František Josef Studnička
Základové nauky o číslech. [III.]

Časopis pro pěstování mathematiky a fysiky, Vol. 4 (1875), No. 5, 193--208

Persistent URL: http://dml.cz/dmlcz/121192

Základové nauky o číslech.

Podává

Dr. **F. J. Studnička.**

(Pokračování.)

§. 8.

O poučce Fermatově.

Jest-li a číslo nesoudělné s kmenným číslem p a zavedeme-li do vzorce (39)

$$n_1 = n_2 = n_3 = \ldots = n_a = 1,$$

obdržíme z něho ihned

$$Z\left(\frac{a^p}{p}\right) = Z\left(\frac{a}{p}\right),$$

aneb převedeme-li výraz z pravé strany na levou,

$$Z\left(\frac{a\,(a^{p-1}-1)}{p}\right) = 0,$$

z čehož jde podlé pravidla 1. o zbytcích dříve uvedeného, jelikož a, p jsou čísla nesoudělná,

$$Z\left(\frac{a^{p-1}-1}{p}\right) = 0, \qquad (47)$$

kteryžto vzorec vyjadřuje *poučku Fermatovu.*

Jiný jednoduchý, ale duchu této nauky méně přiměřený důkaz zakládá se na poučce binomické. Jak známo, jest

$$(a+1)^p = a^p + 1 + pQ,$$

aneb odečteme-li na obou stranách a a spojíme-li příslušně

$$(a+1)\,[(a+1)^{p-1}-1] - a\,(a^{p-1}-1) = pQ;$$

výraz na pravé straně jest dělitelný číslem p, musí tudíž i výraz na straně levé míti tuto vlastnost. A tu jest patrně pro $a = 1$

$$Z\left(2 . \frac{2^{p-1}-1}{p}\right) = 0 \quad \text{neb} \quad Z\left(\frac{2^{p-1}-1}{p}\right) = 0,$$

pro $a = 2$ tedy

$$Z\left(3 . \frac{3^{p-1}-1}{p}\right) = 0 \quad „ \quad Z\left(\frac{3^{p-1}-1}{p}\right) = 0,$$

. . . . . .

a tudíž všeobecně pro hodnotu a nesoudělnou s p

$$Z\left(\frac{a^{p-1}-1}{p}\right) = 0,$$

jako prvé.

Taktéž jednoduchý a zcela přiměřený důkaz plyne z poučky 6. o zbytcích jednající; jestli totiž

$$Z\left(\frac{a}{p}\right) = \alpha_1,$$

$$Z\left(\frac{2a}{p}\right) = \alpha_2,$$

$$\vdots$$

$$Z\left(\frac{(p-1)a}{p}\right) = \alpha_{p-1},$$

a znásobíme-li na obou stranách, bude patrně

$$Z\left(\frac{a^{p-1}(p-1)!}{p}\right) = \alpha_1 \alpha_2 \ldots \alpha_{p-1},$$

kdež ale součin zbytků ze známých příčin skládá se z nestejných faktorů $p-1$ menších nežli p a tudíž jest

$$\alpha_1 \alpha_2 \ldots \alpha_{p-1} = 1 . 2 . \ldots (p-1) = (p-1)!;$$

dosadíme-li tuto hodnotu do vzorce předešlého a převedeme-li zároveň výraz se strany pravé na levou, bude dále

$$Z\left(\frac{(a^{p-1}-1)(p-1)!}{p}\right) = 0,$$

z čehož jde, jelikož $(p-1)!$ a p jsou čísla nesoudělná,

$$Z\left(\frac{a^{p-1}-1}{p}\right) = 0.$$

Z této rovnice jde pak podle známého pravidla, vyjádřeného vzorcem (42),

$$Z\left(\frac{a^{n(p-1)}-1}{p}\right)=0, \tag{48}$$

což značí *rozšířenou rovnici Fermatovu.*

Není-li však p číslo kmenné, nýbrž složené a tudíž

$$p=a_1^{\alpha_1}\, a_2^{\alpha_2}\, a_3^{\alpha_3}\ldots a_n^{\alpha_n},$$

kdež značí $a_1, a_2, a_3, \ldots, a_n$ čísla kmenná, zjednejme si ze vzorce (47) napřed

