Historie matematiky a informatiky 2
7. přednáška

Doc. RNDr. Alena Šolcová, Ph. D.,

KAM, FIT ČVUT v Praze

5. října 2013

Evropský sociální fond

Investujeme do vaší budoucnosti

Kapitoly 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 – L7-2

Najděte všechna řešení kvadratické kongruence

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

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

Vybrané problémy 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 $i = 1, 2, \ldots, r$

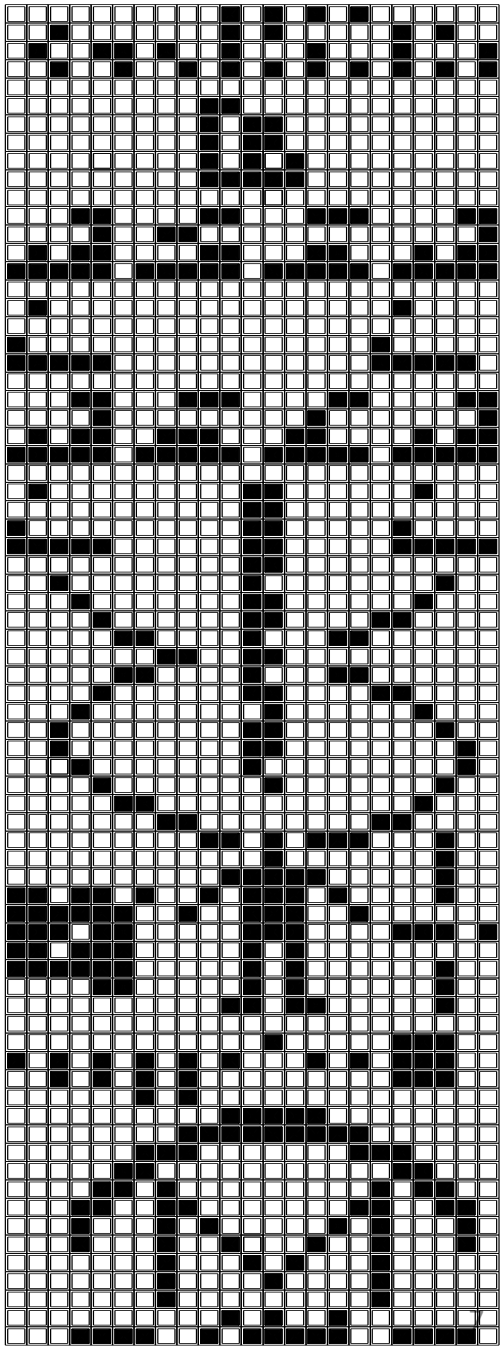
a každé p_i je prvočíslo takové, že

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

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 – L7-1

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

Existuje 5 rozkladů:

94 = 89 + 5

94 = 83 + 11

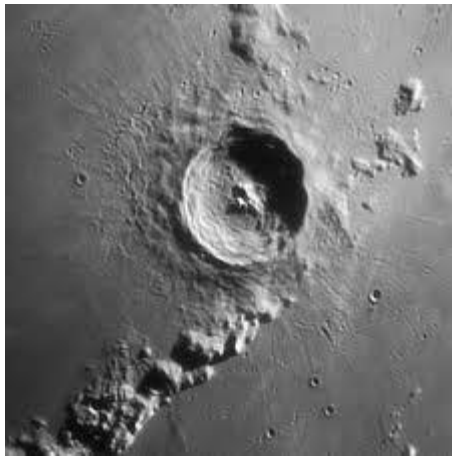
94 = 71 + 23

94 = 53 + 41

94 = 47 + 47

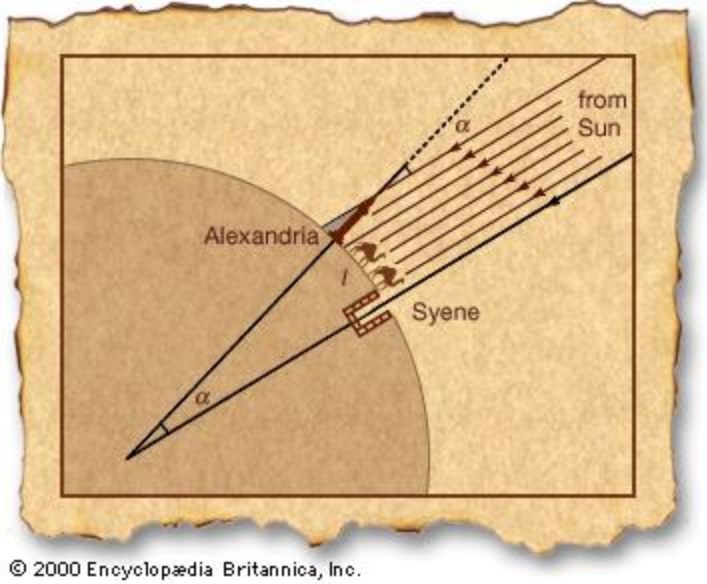
Ératosthenés z Kyrény

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

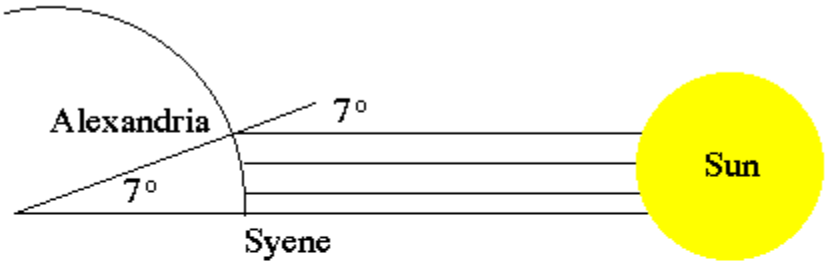


- Vyměřil obvod Země
- Přítel Archimédův
- Je po něm pojmenován kráter na Měsíci.
- Ératosthenovo síto v XI. knize Eukleidových Základů
- Otázka: Existuje největší prvočíslo?

Obvod Země



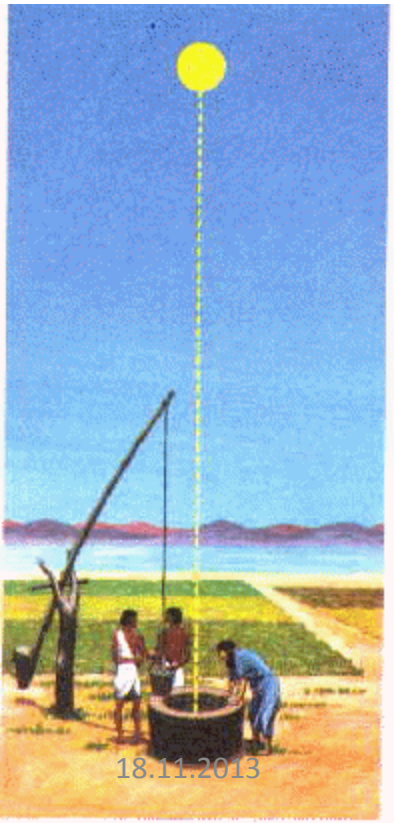
Eratosthenes

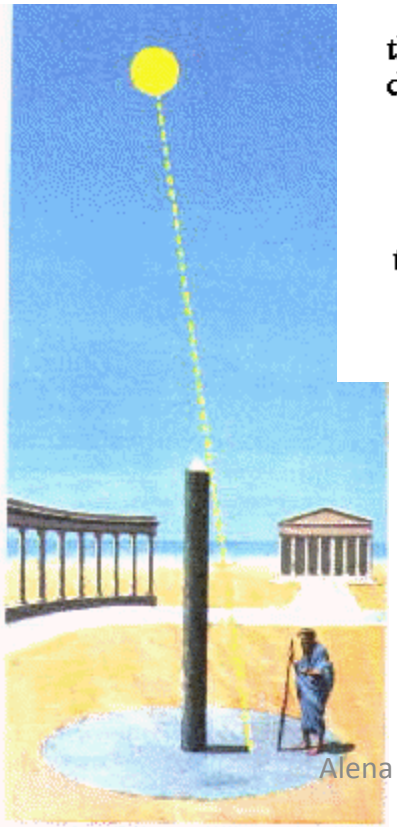


the distance from Alexandria to Syene was 4900 stadia, so the ratio of that distance to the circumference of the Earth, C is given by:

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

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

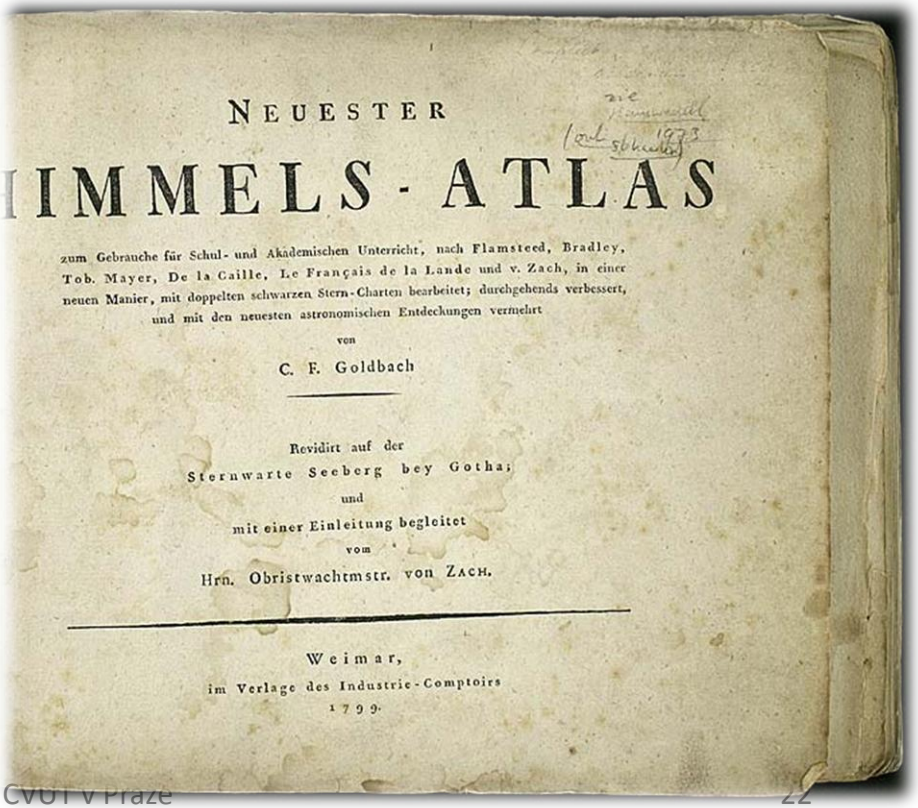
- 1690 Königsberg – 1764 Moskva

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.

Číselně teoretické funkce

(Number-Theoretic Functions)

- Součet a počet dělitelů (The Sum and Number of Divisiors)
- Möbiova funkce (The Möbius inversion formula)
- Celá část čísla (The Greatest Integer Function)
- Eulerova funkce φ (Euler's Phi-Function)
- August Ferdinand Möbius, Leonhard Euler

Součet a počet dělitelů

Definice:

Je dáno kladné celé číslo *n,* označíme

$\tau(n)$ počet kladných dělitelů čísla n a $\sigma(n)$ součet těchto dělitelů.

Příklad: n = 12.

Má tyto kladné dělitele {1, 2, 3, 4, 6, 12}, tedy

$\tau(12) = 6$,

$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$

Určete funkce $\tau(n)$ a $\sigma(n)$ pro prvních několik n!

Součet a počet dělitelů

- Věta: $\tau(n) = 2$ právě tehdy, když n je prvočíslo.
- Věta: $\sigma(n) = n + 1$ právě tehdy, když n je prvočíslo.
- Obě funkce jsou multiplikativní, tj.

$$\tau(mn) = \tau(m)\,\tau(n)$$

$$\sigma(mn) = \sigma(m)\,\sigma(n),$$

pro libovolná vzájemně nesoudělná m, n.

