Základové nauky o číslech.

Podává

Dr. F. J. Studnička.

(Pokračování.)

Př. 3. Chceme-li znáti pravidlo dělitelnosti pro 9 a 11, položme

$$n = 1, \quad A = 10^2 = 100, \quad r = 1,$$

poněvadž

$$100 = 9 \,.\, 11 + 1,$$

načež obdržíme ze vzorce (15)

$$R_1 = x_0 + x_1 + x_2 + x_3 + \ldots$$

kdež značí x_k třídu dvojčíselnou; *číslo dekadické jest tedy dělitelno buď 9 neb 11, je-li součet tříd dvojčíselných dělitelný tímto číslem některým*; v opačném případě platí rovnice (16).

Podlé toho jest tedy číslo

$$N = 23|14|76|96$$

dělitelno číslem 11, poněvadž tu

$$Z\left(\frac{96+76+14+23}{11}\right) = Z\left(\frac{209}{11}\right) = 0.$$

Poznámka. A poněvadž x_k může představovati číslo větší nežli 9 neb 11, postačí, když místo součtu tříd dvojčíselných položíme součet zbytků těchto tříd podle 9 neb 11, takže místo R_1 tu bude rozhodovati

$$R' = Z\left(\frac{x_0}{p}\right) + Z\left(\frac{x_1}{p}\right) + Z\left(\frac{x_2}{p}\right) + \ldots$$

V předcházejícím příkladě máme tudíž

$$Z\left(\frac{23}{11}\right)+Z\left(\frac{14}{11}\right)+Z\left(\frac{76}{11}\right)+Z\left(\frac{96}{11}\right)=1+3-1-3=0.$$

z čehož plyne taktéž dělitelnost číslem 11.

Př. 4. Poněvadž pro 9 známe jednodušší pravidlo, nežli jest předcházející, bude prospěšno i pro 11 vyhledati podobné, což plyne z podmínky

$$n=1, \quad A=10, \quad r=-1,$$

poněvadž

$$10=1.11-1;$$

ze vzorce (15) obdrží se pak

$$R_1=x_0-x_1+x_2-x_3+\ldots$$

z čehož jde, že *číslo dekadické jest* 11 *dělitelno, je-li tímto číslem dělitelný rozdíl součtů čísel na sudých a lichých místech stojících*; v opačném případě platí pak rovnice (16).

Pro číslo dříve uvedené tu bude

$$Z\left(\frac{6+6+4+3-9-7-1-2}{11}\right)=0.$$

Př. 5. Abychom vyšetřili dělitelnosti pravidlo pro čísla 27 a 37, považme, že

$$27.37=999=1000-1,$$

a položme tudíž

$$n=1, \quad A=10^3=1000, \quad r=1,$$

načež obdržíme ze vzorce (15)

$$R_1=x_0+x_1+x_2+x_3+\ldots,$$

kdež značí x_k číslo trojčíselné; *dekadické číslo jest tedy dělitelno* 27 *neb* 37, *jestli tímto číslem některým dělitelný součet tříd trojčíselných*; v opačném případě platí rovnice (16).

Podle toho jest číslo

$$N=355|597|402|237$$

dělitelno číslem 37, poněvadž tu

$$Z\left(\frac{237+402+597+355}{37}\right)=0.$$

A podlé předcházející poznámky bychom měli

$$Z\left(\frac{237}{37}\right)=+15,$$

$$Z\left(\frac{402}{37}\right) = -\ 5,$$

$$Z\left(\frac{597}{37}\right) = +\ 5,$$

$$Z\left(\frac{355}{37}\right) = -15,$$

tudíž součet zbytků 0, z čehož plyne taktéž dělitelnost číslem 37.