$$Z\left(\frac{a^{a_1-1}-1}{a_1}\right)=0,$$

načež bude podlé vzorce (44)

$$Z\left(\frac{a^{(a_1-1)a_1^{\alpha_1-1}}}{a_1^{\alpha_1}}\right)=1$$

a tudíž i

$$Z\left(\frac{a^{(a_2-1)a_2^{\alpha_2-1}}}{a_2^{\alpha_2}}\right)=1$$

$$\vdots$$

$$Z\left(\frac{a^{(a_n-1\,a_n^{\alpha_n-1}}}{a_n^{\alpha_n}}\right)=1.$$

Zavedeme-li tu označení vzorce (30)

$$S_3(p)=\varphi=a_1^{\alpha_1-1}(a_1-1)\,a_2^{\alpha_2-1}(a_2-1)\ldots$$

a použijeme-li vzorce (48), kladouce pro rovnici

první $$n=\frac{\varphi}{(a_1-1)a_1^{\alpha_1-1}},$$

druhou $$n=\frac{\varphi}{(a_2-1)a_2^{\alpha_2-1}},$$

$$\vdots \qquad\qquad \vdots$$

n-tou $$n=\frac{\varphi}{(a_n-1)a_n^{\alpha_n-1}},$$

obdržíme z předcházející soustavy vzorců

$$Z\left(\frac{a^{\varphi}}{a_1^{\alpha_1}}\right)=1,$$

$$Z\left(\frac{a^{\varphi}}{a_2^{\alpha_2}}\right)=1,$$

$$\vdots$$

$$Z\left(\frac{a^{\varphi}}{a_n^{\alpha_n}}\right)=1$$

a tudíž použijeme-li pravidla 7. o zbytcích jednajícího, konečně

$$Z\left(\frac{a^{\varphi}}{a_1^{\alpha_1}, a_2^{\alpha_2}\ldots a_n^{\alpha_n}}\right)=1,$$

aneb což jest totéž, použijeme-li opět symbolu S_3,

$$Z\left(\frac{a^{S_3(p)}-1}{p}\right)=0.$$

A vzorec tento představuje Eulerem ponejprv odůvodněnou *všeobecnou poučku Fermatovu*,*) v níž jest obsažena poučka jednoduchá, vzorcem (47) vyjádřená; neb jestli p číslo kmenné, platí, jak dříve již bylo vytknuto, $S_3(p)=p-1$.

Ze vzorce (47) jde patrně

$$Z\frac{(a^{1/2(p-1)}-1)\,(a^{1/2(p-1)}+1)}{p}=0$$

aneb zkrátka $$Z\left(\frac{a^{1/2(p-1)}\mp 1}{p}\right)=0,$$

při čemž nutno rozhodnouti, kdy platí znamení svrchní, kdy spodní; uvážíme-li, že

$$Z\left(\frac{a}{p}\right)=\alpha_1,$$

*) Uveřejněna jest ponejprv ve „Fermatii opera math.“ Tolosae, 1679, pag. 163. bez důkazu. *Euler* dal první důkaz v Comm. Petrop. T. VIII., druhý v Nov. Comm. Petrop. T. VII., s nímž se v podstatě shoduje *Gaussův* důkaz v Disquis. arithm. pag. 50, v sebraných spisech Bd. I. pag. 41., kdežto první opakuje *Legendre* v „Théorie des nombres“ T. I. pag. 192. Již dříve dal *Lambert* zvláštní důkaz v „Acta erud.“ 1769, pak 109. a *Laplace*, jehož znění podáno v *Lacroix* „Traité du calc. diff. et int. T. III. pag. 722. Dva nové důkazy uveřejnil *Lejeune-Dirichlet* v Crellés Journ. T. III. pag. 390.