Möbiova funkce

- August Ferdinand Möbius
- Definice: Pro kladné celé číslo n definujeme

funkci $\mu(n)$ =

$$\begin{cases} 1 & \text{je-li } n = 1 \\ 0 & \text{je-li } p^2 \mid n \text{ pro nějaké prvočíslo } p \\ (-1)^r & \text{je-li } n = p_1 p_2 \dots p_r, \text{ kde } p_i \text{ jsou různá prvočísla.} \end{cases}$$

Vlastnosti Möbiovy funkce

Příklad:

$\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$

$\mu(1) = 1,\ \mu(2) = -1,\ \mu(3) = -1,$
$\mu(4) = 0,\ \mu(5) = -1,\ \mu(6) = 1.$

Věta: Funkce μ je multiplikativní funkce.

Zkuste samostatně dokázat.

Aplikace najdeme v teorii čísel, kombinatorice, fyzice apod.

Funkce “celá část čísla“

The Greatest Integer Function,

„Bracket“ Function

Definice: Pro libovolné reálné číslo x , označíme $[x]$ nejbližší celé číslo menší než x, tedy x splňuje podmínku $x - 1 < [x] < x$.

Příklady: $[-3/2] = -2$, $[\sqrt{2}] = 1$, $[1/3] = 0$,

$[\pi] = 3$ $[-\pi] = 4$

Věta: $[x] = x$ právě tehdy, když x je celé číslo.

Libovolné reálné číslo lze zapsat ve tvaru

$$x = [x] + \theta, \text{ kde } 0 \leq \theta < 1.$$

Eulerova funkce φ

(Euler's Phi-Function)

Definice:

Pro $n \geq 1$ $\varphi(n)$ označuje počet kladných celých čísel nesoudělných s n a menších nebo rovných než n.

Příklad: $\varphi(30) = 8$

$\{1, 7, 11, 13, 17, 19, 23, 29\}$,

$\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$,

$\varphi(6) = 2$, $\varphi(7) = 6$

Některé vlastnosti funkce φ

Věta: Je-li *n* prvočíslo, pak každé celé číslo menší než *n* je nesoudělné s *n,* tedy

$$\varphi(n) = n - 1$$

Věta: Je-li $n > 1$ složené, pak má *n* dělitele *d* takové, že jsou v intervalu $1 < d < n$. To znamená, že nejméně dvě čísla mezi 1, 2, 3, …, *n* nejsou soudělná s *n,* totiž *d* a *n, tj.*

$$\varphi(n) \leq n - 2$$

Některé vlastnosti funkce φ

Věta: Jestliže p je prvočíslo a $k > 0$, pak

$$\varphi(p^k) = p^k - p^{k-1} = p^k\,(1 - 1/p)$$

Příklad: $\varphi(9) = \varphi(3^2) = 3^2 - 3 = 6$

$$\{1, 2, 4, 5, 7, 8\}$$

$$\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$$

$$\{1, 3, 5, 7, 9, 11, 13, 15\}$$

Věta: Funkce φ je multiplikativní,

tj. $\varphi(m.n) = \varphi(m) \,.\, \varphi(n)$,

kde m a n jsou nesoudělná.

Gaussova věta

Pro každé kladné celé číslo $n \leq 1$ platí

$$n = \sum_{d|n} \varphi(d)$$

(sčítá se přes všechny kladné dělitele d čísla n).

Příklad

- Nechť je $n = 10$.
- Čísla mezi 0 a n rozdělíme do tříd podle d. Je-li d kladný dělitel čísla n, uložíme celé číslo m mezi prvky třídy S_d, jestliže platí $\text{nsd}(m,n) = d$

$$S_d = \{m \mid \text{nsd}(m,n) = d,\ 1 \leq m \leq n\}.$$

$S_1 = \{1, 3, 7, 9\}$

$S_2 = \{2, 4, 6, 8\}$

$S_5 = \{5\}$

$S_{10} = \{10\}$

$$\varphi(10) = 4,\ \varphi(5) = 4,\ \varphi(2) = 1,\ \varphi(1) = 1$$

$$\sum_{d|10}\varphi(d) = \varphi(10) + \varphi(5) + \varphi(2) + \varphi(1) = 4 + 4 + 1 + 1 = 10$$

Teorie kongruencí

(The Theory of Congruences)

- Carl Friedrich Gauss
- Základní vlastnosti kongruencí
- Lineární kongruence
- Čínská věta o zbytcích
- Kvadratická kongruence

..