Př. 6. Abychom vyšetřili pravidlo dělitelnosti pro 17, položme

$$n = 5, \quad A = 10, \quad r = -1,$$

poněvadž

$$5 \, . \, 10 = 3 \, . \, 17 - 1,$$

načež obdržíme ze vzorce (14)

$$\pm R = x_m - 5x_{m-1} + 5^2 x_{n-2} - 5^3 x_{m-3} + \ldots;$$

výraz tento stane se jednodušším, zavedeme-li místo součinitele 5^k pouze zbytek

$$Z\left(\frac{5^k}{17}\right) = r_k < 17,$$

načež obdržíme bez ohledu na znamení

$$R = x_m - 5x_{m-1} + 8x_{m-2} - 6x_{m-3} + \ldots;$$

ale i tento výraz možná ještě zjednodušiti, použijeme-li i zbytků negativních, kladouce tam, kde

$$r_k > 8, \quad Z\left(\frac{5^k}{17}\right) = r_k - 17,$$

načež absolutní hodnota žádného zbytku nepřevýší polovici čísla 17 neb vlastně 8 a tudíž pomocí těchto *nejmenších* zbytků se obdrží

$$\begin{aligned} R = x_0 & - 7x_1 - 2x_2 - 3x_3 + 4x_4 + 6x_5 - 8x_6 + 5x_7 \\ & - x_8 + 7x_9 + 2x_{10} + 3x_{11} - 4x_{12} - 6x_{13} + 8x_{14} - 5x_{15} \\ & + x_{16} - \ldots . \end{aligned}$$

Poněvadž tu x_k značí číslice soustavy desetinné, usnadní se vyšetřování tohoto výrazu, sestavíme-li si pro jednotlivé číslice a pro jednotlivá místa, na nichž mohou státi, příslušné zbytky nejmenší, což možná snadno provésti, uváží-li se, že se tu nevyskytuje více nežli 8 absolutně rozličných zbytků; určíme-li si tedy těchto 8 zbytků pro jednotku, pak je cyklickou záměnou obdržíme i pro číslice ostatní. A tu jest pro jednotku na *prvním* místě

$$Z\left(\frac{1}{17}\right) = 1,$$

na *druhém* desetkrát tolik, tedy 10 neb — 7, na *třetím* desetkrát tolik co na druhém, tedy — 70 neb — 2, podobně na

$$\textit{čtvrtém} \quad Z\left(\frac{-20}{17}\right) = -3,$$

$$\textit{pátém} \quad Z\left(\frac{-30}{17}\right) = +4,$$

$$\textit{šestém} \quad Z\left(\frac{40}{17}\right) = +6,$$

$$\textit{sedmém} \quad Z\left(\frac{60}{17}\right) = -8,$$

$$\textit{osmém} \quad Z\left(\frac{-80}{17}\right) = +5,$$

$$\textit{devátém} \quad Z\left(\frac{50}{17}\right) = -1,$$

čímž jsme se octli opět při zbytku prvním, nepřihlížíme-li k jeho označení.

Napíšeme-li pak řadu těchto zbytků do kola takto:

$$\begin{array}{ccccc} & & \pm 1 & & \\ & \pm 5^* & & \mp 7 & \\ \mp 8 & & \mathbf{17} & & \mp 2 \\ & \pm 6 & & \mp 3 & \\ & & \pm 4 & & \end{array}$$

obdržíme zbytky pro číslo 2, 3, 4, ... na druhém, třetím, čtvrtém ... místě, jdeme-li od $+2$, $+3$, $+4$, ... v kruhu tomto směrem ručičky hodinové a klademe-li u následujících členů znamení buď svrchní neb spodní podle toho, kde stálo první $+$; mezi 5 a 1 značí konečně * skok od znamení svrchního k spodnímu neb naopak. Budou tedy zbytky

pro 2: $+2, +3, -4, -6, +8, -5, +1, -7, -2, \ldots$
„ 3: $+3, -4, -6, +8, -5, +1, -7, -2, -3, \ldots$
„ 4: $+4, +6, -8, +5, -1, +7, +2, +3, -4, \ldots$
. . . . ,

takže nyní snadno sestavíme si pro prvních 10 míst schema toto:

Místo	1	2	3	4	5	6	7	8	9
1	+1	+2	+3	+4	+5	+6	+7	+8	−8
2	−7	+3	−4	+6	−1	−8	+2	−5	+5
3	−2	−4	−6	−8	+7	+5	+3	+1	−1
4	−3	−6	+8	+5	+2	−1	−4	−7	+7
5	+4	+8	−5	−1	+3	+7	−6	−2	+2
6	+6	−5	+1	+7	−4	+2	+8	−3	+3
7	−8	+1	−7	+2	−6	+3	−5	+4	−4
8	+5	−7	−2	+3	+8	−4	+1	+6	−6
9	−1	−2	−3	−4	−5	−6	−7	−8	+8
10	+7	−3	+4	−6	+1	+8	−2	+5	−5

Jak patrno, jsou tu zbytky v sloupci osmém a devátém jakož i řádku prvním a devátém bez ohledu na znamení stejné.

Majíce toto schema před sebou, snadno rozhodneme, zdali některé číslo jest dělitelno číslem 17 a jaký zbytek poskytuje v případě opačném; třebať jen pro jednotlivé číslice jeho sestaviti příslušné zbytky a součet jich R pak rozhodne: jestli totiž

$$Z\left(\frac{R}{17}\right) = 0,$$

jest číslo též dělitelno 17, jestli však

$$Z\left(\frac{R}{17}\right) = \alpha,$$

jest α i zbytek povstávající dělením čísla tohoto číslem 17.

Poněvadž podlé toho poskytuje číslo

$$N = 50370609$$

pro 9	na	prvním	místě zbytek	-8,
„ 6	„	třetím	„ „	$+5$,
„ 7	„	pátém	„ „	-6,
„ 3	„	šestém	„ „	$+1$,
„ 5	„	osmém	„ „	$+8$,

tedy $R = 0$, z čehož jde, že jest dělitelno číslem 17.

Podobným spůsobem bychom mohli sestaviti pro 19

$$R = x_0 - 9x_1 + 5x_2 - 7x_3 + 6x_4 + 3x_5 - 8x_6 - 4x_7 - 2x_8 - x_9 + 9x_{10} - 5x_{11} + 7x_{12} - 6x_{13} - 3x_{14} + 8x_{15} + 4x_{16} + 2x_{17} + x_{18} - \dots$$

a příslušné schema pro zbytky

Místo	1	2	3	4	5	6	7	8	9
1	+1	+2	+3	+4	+5	+6	+7	+8	+9
2	−9	+1	−8	+2	−7	+3	−6	+4	−5
3	+5	−9	−4	+1	+6	−8	−3	+2	+7
4	−7	+5	−2	−9	+3	−4	+8	+1	−6
5	+6	−7	−1	+5	−8	−2	+4	−9	−3
6	+3	+6	+9	−7	−4	−1	+2	+5	+8
7	−8	+3	−5	+6	−2	+9	+1	−7	+4
8	−4	−8	+7	+3	−1	−5	−9	+6	+2
9	−2	−4	−6	−8	+9	+7	+5	+3	+1
10	−1	−2	−3	−4	−5	−6	−7	−8	−9

Abychom rozhodli, zdali jest číslo

$$N = 3450050201$$

dělitelno číslem 19, zjednejme si zbytky pro

1	na	prvním	místě	$+1$,
2	„	třetím	„	-9,
5	„	pátém	„	-8,
5	„	osmém	„	-1,
4	„	devátém	„	-8,
3	„	desátém	„	-3,

načež obdržíme $R = -28$

a tudíž

$$Z\left(\frac{-28}{19}\right) = -9,$$

z čehož patrno, že číslo N není dělitelno 19, nýbrž že při dělení poskytuje zbytek -9 neb $+10$.

Jak se takovýchto schemat i při jiných úkolech, zejmena při řešení neurčitých rovnic stupně prvního dá s velikým prospěchem užiti, poznáme později.

§. 5.

O vlastnostech dělitelů.