$$Z\left(\frac{2a}{p}\right) = \alpha_2,$$

$$\vdots$$

$$Z\left(\frac{{}^1/_2(p-1)a}{p}\right) = \alpha_{{}^1/_2(p-1)}$$

a vrátíme-li se k poslednímu způsobu, jakým byla poučka Fermatova vyvinuta, poznáme, nahradíme-li v řadě zbytků

$$\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{{}^1/_2(p-1)}$$

všech m, které jsou větší nežli ${}^1/_2(p-1)$, negativními menšími nežli ${}^1/_2(p-1)$, že se řada tato promění v

$$1, 2, 3, \ldots, {}^1/_2(p-1),$$

kdež bude m členů míti znamení — a tudíž bude součin

$$\alpha_1 \alpha_2 \ldots \alpha_{{}^1/_2(p-1)} = (-1)^m \left(\frac{p-1}{2}\right)!$$

a za tou příčinou bude tedy

$$Z\left(\frac{a^{{}^1/_2(p-1)} - (-1)^m}{p}\right) = 0, \qquad (50)$$

kterýžto vzorec jest nanejvýš důležitým pro nauku o zbytcích kvadratických.

Podlé toho obdržíme na př. místo

$$Z\left(\frac{6^{10}-1}{11}\right) = 0,$$

kde $a = 6$, $p = 11$ a tudíž prvních 5 zbytků

$$\alpha_1 = 6, \quad \alpha_2 = 1, \quad \alpha_3 = 7, \quad \alpha_4 = 2, \quad \alpha_5 = 8,$$

$$Z\left(\frac{6^5+1}{11}\right) = 0,$$

poněvadž tu $\alpha_1 > 5$, $\alpha_3 > 5$, $\alpha_5 > 5$ a tudíž $m = 3$.

§. 9.

O poučce Wilsonově a souvislosti její s poučkon Fermatovou.

Zavedeme-li do vzorce (46)

$$f(x) = x^{p-1} - 1,$$

kdež značí p číslo kmenné, a vedlé toho

$$\alpha_k = k\,,$$

takže podlé poučky Fermatovy tu jest

$$Z\left(\frac{\alpha_k^{p-1}-1}{p}\right) = Z\left(\frac{f(\alpha_k)}{p}\right) = 0,$$

obdržíme především

$$x^{p-1}-1 = (x-1)(x-2)\ldots(x-p+1)+pQ,$$

a tudíž porovnáme-li stálé členy na obou stranách a považíme-li, že součin na pravé straně skládá se ze *sudého* počtu faktorů,

$$-1 = (p-1)!+pQ_0\,,$$

z čehož jde konečně

$$Z\left(\frac{(p-1)!+1}{p}\right) = 0, \qquad (51)$$

kteryžto vzorec představuje *poučku Wilsonovu.*

Sestavíme-li tedy z prvků

$$1,\ 2,\ 3,\ \ldots,\ p-1,$$

kdež značí p číslo kmenné, součin neb kombinaci $(p-1)$ní třídy a přidáme-li k součinu tomuto 1, obdržíme číslo dělitelné číslem p; jest to zvláštní případ, který platí jen o této kombinaci, kdežto všechny ostatní jsou samy o sobě číslem p dělitelny. Nejlépe poznáme tuto okolnost, vyvineme-li poučku Wilsonovu spůsobem Lagrange-ovým, který jest všeobecnější, ač méně přiměřený.

Rozvineme-li fakultu

$$(x+1)^{p-1,1} = (x+1)(x+2)(x+3)\ldots(x+p-1)$$

podlé mocnin veličiny x, obdržíme všeobecně

$$(x+1)^{p-1,1} = x^{p-1}+C_1x^{p-2}+C_2x^{p-3}+\ldots+C_{p-1},$$

kdež značí C_k neurčité koëfficienty, o nichž však víme, že C_k jest součet kombinací z prvků dříve vytknutých po k činitelích; znásobíme-li tento vzorec s $(x+p)$, obdržíme

$$(x+1)^{p,1} = (x+p)[x^{p-1}+C_1x^{p-2}+\ldots+C_{p-1}]$$

a píšeme-li v něm $x+1$ za x a znásobíme-li pak s $(x+1)$, taktéž

$$(x+1)^{p,1} = (x+1)[(x+1)^{p-1}+C_1(x+1)^{p-2}+\ldots+C_{p-1}];$$

porovnáme-li konečně v těchto sobě rovných výrazech koëfficienty stejně vysokých mocnin, dejme tomu mocniny $(p-i-1)$ní, obdržíme

$$(i-1)\,C_{i-1} = \binom{p}{i} + \binom{p-1}{i-1} C_1 + \binom{p-2}{i-2} C_2 + \ldots$$
$$\ldots + \left(\frac{p-i+2}{2}\right) C_{i-2} \qquad (52)$$

