Václav Šimerka
Řetězové pravidlo u shod

*Časopis pro pěstování mathematiky a fysiky*, Vol. 6 (1877), No. 5, 274--277

Persistent URL: http://dml.cz/dmlcz/121684

# Řetězové pravidlo u shod.

Podává

**Václav Šimerka.**

Shody téhož modulu $p$,

$$\begin{aligned} A &\equiv aB \\ B &\equiv bC \\ C &\equiv cD \\ &\vdots \\ M &\equiv mN \\ N &\equiv n \end{aligned}$$

v nichž $a$, $b$, $c$, ... $m$, $n$ jisté vlastnosti mají, které $B$, $C$, $D$ ... $M$, $N$ nemají, při čemž $A$ tedy i všechna ostatní čísla s $p$ nesoudělná jsou, dávají násobeny

$$ABC \ldots . MN \equiv abc \ldots mn \times BCD \ldots N$$

což zkráceno v

$$A \equiv abc \ldots mn$$

přechází, tak že tímto spůsobem ve velmi četných případech číslu $A$ jinou přiměřenou podobu dáti lze. Při tom ovšem patrno, že pravý člen poslední shody, jímžto se řetěz končí, pouze činitele předkem určeného druhu míti smí. Podoby $aB$, $bC$, $cD$, ..., $mN$ dávají se číslům $A$, $B$, $C$, ..., $M$ přičtením neb odejmutím násobného daného modulu neb jakýmkoli jiným spůsobem na př. v rozsáhlejších počtech ze známých výsledků.

Místo shodových znamení jest při tom záhodno dvě kolmice táhnouti; v levo podle první budou se čísla $A$, $B$, $C$ ..., psáti, mezi ně pro lepší přehled a uvarování omylů zbytky, které z nich povstaly co obyčejná čísla, a v pravo za druhou kolmici tytéž zbytky v podobách $aB$, $bC$, $cD$. Při tom jest dobře modul svrchu nad shody napsati. Jakých výhod toto velmi obecné pravidlo v neurčité analytice poskytuje, objasnětež následující příklady:

1. U modulu 61 má se řešiti shoda $2^x = 11$? Toho docílíme tím, že za $a$, $b$, $c$, ... budeme bráti pouze mocnosti z 2ky vyhýbajíce se zápornosti. Takto nalezneme:

$$\begin{array}{r|c|l} & \overset{\smile}{61} & \\ 11 & 72 & 2^3 \times 9 \\ 9 & 70 & 2 \times 35 \\ 35 & 96 & 2^5 \times 3 \\ 3 & 64 & 2^6 \end{array}$$

Protož bude $11 \equiv 2^3 \times 2 \times 2^5 \times 2^6$ čili $11 \equiv 2^{15}$, tedy $x = 15$.

2. Bylo-li by řešiti $x^2 \equiv 5 \pmod{151}$, třeba za $a$, $b$, $c$ bráti pouze čtverce, nic však nevadí, proč by se i záporných zbytků použíti nemohlo, jelikož se jeden záporný zbytek druhým záporným buď ruší, neb záporný činitel do levého členu přenésti může. Bude tedy

$$\begin{array}{r|c|l} & \overset{\smile}{151} & \\ 5 & 156 & 2^2 \times 39 \\ 39 & -112 & -4^2 \times 7 \\ -7 & 144 & 12^2 \end{array}$$

Z toho jde $5 \equiv 96^2 \equiv 55^2$, tedy $x \equiv 55$, jelikož se 55 a 96 do modulu doplňují, což ve shodách psáno dává

$$5 \equiv 96^2 \equiv (96 - 151)^2 \equiv (-55)^2 \equiv 55^2.$$

3. Má se číslu 7 u mod. 131 dáti podoba $2^x \times 3^y$. Zde budou opět $a$, $b$, $c$ mocnosti z 2ky a 3ky.

$$\begin{array}{r|c|l} & \overset{\smile}{131} & \\ 7 & 138 & 2 \times 3 \times 23 \\ 23 & 154 & 2 \times 77 \\ 77 & 208 & 2^4 \times 13 \\ 13 & 144 & 2^4 \times 3^2 \end{array}$$

Zde máme $7 \equiv 2^{10} \times 3^3$.

4. Mají se u mod. 1433 číslům kmenným 7, 11, 13, 17 dáti podoby $\pm 2^m \times 3^n \times 5^r$!

$$\begin{array}{r|c|l} & \overset{\smile}{1433} & \\ 7 & 1440 & 2^5 \times 3^2 \times 5; \end{array}$$

což dává $7 \equiv 2^5 \times 3^2 \times 5$

$$\begin{array}{r|c|l} 11 & -1422 & -2 \times 3^2 \times 79 \\ 79 & 1512 & 2^3 \times 3^3 \times 7 \\ 7 & . \ . & 2^5 \times 3^2 \times 5 \end{array}$$

z toho jde $11 \equiv -2^9 \times 3^7 \times 5$.

