



Historie matematiky a informatiky

Cvičení 2

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

2014



Evropský sociální fond
Investujeme do vaší budoucnosti

© Alena Šolcová

Číselně teoretické funkce

(Number-Theoretic Functions)

- Součet a počet dělitelů (The Sum and Number of Divisors)
- 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

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

Vlastnosti Möbiovy funkce

Příklad:

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

$$\begin{aligned} \mu(1) &= 1, & \mu(2) &= -1, & \mu(3) &= -1, \\ \mu(4) &= 0, & \mu(5) &= -1, & \mu(6) &= 1. \end{aligned}$$

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 $1, 2, 3, \dots, n$ 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,

$$\text{tj. } \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n),$$

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

- Necht' 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 $\text{nsd}(m, n) = d$

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

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

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

$$S_5 = \{5\}$$

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

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

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

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 $a + b \equiv c + d \pmod{n}$ 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 $2^{20} \equiv 81 \cdot 81 \pmod{41}$

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

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

Podle vlastností kongruence pokračujeme:

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

tedy 41 dělí $20^{20} - 1$.

Příklad - kongruence

- Chceme najít zbytek po dělení součtu $1! + 2! + 3! + 4! + \dots + 99! + 100!$ číslem 12.
- Zahájíme zjištěním, že $4! \equiv 24 \pmod{12}$, takže

Pro $k \geq 4$ platí

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

Takto dostaneme

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

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. $3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$.

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

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

na $5(-7) \equiv 5 \cdot 9 \pmod{8}$. Číslo 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, \dots, n_r kladná celá čísla taková, že
 $\text{nsd}(n_i, n_j) = 1$ pro $i \neq j$.

Pak soustava lineárních kongruencí

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

.

.

.

$$x \equiv a_r \pmod{n_r}$$

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

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:

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

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

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

$$21x \equiv 1 \pmod{5},$$

$$15x \equiv 1 \pmod{7},$$

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

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

Pro mod (105) dostáváme jediné řešení:

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

Zákon kvadratické reciprocity

(The Quadratic Reciprocity Law)

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

Kvadratické reziduum

- **Definice:** Necht' p je liché prvočíslo a $\text{nsd}(a, p) = 1$. 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 kritérium

Euler's Criterion

Věta: Necht' p je liché prvočíslo

a platí $\text{nsd}(a,p) = 1$,

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: Necht' p je liché prvočíslo a necht' $\text{nsd}(a, p) = 1$.

Legendrův symbol (a/p) je definován takto:

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

Příklady

- Příklad: Necht' $p = 13$. 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 necht' 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 $x^2 \equiv -46 \pmod{17}$?

$(-46/17) = (-1/17) (46/17) = (-1)^8 (12/17) = (3 \cdot 2^2/17) =$
 $= (3/17) (2^2/17) = (3/17) \equiv 3^8 \equiv 81^2 \equiv (-4)^2 = -1 \dots$ **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,

$$\text{pak } \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2}$$

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

pak

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

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 $p \neq 3$, 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 $p \equiv 2 \pmod{3}$. 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 – L3

Najděte všechna řešení kvadratické kongruence

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