Jak z výrazu tohoto patrno, ustanoveny jsou neurčité koëfficienty C_k rekurrentně*) pomocí binomických koëfficientů a sice tu jest

$$C_1 = \binom{p}{2},$$
$$2\,C_2 = \binom{p}{3} + \binom{p-1}{2} C_1,$$
$$3\,C_3 = \binom{p}{4} + \binom{p-1}{3} C_1 + \binom{p-2}{2} C_2 \qquad (53)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Poněvadž p jest číslo kmenné a tudíž, jak známo, každý binomický koëfficient $\binom{p}{i}$ jest tímto číslem dělitelný, musí i pro $k = 1, 2, 3 \ldots (p-2)$ býti

$$Z\left(\frac{C_k}{p}\right) = 0; \qquad (54)$$

jest-li však ve vzorci (52) $i = p$ a tudíž

---

*) Neodvisle ustanovují se podle vzorce

$$(i-1)!\,C_{i-1} = \begin{vmatrix} \binom{p}{2}, & -1, & 0, & \ldots, & 0 \\ \binom{p}{3}, & \binom{p-1}{2}, & -2, & \ldots, & 0 \\ \binom{p}{4}, & \binom{p-1}{3}, & \binom{p-2}{2}, & \ldots, & 0 \\ \vdots & & & & \\ \binom{p}{i}, & \binom{p-1}{i-1}, & \binom{p-2}{i-2}, & \ldots, & \binom{p-i+1}{2} \end{vmatrix},$$

o čemž snadno se přesvědčíme, vyloučíme-li ze soustavy vzorců (53) příslušných všechny střední C, při čemž determinant soustavy se bude rovnati 0 a po rozkladu dá tvar tuto uvedený.

$$(p-1)\,C_{p-1} = 1 + C_1 + C_2 + \ldots + C_{p-2},$$

tož patrno, že podlé vzorce (54) jest

$$Z\left(\frac{(p-1)\,C_{p-1}}{p}\right) = Z\left(\frac{pC_{p-1} - C_{p-1}}{p}\right) = 1,$$

neb odstraníme-li člen číslem p dělitelný, že

$$Z\left(\frac{-C_{p-1}}{p}\right) = 1, \text{ neb } Z\,\frac{(p-1)!+1}{p} = 0, \qquad (55)$$

což se shoduje úplně se vzorcem (51).

Jak patrno, činí Wilsonova poučka výminku v pravidle vzorcem (54) vyjádřeném; všechny kombinace prvků dříve vytknutých dají čísla dělitelná číslem p, jen nejvyšší nutno doplniti jednotkou, aby měla tutéž vlastnost. Jestli na př. $p = 5$, bude

$C_1 = 1 + 2 + 3 + 4 = 5 \,.\, 2$
$C_2 = 1 \,.\, 2 + 1 \,.\, 3 + 1 \,.\, 4 + 2 \,.\, 3 + 2 \,.\, 4 + 3 \,.\, 4 = 5 \,.\, 7$
$C_3 = 1 \,.\, 2 \,.\, 3 + 1 \,.\, 2 \,.\, 4 + 1 \,.\, 3 \,.\, 4 + 2 \,.\, 3 \,.\, 4 = 5 \,.\, 10$
$C_4 = 1 \,.\, 2 \,.\, 3 \,.\, 4 = 5 \,.\, 5 - 1.$

Vrátíme-li se k stejnině původní a uvedeme-li ji na tvar

$$(x+1)^{p-1,1} - x^{p-1} + 1 = C_1\,x^{p-2} + \ldots\,(C_{p-1} + 1),$$

poznáme, použijeme-li vzorce (54) a (55), že výraz na pravé straně jest číslem p dělitelný, z čehož jde, že totéž platí i o výrazu na straně levé, takže i

$$Z\left[\frac{(x+1)^{p-1,1} - x^{p-1} + 1)}{p}\right] = 0, \qquad (56)$$

což vyjadřuje Wilsonovu poučku Lagrangem rozšířenou.