Dále obdržíme

$$\begin{array}{r|r|l} 13 & -1420 & -2^2 \times 5 \times 71 \\ 71 & 1504 & 2^5 \times 47 \\ 47 & -1386 & -2 \times 3^2 \times 77 \\ & 7 \times 11 & -2^{14} \times 3^9 \times 5^2 \end{array}$$

čili $13 \equiv -2^{22} \times 3^{11} \times 5^3$.

Poslední shoda plyne zde z obou předcházejících výsledků. Taktéž obdržíme

$$\begin{array}{r|r|l} 17 & 1450 & 2 \times 5^2 \times 29 \\ 29 & -1404 & -2^2 \times 3^3 \times 13 \\ & 13 & -22^2 \times 3^{11} \times 5^3 \end{array}$$

protož jest $17 \equiv 2^{24} \times 3^{14} \times 5$.

5. U mod. 4391 budiž číslo 107 v součin ze čtverce a prvočísel 2, 3, 5, 7!

$$\overset{4391}{\smile}$$

$$\begin{array}{r|r|l} 107 & -4284 & -6^2 \times 7 \times 17 \\ 17 & -4374 & -27^2 \times 2 \times 3 \end{array}$$

$$107 \equiv 2 \times 3 \times 7 \times 162^2.$$

6. Ukol 2. podává sice návod řešiti shodu $x^2 = a \pmod p$ čili rovnici $x^2 = py + a$, než při modulech poněkud větších jest velmi pracný. Tomu lze odpomoci jiným pravidlem, jež ale opět jiné vlastnosti čísla $a$ vyžaduje, při čemž řetězové pravidlo dobré služby konává. Takť se shoda $x^2 \equiv 3371 \pmod{8867}$ dá snadněji řešiti, nalezne-li se $3371 \equiv m^2 q$, při čemž by $q$ bylo $< 3371$ a buď kladné číslo kmenné z podoby $4\varphi + 1$ neb záporné z podoby $4\varphi + 3$.

Ohledně toho nalezneme

$$\overset{8867}{\smile}$$

$$\begin{array}{r|r|l} x^2 \equiv 3371 & 21105 & 3^2 \times 2345 \\ 2345 & 11212 & 2^2 \times 2803 \\ 2803 & -6064 & -4^2 \times 379 \end{array}$$

takže při $x^3 \equiv -24^2 \times 379$ přestati můžeme.

*Poznamenání.* Byť i pravidlo toto ve mnohých případech k žádoucímu cíli nevedlo buď proto, že s velikými čísly počítati vůbec obtížno jest, nebo že se v postupu mezi veličinami $A$, $B$, $C$, $D$, ... perioda objeví, nebývá předce počet marným; jelikož

výsledků takto nabytých u jiných pravidel s prospěchem použíti lze. Mimo to poukazuje též na důležitost číslového rozboru, totiž rozvrhování veličin v součiny z mocností, jichžto kořeny pouhá kmenná čísla jsou.

---

# Příspěvek k mocnění.

Podává

**J. M. Pastorček,**

posluchač II. roč. na české polytechnice.

Při praktickém mocnění čísel zvláštních dá se s výhodou upotřebiti známá věta:

$$[\Sigma(a)]^2 = \Sigma(a^2) + 2\Sigma(aa)$$

t. j. algebraický polynom na druhou mocnost povýšený může se vždy vyjádřiti součtem čtverců jednotlivých členů a dvojnásobným součtem ze všech možných součinů, kteréž si z daných členů co činitelů na spůsob *amb* tvoříme.

Měl by se podle hořejší rovnice smocniti dekadický polynom

$$\Sigma(a) = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_2 10^2 + a_1 10 + a_0$$

v němž $a_n$, $a_{n-1}$, $\ldots$, $a_2$, $a_1$, $a_0$ zastupují jednotlivé číslice, kdežto mocnosti z 10 udávají hodnoty jejich.

První součet $\Sigma(a^2)$ plyne přímo z daného čísla

$$\Sigma(a^2) = a_n^2 10^{2n} + a_{n-1}^2 10^{2(n-1)} + \ldots a_2^2 10^{2\cdot 2} + a_1^2 10^2 + a_0^2.$$

Pouhý pohled na tento tvar nás poučuje, že je to opět dekadický polynom, ale že se musí postupně čtvercům jednotlivých číslic dvě desetinná místa za sebou vytknouti.

Význam součtu druhého $\Sigma(aa)$ jest ten, že povstal sečtením takových součinů, které jsme si utvořili střídavým násobením vždy dvou nových členů. K těmto součinům nejsnadněji přijdeme podobným spůsobem, jakým si tvoříme z daných prvků amba a sice: utvoříme si napřed součin nejvyšší, tedy první číslice se všemi ostatními; pak se vytkne druhý člen za činitele a násobí se jím všechny členy vyjímaje první, tedy všechny za ním následující členy; třetí člen násobí se taktéž jen všemi za ním jdoucími atd.; konečný součin bude z posledního a předposledního členu.