Historie matematiky a informatiky
Cvičení 1

Doc. RNDr. Alena Šolcová, Ph. D.,
KAM, FIT ČVUT v Praze

2014

Evropský sociální fond
Investujeme do vaší budoucnosti

Kapitola z teorie čísel

- Co předcházelo?
- Fermat a Mersenne – mistři 17. století
- Pokračovatelé v 18. stol.– Euler, Goldbach, Legendre, J. H. Lambert
- 19. stol. - Carl Friedrich Gauss – Aritmetická zkoumání, P. Dirichlet a další
- Analytická teorie čísel – první kroky do století dvacátého

Lámejte si hlavu – L1

Najděte všechna řešení kvadratické kongruence

$$x^2 \equiv 196 \pmod{1357}$$

x = 14, x = 1343, x = 635, x = 722

Vybrané úlohy z teorie čísel

Prvočísla a jejich rozmístění

Goldbachova hypotéza.

Číselně teoretické funkce.

Základní vlastnosti kongruencí.

Čínská věta o zbytcích.

Kvadratická kongruence.

Gaussovy algoritmy. Výpočet kalendáře.

Prvočísla a jejich rozmístění

(Primes and their distribution)

- Prvočísla (Primes)
- Základní věta aritmetiky
  (Fundamental Theorem of Arithmetic)
- Eratosthenovo síto (The Sieve of Eratosthenes)
- Goldbachova hypotéza
  (The Goldbach Conjecture)

Základní věta aritmetiky

Každé kladné celé číslo $n > 1$ může být vyjádřeno jako součin prvočísel. Tento rozklad je jednoznačný.

- Důsledek: Kladné celé číslo $n > 1$ může být

vyjádřeno v kanonickém tvaru jediným způsobem

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r},$$

kde každé k_i *je* kladné celé číslo pro $i = 1, 2, \ldots, r$

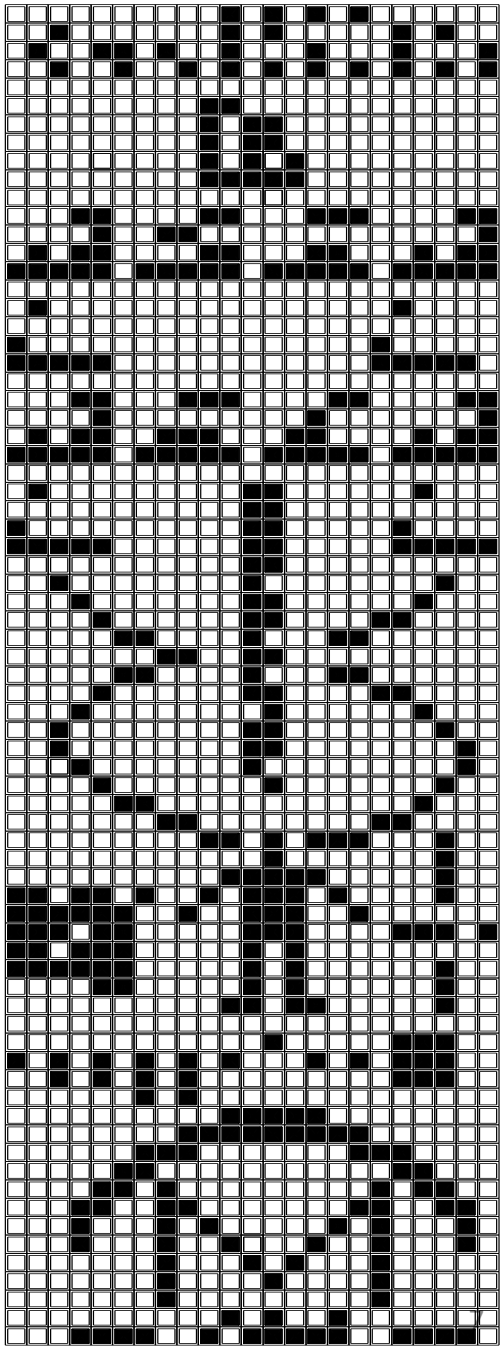
a každé p_i je prvočíslo takové, že

$$p_1 < p_2 < \ldots < p_r$$

Příklady

- $360 = 2^3\, 3^2\, 5$
- $4725 = 3^3\, 5^2\, 7$
- $17640 = 2^3\, 3^2\, 5\, 7^2$

- $65536 = 2^{16}$
- $143 = 11 \,.\, 13$
- $1679 = 23 \,.\, 73$
- $1271 = 31 \,.\, 41$



Testování prvočíselnosti

Je-li a složené celé číslo, pak můžeme psát

$a = b.c$, kde $1 < b < a$ a $1 < c < a$.