Jestli tu konečně $x > 0$ a značí-li zároveň x a p čísla nesoudělná, tedy

$$Z\left(\frac{x}{p}\right) = p - p'.$$

tedy $x = mp + p - p'$ neb $x + p' = p\,(m+1)$,
poznáváme, že i fakulta

$$(x+1)^{p-1,1} = (x+1)\,(x+2)\ldots(x+p')\ldots(x+p-1)$$

jest číslem p dělitelna, poněvadž obsahuje faktor $x + p'$, načež ze vzorce (56) jde, odstraníme-li člen dělitelný a obrátíme-li znamení,

$$Z\left(\frac{x^{p-1}-1}{p}\right)=0,$$

což vyjadřuje poučku Fermatovu.

Jak z tohoto pochodu Lagrange-ova jde na jevo, vyvine se napřed všeobecná poučka (54), kteráž platí pro $i<p-1$; na základě této poučky přijde se k výmince pro $i=p-1$, kteráž představuje poučku Wilsonovu, načež se obdrží pomocí obou rozšířená poučka Lagrange-Wilsonova, z níž co zvláštní případ plyne poučka Fermatova. *)

§. 10.

O shodnosti čísel.

Dělíme-li čísla a, b číslem m a obdržíme-li v obou případech tentýž zbytek α, jestli tedy

$$Z\left(\frac{a}{m}\right)=Z\left(\frac{b}{m}\right), \qquad (57)$$

jsou čísla a, b *podlé* m *stejného zbytku*, v kterémžto případě slují *shodná* neb *kongruentní* podlé čísla m, zvaného *míra* neb *modul.*

Vzorec (57) praví tedy též, že

$$Z\left(\frac{a-b}{m}\right)=Z\left(\frac{b-a}{m}\right)=0,$$

což se podlé *Gausse* vyznačuje symbolem

$$a\equiv b \pmod{m} \qquad (58)$$

a čte „(číslo) a *shoduje se* s (číslem) b *dle míry* (modulu) m“, při čemž výraz (58) sluje *shoda* neb *kongruence.*

Podlé toho jest na př.

$$Z\left(\frac{17}{5}\right)=Z\left(\frac{22}{5}\right)$$

neb $17\equiv 22 \pmod{5}$,

jelikož

$$\frac{17-22}{5}=-1.$$

*) Poučka Wilsonova jmenuje se podlé Angličana *Johna Wilsona*, a vyskytuje se ponejprv ve *Waringových* „Meditationes algebraicae“ Ed. 3. pag. 380. Zvláštní důkazy podali *Lagrange* „Mém. de Berlin“, 1771, pag. 125, *Euler* „Opuscula analytica“ Tom. I. pag. 329 a m. j.

Jak z tohoto výměru shodnosti patrno, možná všechny vzorce §. 7. psáti též co shody, jako na př.

$$Z\left(\frac{a}{p}\right)=0 \text{ jest } a\equiv 0 \pmod{p}$$

$$Z\left(\frac{a}{p}\right)=\alpha \text{ jest } a\equiv \alpha \pmod{p}$$

$$Z\left(\frac{a^{p-1}-1}{p}\right)=0 \text{ jest } a^{p-1}\equiv 1 \pmod{p}\text{*) atd.}$$

Shody mají velmi mnoho zajímavých vlastností, jichž se při rozmanitých příležitostech s velikým prospěchem užívá; pročež sestaveny jsou tuto nejdůležitější z nich spůsobem dvojím vedlé sebe, i podlé vzorce (57) i podlé vzorce (58) vyjádřeny, aby se zároveň poznalo, který spůsob psaní jest v kterém případě výhodnější.

1. Vyhovují-li a, b, m podmínce

$$Z\left(\frac{a}{m}\right)=Z\left(\frac{b}{m}\right), \quad | \quad a\equiv b \pmod{m},$$

bude zajisté i podlé významu tohoto symbolu

$$Z\left(\frac{b}{m}\right)=Z\left(\frac{a}{m}\right). \quad | \quad b\equiv a \pmod{m}.$$

2. Platí-li současně

$$Z\left(\frac{a}{m}\right)=Z\left(\frac{h}{m}\right), \quad | \quad a\equiv h \pmod{m},$$

$$Z\left(\frac{b}{m}\right)=Z\left(\frac{h}{m}\right), \quad | \quad b\equiv h \pmod{m},$$

bude zajisté i

$$Z\left(\frac{a}{m}\right)=Z\left(\frac{b}{m}\right), \quad | \quad a\equiv b \pmod{m},$$