Základní vlastnosti kongruencí

Definice:

Nechť n je kladné celé číslo. Dvě čísla a a b jsou kongruentní podle modulu n

$$a \equiv b \pmod{n},$$

jestliže n dělí rozdíl $a - b$,

tedy $a - b = kn$ pro k celé.

Kongruence je zobecněná forma ekvivalence.

Věta: Nechť n > 1, a,b, c, d jsou libovolná celá čísla.

Pak platí

a) $a \equiv a \pmod{n}$

b) Je-li $a \equiv b \pmod{n}$, pak $b \equiv a \pmod{n}$

Základní vlastnosti kongruencí

Věta:

c) Je-li $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, pak $a \equiv c \pmod{n}$.

d) $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$,

pak a $a + b \equiv c + d \pmod{n}$ a

$ac \equiv bd \pmod{n}$.

e) Je-li $a \equiv b \pmod{n}$, pak

$a + c \equiv b + c \pmod{n}$ a ac $\equiv bc \pmod{n}$.

f) Je-li $a \equiv b \pmod{n}$, pak $a^k \equiv b^k \pmod{n}$, pro libovolné kladné k.

Příklad - kongruence

- Ukažte, že 41 dělí $20^{20} - 1$
- Začneme tím, že $2^5 \equiv -9 \pmod{41}$, jinak také

$2^{20} \equiv 81 \,.\, 81 \pmod{41}$

Ale $81 \equiv -1 \pmod{41}$,

a tedy $81.\, 81 \equiv 1 \pmod{41}$.

Podle vlastností kongruence pokračujeme:

$2^{20} - 1 \equiv 81 \,.\, 81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}$,

tedy 41 dělí $20^{20} - 1$.

Příklad - kongruence

- Chceme najít zbytek po dělení součtu

$1! + 2! + 3! + 4! + \ldots + 99! + 100!$ číslem 12.

- Zahájíme zjištěním, že $4! \equiv 24 \pmod{12}$, takže

Pro $k \geq 4$ platí

$k! \equiv 4! + 5 \cdot 6 \ldots k \equiv 0 \cdot 5 \cdot 6 \ldots k \equiv 0 \pmod{12}$

Takto dostaneme

$1! + 2! + 3! + 4! + \ldots + 99! + 100! \equiv 1! + 2! + 3! + 0 + \ldots + 0 \equiv 9 \pmod{12}$

Odtud součet dává zbytek 9 při dělení 12.

Další vlastnosti

- Věta: Je-li $ca \equiv cb \pmod{n}$,

  pak $a \equiv c \pmod{n/d}$, kde $d = \text{nsd}(c,n)$.
- Důsledek: Je-li $ca \equiv cb \pmod{n}$ a $\text{nsd}(c,n) = 1$, pak $a \equiv b \pmod{n}$.
- Důsledek: Je-li $ca \equiv cb \pmod{p}$, a p nedělí c, kde p je prvočíslo, pak $a \equiv b \pmod{p}$.

Důkaz: Podmínky: p nedělí c a p je prvočíslo implikují $\text{nsd}(c, p) = 1$.

Příklady

- Uvažujme o kongruenci $33 \equiv 15 \pmod 9$,

tj. $3.\ 11 \equiv 3\ .\ 5 \pmod 9$.

Protože nsd (3, 9) = 3 podle předcházející věty můžeme psát $11 \equiv 5 \pmod 3$.

