	6	16	1	11
	X	12	5	15	2
	XI	8	9	3	14
	XII	13	4	10	7
Čtvrtý směr	XIII	7	12	14	1
	XIV	2	13	8	11
	XV	16	3	10	5
	XVI	9	6	4	15
Pátý směr	XVII	1	8	15	10
	XVIII	9	2	7	16
	XIX	3	12	13	6
	XX	5	14	11	4

Věta: **Konečná afinní rovina řádu $n \geq 3$ existuje právě tehdy, když existuje $n-1$ latinských čtverců n-tého řádu, z nichž každé dva jsou navzájem ortogonální.**

Důsledek: **Neexistuje konečná rovina 6. řádu.**

Konečných afinních rovin existuje nekonečně mnoho,

Věta: Je-li přirozené číslo n mocninou nějakého prvočísla, existuje konečná rovina n-tého řádu.

Věta: (P. H. Bruck - H. J. Ryser 1949) Nechť přirozené číslo n není součtem čtverců dvou přirozených čísel a nechť n=1 (mod 4) nebo n=2 (mod 4). Pak neexistuje konečná rovina řádu n .

$10!\ 9!\ 8!\ 7!\ 6!\ 5!\ 4!\ 3!\ 2!\ 1! = 6{,}658\ 606\ 583 \cdot 10^{27}$.

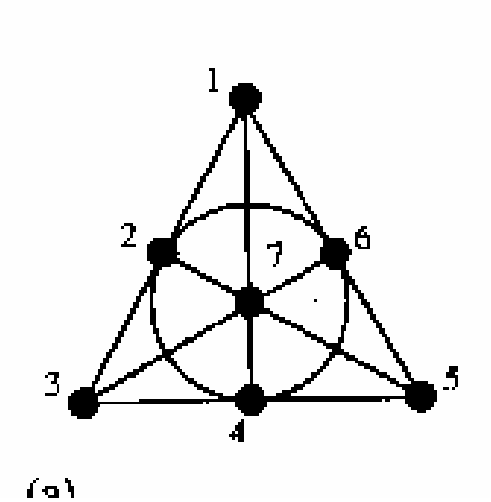
Analogicky se definuje projektivní rovina:

Definice: Buď A konečná neprázdná množina, $\mathfrak{R}$ nějaký systém jejích neprázdných podmnožin. Prvky množiny A v dalším nazýváme *body*, prvky množiny $\mathfrak{R}$ *přímky*. Dvojici (A, $\mathfrak{R}$) nazveme *konečnou* ***projektivní* *rovinou*, jestliže platí:**

I. **Každé dva různé body leží na právě jedné přímce.**
II. **Každé dvě různé přímky mají společný právě jeden bod.**
III. **Existují čtyři navzájem různé body, z nichž žádné tři neleží na jedné přímce.**

Jestliže všechny přímky mají n+1 bodů, nazýváme řádem roviny číslo n .

Příklad konečné projektivní roviny 2. řádu:



(a)

Bloková schemata

Jacob STEINER (1796 - 1863) zformuloval v r. 1853 problém trojic:

Pro která přirozená n lze z daných objektů vytvořit trojice tak, aby se každé dva prvky vyskytly společně právě v jedné trojici?

V r. 1859 dokázal M. RIESS, že vcelku evidentní nutná podmínka je i dostatečná:

Věta: Na n-prvkové množině existuje systém Steinerových trojic právě tehdy, když $n = 6k + 1$ nebo $n = 6k + 3$, $n \geq 3$, k celé. V tom případě je těchto trojic $n(n-1)/6$ a každý prvek se vyskytuje v $(n-1)/2$ trojicích.

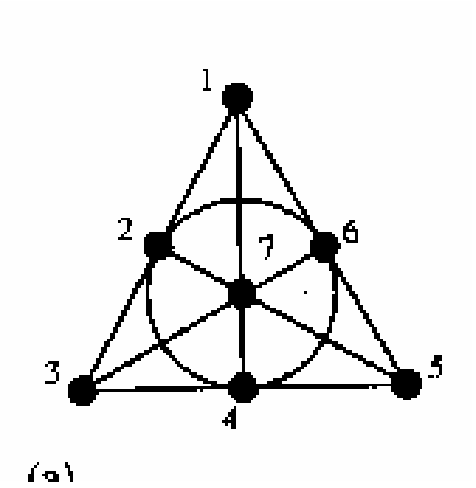
Příklad:

n = 3 : 123

n = 7 : **123 167 257 356**
145 246 347

n = 9 : **123 179 278 369**
145 249 348 467
168 256 357 589

X	X	X				
X			X	X		
X					X	X
	X		X		X	
	X			X		X
		X	X			X
		X		X	X	



(a)

TEORIE ENUMERACE

Centrální roli hraje tzv. Burnsidovo lemma.

William BURNSIDE (1852 – 1927)

Historie: V roce 1897 publikoval Burnside toto tvrzení ve své klasické knize o konečných grupách. V této knize je v poznámce pod čarou uvedena jako pramen tohoto tvrzení práce Georga FROBENIA (1849 – 1917) z roku 1887. Ve 2. vydání Burnsidovy knihy byla tato poznámky vynechána a tvrzení se začalo říkat *Burnsidovo lemma.* Ve skutečnosti se však toto tvrzení poprvé vyskytuje v práci Augustina-Louise CAUCHYHO (1789 – 1857) z roku 1847.

Označme S_n symetrickou grupu na n-prvkové množině X. Nechť G je podgrupa v S_n . Pro $x,y \in X$ položíme

$$x \equiv y \ (G)$$

právě tehdy, když existuje permutace $g \in G$ taková, že $g(x) = y$.
Je zřejmé, že $\equiv$ je ekvivalence na G. Třídy příslušného rozkladu na G se nazývají orbity.

Věta: Nechť O_k je orbita obsahující prvek k a G_k podgrupa v G permutací s pevným prvkem k . Pak

$$|G_k| \times |O_k| = |G| .$$

Příklad: Nechť G je podgrupa v S_5 generovaná permutací a = [1 2 3][4 5].
G tedy tvoří permutace

$a = [1\ 2\ 3]\ [4\ 5]$
$a^2 = [1\ 3\ 2]\ [4]\ [5]$
$a^3 = [1]\ [2]\ [3]\ [4\ 5]$
$a^4 = [1\ 2\ 3]\ [4]\ [5]$
$a^5 = [1\ 3\ 2]\ [4\ 5]$
$a_6 = [1]\ [2]\ [3]\ [4]\ [5]\ [6] = e$.

Orbity jsou tedy {1, 2, 3} a {4, 5}, $O_1 = \{1, 2, 3\}$, $G_1 = \{a^3, a^6\}$.
Platí

$$|G_1| \times |O_1| = |G| = 6 .$$

.

Burnsidovo lemma: Označme p(g) počet pevných bodů permutace g . Počet orbit podgrupy $G \subseteq S_n$ je roven číslu

$$\frac{1}{|G|} \cdot \sum_{g \in G} p(g) .$$

Příklad: Aplikací na předcházející příklad dostaneme

$p(a) = 0$, $p(a^2) = 2$, $p(a^3) = 3$, $p(a^4) = 2$, $p(a^5) = 0$, $p(a^6) = 5$, takže počet orbit je

$$(2 + 3 + 2 + 5)/6 = 2 .$$

1937 Pólyova věta.

George PÓLYA (1887 – 1985)

Jak v r. 1960 uvedl F. Harary, podstatné myšlenky tohoto tvrzení lze nalézt v práci J. H. Redfielda z r. 1927.