3. Značí-li p a q čísla celistvá a jestli

$$Z\left(\frac{a}{m}\right)=Z\left(\frac{b}{m}\right), \quad | \quad a\equiv b \pmod{m},$$

jest patrně též

*) Podlé toho vyznačiti lze

číslo *sudé* buď tvarem $Z\left(\frac{n}{2}\right)=0$ neb $n\equiv 0 \pmod 2$,

„ *liché* „ „ $Z\left(\frac{n}{2}\right)=1$ „ $n\equiv 1 \pmod 2$.

$$Z\left(\frac{a+pm}{m}\right) = Z\left(\frac{b+qm}{m}\right), \qquad a + pm \equiv b + qm \pmod{m};$$

zbytek se nemění, přičteme-li k dělencům multiplum dělitele.

shoda se neruší, přičteme-li k shodným číslům multiplum modulu.

Že p neb q mohou býti též negativní neb 0, netřeba zvláště uváděti.

4. Značí-li p číslo celistvé a jestli

$$Z\left(\frac{a}{m}\right) = Z\left(\frac{b}{m}\right), \qquad a \equiv b \pmod{m},$$

jest patrno, že i

$$Z\left(\frac{ap}{m}\right) = Z\left(\frac{bp}{m}\right); \qquad ap \equiv bp \pmod{m},$$

zbytek se nemění, znásobíme-li dělence stejným číslem celistvým.

shoda se neměni, znásobímc-li čísla shodná stejným číslem celistvým.

5. Jestli však naopak

$$Z\left(\frac{ap}{m}\right) = Z\left(\frac{bp}{m}\right), \qquad ap \equiv pb \pmod{m}$$

platí jen pro *nesoudělné* m a p

$$Z\left(\frac{a}{m}\right) = Z\left(\frac{b}{m}\right), \qquad a \equiv b \pmod{m};$$

dělence možná děliti jen číslem nesoudělným s dělitelem.

oba členy shody možná děliti jen číslem nesoudělným s modulem.

Neb kdyby p a m byla čísla soudělná a tudíž

$$m = \alpha s, \; p = \alpha r,$$

kdež r a s jsou čísla nesoudělná, bylo by

$$Z\left(\frac{ar}{s}\right) = Z\left(\frac{br}{s}\right)$$

a tudíž podlé známého pravidla jen

$$Z\left(\frac{a}{s}\right) = Z\left(\frac{b}{s}\right). \qquad a \equiv b \pmod{s},$$

Na př. máme patrně

$$Z\left(\frac{33}{6}\right) = Z\left(\frac{21}{6}\right), \quad | \quad 33 \equiv 21 \pmod 6,$$

dělíme-li však 3, nebude

$$Z\left(\frac{11}{6}\right) = Z\left(\frac{7}{6}\right), \quad | \quad 11 \equiv 7 \pmod 6,$$

nýbrž $$Z\left(\frac{11}{2}\right) = Z\left(\frac{7}{2}\right). \quad | \quad 11 \equiv 7 \pmod 2.$$

6. Jestli v některém případě

$$Z\left(\frac{a}{pq}\right) = Z\left(\frac{b}{pq}\right), \quad | \quad a \equiv b \pmod{pq},$$

bude nutně i

$$Z\left(\frac{a}{p}\right) = Z\left(\frac{b}{p}\right), \quad | \quad a \equiv b \pmod p$$

a $$Z\left(\frac{a}{q}\right) = Z\left(\frac{b}{q}\right), \quad | \quad a \equiv b \pmod q,$$

což bez důkazu snadno se poznává a i na více dělitelů dá rozšířiti.

Jest-li však naopak

$$Z\left(\frac{a}{p}\right) = Z\left(\frac{b}{p}\right) \quad | \quad a \equiv b \pmod p$$

$$Z\left(\frac{a}{q}\right) = Z\left(\frac{b}{q}\right), \quad | \quad a \equiv b \pmod q,$$

platí jen tehdáž

$$Z\left(\frac{a}{pq}\right) = Z\left(\frac{b}{pq}\right) \quad | \quad a \equiv b \pmod{pq},$$

značí-li p a q čísla *nesoudělná*, jakž snadno možná odůvodniti a i na více dělitelů nesoudělných rozšířiti.