Předpokládáme-li, že $b \leq c$, dostaneme

$b^2 \leq bc = a$, a dále $b \leq \sqrt{a}$.

Protože $b > 1$, má b podle ZVA nejméně jednoho prvočíselného dělitele p.

Pak platí $p \leq b \leq \sqrt{a}$, dále $p \mid b$ a $b \mid a \Rightarrow p \mid a$.
Složené číslo a má vždy prvočíselného dělitele

$$p \leq \sqrt{a},$$

odtud plyne:

stačí testovat čísla menší než $\sqrt{a}$ nebo rovna $\sqrt{a}$.

Testování prvočíselnosti - příklady

Příklad: $a = 509$

$22 < \sqrt{509} < 23$

Otestujeme jako možné dělitele prvočísla menší než 22, tj. { 2, 3, 5, 7, 11, 13, 17, 19}.

Protože žádné z nich není dělitel 509, musí být dané *a* prvočíslo.

Testování prvočíselnosti - příklady

Příklad : $a = 2093$

$45 < \sqrt{2093} < 46$

Otestujeme jako možné dělitele prvočísla menší než 22, tj. { 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43}.

První dělitel 2093 je 7: $2093 = 7 \cdot 299$

$17 < \sqrt{299} < 18$, testujeme {2, 3, 5, 7, 11, 13}

První dělitel 299 je 13: $299 = 13 \cdot 23$.

23 je též prvočíslo.

Rozklad čísla je $2093 = 7 \cdot 13 \cdot 23$.

Eratosthenovo síto

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Čísla dělitelná dvěma, třemi a pěti

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Lámejte si hlavu – L2

- Použijte Ératosthenova síta k rozkladu čísla 94 na součet dvou prvočísel.
- Kolik takových rozkladů existuje?

Existuje 5 rozkladů:

94 = 89 + 5

94 = 83 + 11

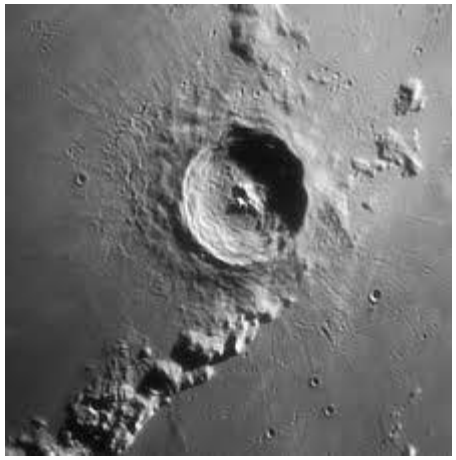
94 = 71 + 23

94 = 53 + 41

94 = 47 + 47

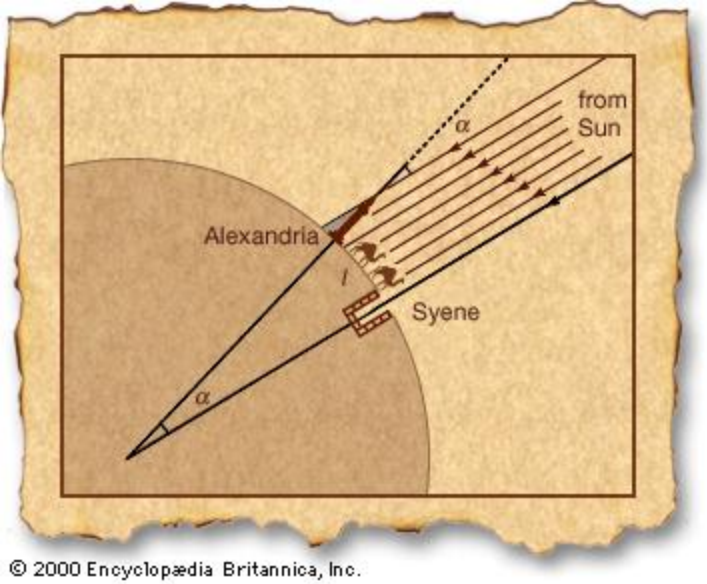
Ératosthenés z Kyrény

- 276 – 194 př. n. l.
- Žil v Alexandrii.
- Přezdívka „Beta“

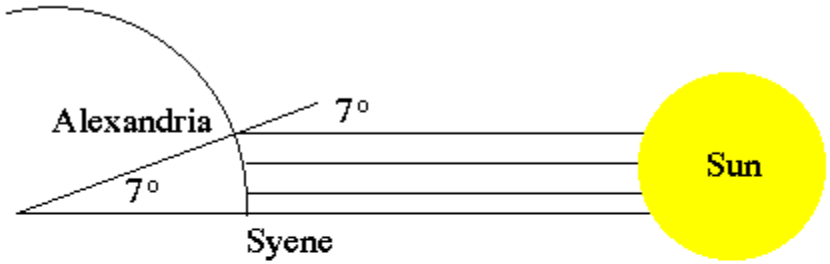


- Vyměřil obvod Země
- Přítel Archimédův
- Je po něm pojmenován kráter na Měsíci.
- Ératosthenovo síto v XI. knize Eukleidových Základů
- Otázka: Existuje největší prvočíslo?

Obvod Země



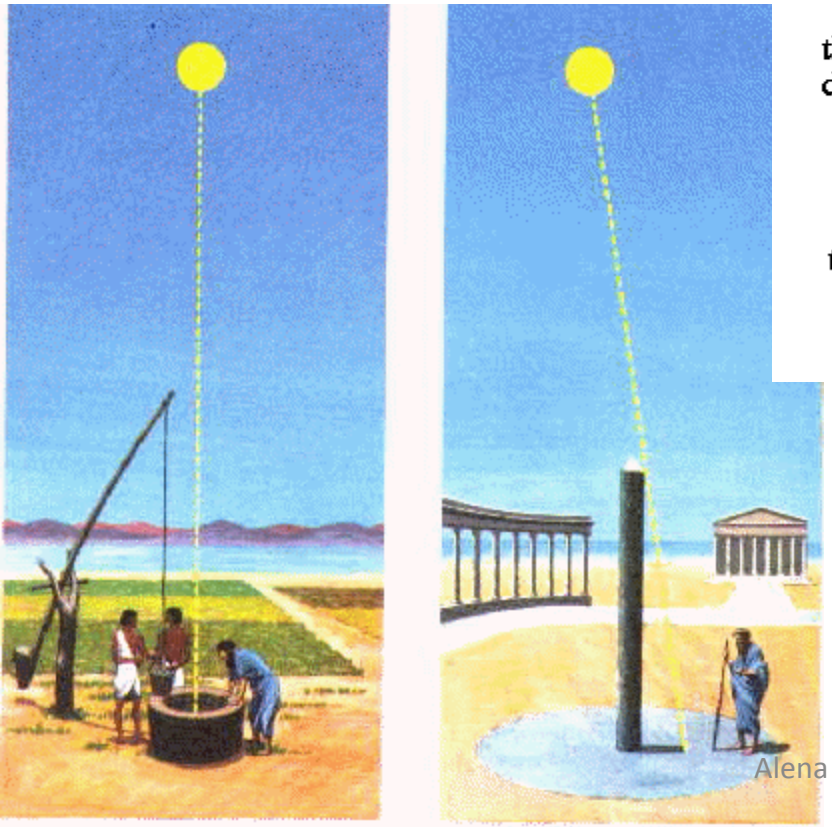
Eratosthenes



the distance from Alexandria to Syene was 4900 stadia, so the ratio of that distance to the circumference of the Earth, C is given by:

$$\frac{C}{4900 \text{ stadia}} = \frac{360^\circ}{7^\circ}$$

therefore, C = 252,000 stadia (1 stadia = 0.16 km)
= 40,320 km (textbook gives circumference of Earth as 40,030 km)



Eukleidova věta

- Věta:

  Počet všech prvočísel je nekonečný.