- Jinou kongruenci $-35 \equiv 45 \pmod 8$ můžeme rozložit stejným způsobem

  na $5\ (-7) \equiv 5.\ 9 \pmod 8$. Čísla 5 a 8 jsou nesoudělná, proto upravíme na

  $$-7 \equiv 9 \pmod 8.$$

Čínská věta o zbytcích

The Chinese Remainder Theorem

Věta:

Nechť $n_1, n_2, \ldots, n_r$ kladná celá čísla taková, že

$$\text{nsd}(n_i, n_j) = 1 \text{ pro } i \neq j.$$

Pak soustava lineárních kongruencí

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

má jedno řešení x modulo n, kde $n = n_1, n_2, \ldots, n_r$.

Příklad

Problém Sun-Tsu (Sun Zi)

- Vyřešte soustavu kongruencí

  $x \equiv 2 \pmod 3$

  $x \equiv 3 \pmod 5$

  $x \equiv 2 \pmod 7$

Řešení:

$n = 3.\ 5.\ 7 = 105$

$N_1 = n/3 = 35$, $N_2 = n/5 = 21$ $N_3 = n/7 = 15$

Sestavíme lineární kongruence: $35x \equiv 1 \pmod 3$,

$21x \equiv 1 \pmod 5$,

$15x \equiv 1 \pmod 7$,

které dávají řešení pro $x_1 = 2$, $x_2 = 1$, $x_3 = 1$

$x = 2.\ 35\ .\ 2 + 3\ .\ 21\ .\ 1 + 2\ .\ 15\ .\ 1 = 233$

Pro mod (105) dostáváme jediné řešení:

$x = 233 \equiv 23 \pmod{105}$.

Zákon kvadratické reciprocity

(The Quadratic Reciprocity Law)

- Eulerovo kriterium (The Euler Criterion)
- Legendrův symbol (The Legendre Symbol)

Kvadratické reziduum

- Definice: Nechť p je liché prvočíslo a nsd (a,p) = 1. Má-li kvadratická kongruence

$$x^2 \equiv a \pmod{p}$$

řešení x, pak řekneme, že a je kvadratické reziduum čísla p.

Jestliže žádné takové x neexistuje, nazývá se a kvadratické nereziduum čísla p.

Příklad kvadratického rezidua pro n=13

Určíme čtverce všech zbytkových tříd (mod 13):

$$1^2 \equiv 12^2 \equiv 1$$

$$2^2 \equiv 11^2 \equiv 4$$

$$3^2 \equiv 10^2 \equiv 9$$

$$4^2 \equiv 9^2 \equiv 3$$

$$5^2 \equiv 8^2 \equiv 12$$

$$6^2 \equiv 7^2 \equiv 10$$

Kvadratická rezidua čísla 13 jsou: 1,3,4,9,10,12.

Kvadratická nerezidua čísla 13 jsou: 2,5,6,7,8,11.

Eulerovo kriterium

Euler's Criterion

Věta: Nechť p je liché prvočíslo

a platí nsd(a,p) = 1,

pak číslo a je kvadratické reziduum prvočísla p právě tehdy,

když $a^{(p-1)/2} \equiv 1 \pmod{p}$

Legendrův symbol a jeho vlastnosti

- Definice: Nechť p je liché prvočíslo a nechť

  nsd $(a, p) = 1$.

Legendrův symbol (a/p) je definován takto:

$$(a/p) = \begin{cases} 1 & \text{je-li } a \text{ kvadratické reziduum } p \\ -1 & \text{je-li } a \text{ kvadratické nereziduum } p \end{cases}$$

Příklady

- Příklad: Nechť $p = 13$. Použijeme-li Legendrův symbol, pak mohou být výsledky zaznamenány takto:

$$1 = (1/13) = (3/13) = (4/13) = (9/13) = (10/13) = (12/13)$$

$$-1 = (2/13) = (5/13) = (6/13) = (7/13) = (8/13) = (11/13)$$

Vlastnosti Legendrova symbolu

Nechť p je liché prvočíslo a nechť celá čísla a a b jsou nesoudělná s p. Potom

(a) Jestliže $a \equiv b \pmod{p}$, pak $(a/p)=(b/p)$.

(b) $(a^2/p) = 1$.

(c) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.

(d) $(ab/p) = (a/p)(b/p)$.