7. Z rovnic neb shod

$$Z\left(\frac{a}{m}\right) = Z\left(\frac{b}{m}\right) \quad | \quad a \equiv b \pmod m,$$

$$Z\left(\frac{c}{m}\right) = Z\left(\frac{d}{m}\right) \quad | \quad c \equiv d \pmod m$$

jde patrně, sečteme-li neb odečteme-li,

$$Z\left(\frac{a \pm c}{m}\right) = Z\left(\frac{b \pm d}{m}\right) \quad \Big| \quad a \pm c \equiv b \pm d \pmod{m}$$

a znásobíme-li

$$Z\left(\frac{ac}{m}\right) = Z\left(\frac{bd}{m}\right); \quad \Big| \quad ac \equiv bd \pmod{m};$$

pro $a = c$, $b = d$ bude tudíž

$$Z\left(\frac{a^2}{m}\right) = Z\left(\frac{b^2}{m}\right) \quad \Big| \quad a^2 \equiv b^2 \pmod{m}$$

a podlé toho i všeobecně pro celistvé a positivní n

$$Z\left(\frac{a^n}{m}\right) = Z\left(\frac{b^n}{m}\right), \quad \Big| \quad a^n \equiv b^n \pmod{m}, \qquad (59)$$

jakž možná dokázati rozmanitým spůsobem. Jestli totiž s jedné strany

$$\left.\begin{array}{lll} Z\left(\frac{a_1}{m}\right) = Z\left(\frac{b_1}{m}\right), & \Big| & a_1 \equiv b_1 \\ Z\left(\frac{a_2}{m}\right) = Z\left(\frac{b_2}{m}\right), & \Big| & a_2 \equiv b_2 \\ \vdots \qquad\qquad\quad \vdots & & \vdots \\ Z\left(\frac{a_n}{m}\right) = Z\left(\frac{b_n}{m}\right), & \Big| & a_a \equiv b_n \end{array}\right\} \pmod{m},$$

obdržíme, znásobíme-li na obou stranách,

$$Z\left(\frac{a_1 a_2 \ldots a_n}{m}\right) = Z\left(\frac{b_1 b_2 \ldots b_n}{m}\right), \Big| \; a_1 a_2 \ldots a_n \equiv b_1 b_2 \ldots b_n \pmod{m},$$

a z tohoto všeobecného vzorce pro

$$a_1 = a_2 = \ldots = a_n = a,$$
$$b_1 = b_2 = \ldots = b_n = b$$

vzorec (59); jestli pak s druhé strany

$$Z\left(\frac{a}{m}\right) = Z\left(\frac{b}{m}\right), \quad \Big| \quad a \equiv b \pmod{m},$$

což značí totéž jako rovnice

$$a = b + mp,$$

uveďme na obou stranách na $n$tou mocninu, načež obdržíme

$$a^n = b^n + m\,P,$$

kdež význam čísla P jest patrný, načež bude opět $(a^n - b^n)$ dělitelno číslem m, což vyznačuje vzorec (59); konečně budiž poznamenáno, že

$$a^n - b^n = (a - b)\,(a^{n-1} + \ldots + b^{n-1}),$$

z čehož jasně jde souvislost předešlých dvou vzorců na jevo.

8. Značí-li tedy $f(x)$ celistvou rationální algebraickou funkci tvaru

$$f(x) = Ax^m + Bx^n + Cx^p + \ldots,$$

kdež $A, B, C, \ldots$ jsou čísla celistvá, a platí-li tu

$$Z\left(\frac{a}{m}\right) = Z\left(\frac{b}{m}\right), \quad \Big| \; a \equiv b \pmod{m},$$

platí zároveň podlé pouček předcházejicích

$$Z\left(\frac{f(a)}{m}\right) = Z\left(\frac{f(b)}{m}\right). \quad \Big| \; f(a) \equiv f(b) \pmod{m}.$$