Důkaz: Eukleidés postupuje sporem.

Nechť existuje rostoucí posloupnost prvočísel

$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ … a p_n je poslední z nich.

Uvažujme $P = p_1 p_2 \ldots p_n + 1$. Protože $P > 1$ podle ZVA je P dělitelné nějakým prvočíslem.

Důkaz Eukleidovy věty

- $p_1 p_2 \ldots p_n$ jsou jediná prvočísla menší než P, proto další prvočíslo p se musí rovnat jednomu z nich.
- Když spojíme dělitelnost $p \mid p_1 p_2 \ldots p_n$ a $p \mid P$, dostaneme $p \mid P - p_1 p_2 \ldots p_n$, ekvivalentně $p \mid 1$.
- Jediný kladný dělitel čísla 1 je 1, ale $p > 1$,

  tj. spor!
- Žádný konečný seznam prvočísel není úplný, počet prvočísel je nekonečný.

  The number of primes is infinite.

Eukleidova čísla (Euclid Numbers) jsou čísla tvaru

$p_1 p_2 \ldots p_n + 1$, mezi nimi je asi 19 prvočísel.

Goldbachova hypotéza

- Rozmístění prvočísel (Prime Distribution)

mezi čísly složenými – neznáme odpověď.

- Prvočíselná dvojčata (Prime Twins): dvojice lichých čísel (p, p + 2) - 11 a 13, 17 a 19 nebo 100000000061 a 100000000063.

Intervaly mezi prvočísly jsou libovolně dlouhé.

Nejdelší mezera má 1132 složených čísel.

Otázka: Je počet prvočíselných dvojčat konečný?

Goldbachova hypotéza

- 1742 píše Christian Goldbach Leonhardu Eulerovi:

> Každé sudé číslo může být vyjádřeno součtem dvou čísel, jež jsou prvočísla nebo jedničky.

- Prověřeno do $4 . 10^{14}$
- Ukážeme si rozklady do 30:

Goldbachovy rozklady

$2 = 1 + 1$

$4 = 2 + 2 = 1 + 3$

$6 = 3 + 3 = 1 + 5$

$8 = 3 + 5 = 1 + 7$

$10 = 3 + 7 = 5 + 5$

$12 = 5 + 7 = 1 + 11$

$14 = 3 + 11 = 7 + 7 = 1 + 13$

$16 = 3 + 13 = 5 + 11$

$18 = 5 + 13 = 7 + 11 = 1 + 17$

$20 = 3 + 17 = 7 + 13 = 1 + 19$

$22 = 3 + 19 = 5 + 17 = 11 + 11$

$24 = 5 + 19 = 7 + 17 = 11 + 13 = 1 + 24$

$26 = 3 + 23 = 7 + 19 = 13 + 13$

$28 = 5 + 23 = 11 + 17$

$30 = 7 + 23 = 11 + 19 = 13 + 17 = 1 + 29$

Goldbachova hypotéza

- Euler omezil hypotézu takto:

  Libovolné sudé číslo (≥ 6) tvaru $4n + 2$ je součet dvou čísel,

  jež jsou prvočísla tvaru $4n + 1$ nebo 1.

  Lze ukázat:

  Každé sudé číslo je součtem 6 nebo méně prvočísel.

Lemma: Součin dvou nebo více čísel tvaru $4n + 1$ je též tvaru $4n + 1$. Dokažte si samostatně.

Věta: Počet prvočísel tvaru $4n + 3$ je nekonečný.

Důkaz sporem.