(e) $(1/p) = 1$ a $(-1/p) = (-1)^{(p-1)/2}$.

Příklad:

Existuje nějaké řešení kongruence $x^2 \equiv -46 \pmod{17}$?

$(-46/17) = (-1/17)\,(46/17) = (-1)^8\,(12/17) = (3.2^2/17) =$

$= (3/17)\,(2^2/17) = (3/17) \equiv 3^8 \equiv 81^2 \equiv (-4)^2 = -1$ … NEEX.

Nebo jinak: $(-46/17) = (5/17) \equiv 5^8 \equiv 25^4 \equiv 8^4 \equiv 64^2 \equiv 13^2 \equiv -1$

Zákon kvadratické reciprocity

Quadratic Reciprocity Law – Theorema aureum

Věta: Jsou-li p a q různá lichá čísla,

pak $(p/q)\,(q/p) = (-1)^{(p-1)/2 \cdot (q-1)/2}$

Důsledek: Jsou-li p a q různá lichá čísla,

pak

$$(p/q) = \begin{cases} (q/p), \text{ je-li } p \equiv 1 \pmod 4 \text{ nebo } q \equiv 1 \pmod 4 \\ -(q/p), \text{ je-li } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Příklad

Uvažujme o Legendrově symbolu (29/53)

Protože $29 \equiv 1 \pmod 4$ a $53 \equiv 1 \pmod 4$,

můžeme upravit (29/53) = (53/29) = (24/29) = (2/29) (3/29) (4/29) = (2/29) (3/29).

(2/29) = -1, druhý LS invertujeme (3/29) = (29/3) = (2/3) = -1, dále použijeme kongruenci.

$29 \equiv 2 \pmod 3$ a dostaneme (29/53) = (2/29) (3/29) = (-1)(-1) = 1.

Pokračování

- Zákon kvadratické reciprocity dává odpověď na nalezení prvočísel p ≠ 3, pro něž je 3 kvadratické reziduum. Protože $3 \equiv 3 \pmod 4$

  z důsledku Zákona kvadratické reciprocity plyne:

$(3/p) = (p/3)$, je-li $p \equiv 1 \pmod 4$,

nebo $-(p/3)$, je-li $p \equiv 3 \pmod 4$.

Dále probereme $p \equiv 1 \pmod 3$ nebo

$p \equiv 1 \pmod 4$. Podle věty o vlastnostech LS platí:

$(p/3) = 1$, je-li $p \equiv 1 \pmod 3$,

nebo -1 , je-li $p \equiv 2 \pmod 3$.

Pokračování 2

Odtud plyne

$(3/p) = 1$ právě tehdy, když

$$p \equiv 1 \pmod 4 \text{ a } p \equiv 1 \pmod 3$$

nebo

$$p \equiv 3 \pmod 4 \text{ a } p \equiv 2 \pmod 3.$$

Lámejte si hlavu – L7 - 3

Najděte všechna řešení kvadratické kongruence

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

Odpověď zašlete na adresu

alena.solcova@fit.cvut.cz

Předmět: JménoPříjmení-L7-3

Výpočet Velikonoc

Gaussův algoritmus

Pro období 1900 – 2099 volíme konstanty

$$m = 24 \text{ a } n = 5.$$

Nechť a, b, c, d, e jsou nejmenší nezáporná čísla, která splňují kongruence

$a \equiv r \pmod{19}$,

$b \equiv r \pmod{4}$,

$c \equiv r \pmod{7}$,

$d \equiv (m + 19a) \pmod{30}$,

$e \equiv (n + 2b + 4c + 6d) \pmod{19}$.

Pak pro $d + e < 10$ připadá velikonoční neděle na březnový den, který výpočteme jako (22 + d + e).

Výpočet Velikonoc 2

- Pro $d + e = 35$ připadá velikonoční neděle

  na $(d + e - 16)$ – tý den v dubnu a ve zbývajících případech měsíce dubna na den

  $(d + e - 9)$.

  Tento algoritmus má však nejméně dvě výjimky, roky 1954 a 2049, kdy velikonoční neděle nepřipadne na 25. dubna.