9. Jestli dále

$$Z\left(\frac{a}{p^n}\right) = Z\left(\frac{b}{p^n}\right), \quad \Big| \; a \equiv b \pmod{p^n},$$

což značí podlé předešlého, že

$$a = b + mp^n,$$

obdržíme, uvedeme-li na mocninu $p$tou,

$$a^p = b^p + p^{n+1}Q,$$

kdež význam veličiny Q jest patrný; i bude tudíž

$$Z\left(\frac{a^p}{p^{n+1}}\right) = Z\left(\frac{b^p}{p^{n+1}}\right); \quad \Big| \; a^p \equiv b^p \pmod{p^{n+1}};$$

opakujeme-li pak toto pravidlo αkráte, bude všeobecně

$$Z\left\{\frac{a^{p^\alpha}}{p^{n+\alpha}}\right\} = Z\left\{\frac{b^{p^\alpha}}{p^{n+\alpha}}\right\}, \quad \Big| \; a^{p^\alpha} \equiv b^{p^\alpha} \pmod{p^{n+\alpha}},$$

z čehož jde, položíme-li $n = 1$,

$$Z\left\{\frac{a^{p^\alpha}}{p^{\alpha+1}}\right\} = Z\left\{\frac{b^{p^\alpha}}{p^{\alpha+1}}\right\} \quad \Big| \quad a^{p^\alpha} \equiv b^{p^\alpha} \pmod{p^{\alpha+1}}$$

což souhlasí se vzorcem (43) pro $b = 1$.

10. Jestli současně

$$a \equiv b \pmod{P}, \quad a \equiv b \pmod{Q},$$

kdež jest

$$P = p^\alpha q^b r^c s^d \ldots$$
$$Q = p^\alpha q^\beta r^\gamma s^\delta \ldots,$$

při čemž značí $p, q, r, s \ldots$ čísla kmenná, a platí-li zároveň

$$a > \alpha, \quad b < \beta, \quad c > \gamma, \quad d < \delta, \ldots$$

takže tu největší společnou mírou čísel P a Q jest

$$m = p^\alpha q^b r^\gamma s^d \ldots,$$

pak jde z daných shod neb kongruencí

$$a^m \equiv b^m \pmod{PQ}.$$

Neb především se z nich obdrží

$$a \equiv b \pmod{p^\alpha},$$
$$a \equiv b \pmod{q^\beta},$$
$$a \equiv b \pmod{r^c},$$
$$a \equiv b \pmod{s^\delta},$$
$$\ldots\ldots$$

na to podlé pravidla předešlého

$$a^{p^\alpha} \equiv b^{p^\alpha} \pmod{p^{a+\alpha}},$$
$$a^{q^b} \equiv b^{q^b} \pmod{q^{b+\beta}},$$
$$a^{r^\gamma} \equiv b^{r^\gamma} \pmod{r^{c+\gamma}},$$
$$a^{s^d} \equiv b^{s^d} \pmod{s^{d+\delta}},$$
$$\ldots\ldots\ldots.$$

dále pak uvedením první shody na mocninu $q^b r^\gamma s^d \ldots$,

druhé „ „ „ $p^\alpha r^\gamma s^d \ldots$,

třetí „ „ „ $p^\alpha q^b s^d \ldots$,

čtvrté „ „ „ $p^\alpha q^b r^\gamma \ldots$,

. . . . . .

a dosazením čísla m

$$a^m \equiv b^m \pmod{p^{a+\alpha}},$$

$$a^m \equiv b^m \pmod{q^{b+\beta}},$$

$$a^m \equiv b^m \pmod{r^{c+\gamma}},$$

$$a^m \equiv b^m \pmod{b^{d+\delta}},$$

. . . . . .,

z čehož jde konečně, poněvadž jsou p, q, r, s ... čísla kmenná.

$$a^m \equiv b^m \pmod{p^a q^b r^c \ldots p^\alpha q^\beta r^\gamma}$$

aneb podlé významu čísla P a Q

$$a^m \equiv b^m \pmod{PQ},$$

jakž bylo s počátku praveno.

Jestli pak ve zvláštním případě Q obsaženo v P, a jestli tudíž číslo Q samo největší společnou mírou, bude

$$a^Q \equiv b^Q \pmod{PQ}.$$

Jestli tedy na př.

$$25 \equiv 1 \pmod{12},$$

bude podlé tohoto pravidla též

$$25^4 \equiv 1 \pmod{96},$$

poněvadž 4 jest největší společnou mírou čísel 12 a 8.

(Pokračování.)