Christian Goldbach

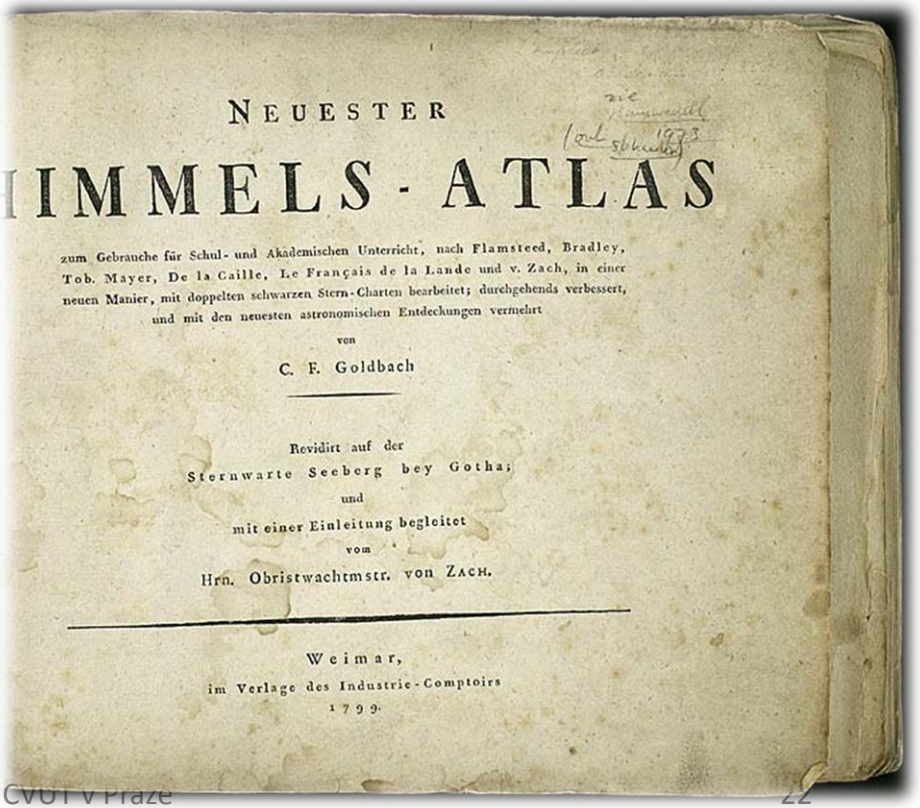
- 1690 Königsberg – 1764 Moskva

Otec: protestantský kněz

Studium v Königsbergu.

Korespondence

s Leibnizem, Eulerem.


NEUESTER

IMMELS-ATLAS

zum Gebrauche für Schul- und Akademischen Unterricht, nach Flamsteed, Bradley, Tob. Mayer, De la Caille, Le Français de la Lande und v. Zach, in einer neuen Manier, mit doppelten schwarzen Stern-Charten bearbeitet; durchgehends verbessert, und mit den neuesten astronomischen Entdeckungen vermehrt

von

C. F. Goldbach

Revidirt auf der

Sternwarte Seeberg bey Gotha;

und

mit einer Einleitung begleitet

vom

Hrn. Obristwachtmstr. von Zach.

Weimar,

im Verlage des Industrie-Comptoirs

1799.

Dirichletova věta

- Věta:

  Jestliže a a b jsou vzájemně nesoudělná čísla,

  pak aritmetická posloupnost

  $$a, a + b, a + 2b, a + 3b \ldots$$

  obsahuje nekonečně mnoho prvočísel.

  Dirichlet zjistil např. , že je nekonečně mnoho prvočísel končících na 999: 1999, 100999, 1000999, … . Tato aritmetická posloupnost je určena tvarem $1000k + 999$ a nsd(1000, 999) =1

Jean Johann Peter Gustav Le Jeune Dirichlet

- 1805 Düren – 1859 Göttingen
- Otec - poštmistr v Dürenu, půl cesty mezi Cáchami a Kolínem
- Pochází z Belgie: Le jeune de Richelet
- Měl rád historii i matematiku.
- Nástupce Gausse v Göttingen.

Čemu se dlouho věřilo?

- Euler se také někdy mýlil. V roce 1772 ukázal, že kvadratický polynom
- $f(n) = n^2 + n + 41$ dává pouze prvočíselné hodnoty.

Prověřil pouze tyto hodnoty {0, 1, 2, …, 39}. Použil metodu neúplné indukce.

$f(40) = 40^2 + 40 + 41 = 40(40 + 1) + 41 =$

$40 \cdot 41 + 41 = 41\,(40 + 1) = 41^2$ složené číslo

$f(41) = 41^2 + 41 + 41 = 41\,(41 + 1 + 1) = 41 \cdot 43$

$f(42) = 42^2 + 42 + 41 = 1847$ opět dává prvočíslo.