Jak dříve bylo uvedeno, možná každé číslo vyjádřiti tvarem

$$N = a^\alpha b^\beta c^\gamma \ldots, \tag{17}$$

kdež $a, b, c, \ldots$ jsou čísla kmenná, $\alpha, \beta, \gamma, \ldots$ pak čísla celistvá, ukazující, kolikrát které číslo kmenné jest v N obsaženo co faktor; a tu, jak patrno, jest dělitelem

$$\left.\begin{array}{lll} \text{podlé } a & \text{číslo} & a^0, a^1, a^2, \ldots, a^\alpha, \\ \quad „\ b & \quad „ & b^0, b^1, b^2, \ldots, b^\beta, \\ \quad „\ c & \quad „ & c^0, c^1, c^2, \ldots, c^\gamma, \\ \ldots & \ldots & \ldots \end{array}\right\} \tag{18}$$

Abychom tedy obdrželi všechny možné dělitele čísla N, jichž *počet* označíme symbolem $S_1(N)$, nutno kombinovati dělitele soustavy (18), jichž jest

$$\begin{array}{lll} \text{podlé } a & \text{počet} & \alpha + 1, \\ \quad „\ b & \quad „ & \beta + 1, \\ \quad „\ c & \quad „ & \gamma + 1, \\ \ldots & \ldots & \ldots; \end{array}$$

a poněvadž každý člen jedné řádky může býti spojen s kterýmikoli členy řádků ostatních, tož patrno, že počet všech možných, 1 a N k nim počítajíc, bude součinem počtů podle jednotlivých dělitelů aneb

$$S_1(N) = (\alpha + 1)(\beta + 1)(\gamma + 1)\ldots \qquad (19)$$

Jestli pak N číslo kmenné, bude patrně

$$S_1(N) = 2, \text{ totiž } 1 \text{ a } N.$$

Podlé toho má na př. číslo

$$60 = 2^2 . 3 . 5$$

dělitelů 12, jelikož $S_1(60) = (2+1)(1+1)(1+1) = 12$ a sice

1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

Poněvadž jest i pro mnohé praktické potřeby prospěšno znáti počet dělitelů daného čísla, sestavena tuto tabulka pro prvních 50 čísel.

N	$S_1(N)$	N	$S_1(N)$	N	$S_1(N)$	N	$S_1(N)$	N	$S_1(N)$
1	1	11	2	21	4	31	2	41	2
2	2	12	6	22	4	32	8	42	4
3	2	13	2	23	2	33	4	43	2
4	3	14	4	24	8	34	4	44	6
5	2	15	4	25	3	35	4	45	6
6	4	16	5	26	4	36	9	46	4
7	2	17	2	27	4	37	2	47	2
8	4	18	6	28	6	38	4	48	10
9	3	19	2	29	2	39	4	49	3
10	4	20	6	30	6	40	8	50	6

Podobně obdržíme pro číslo

$$N_1 = a_1^{\alpha_1} b_1^{\beta_1} c_1^{\gamma_1} \dots \tag{20}$$
$$S_1(N_1) = (\alpha_1 + 1)(\beta_1 + 1)(\gamma_1 + 1) \dots$$

a tudíž i pro součin $N.N_1$

$$S_1(NN_1) = (\alpha+1)(\beta+1)(\gamma+1) \dots (\alpha_1+1)(\beta_1+1)(\gamma_1+1) \dots$$

takže snadno tu poznáme, že o počtu dělitelů dvou čísel platí

$$S_1(N)\, S_1(N_1) = S_1(NN_1) \tag{21}$$

a tudíž i všeobecně o n číslech *nesoudělných*

$$\prod_{k=1}^{n} S_1(N_k) = S_1\left(\prod_{k=1}^{n} N_k\right), \tag{22}$$

kdež značí symbol Π násobení, jako Σ sečítání.

Abychom určili *součet* všech dělitelů čísla N, jejž označíme podobným symbolem $S_2(N)$, uvažme, že v soustavě (18) součet dělitelů

$$\begin{array}{lll} \text{podlé } a \text{ jest} & \dfrac{a^{\alpha+1}-1}{a-1}, \\ \text{„}\quad b \quad\text{„} & \dfrac{b^{\beta+1}-1}{b-1}, \\ \text{„}\quad c \quad\text{„} & \dfrac{c^{\gamma+1}-1}{c-1}, \\ \dots\dots\dots & , \end{array}$$

načež poznáme, poněvadž každý člen jednoho řádku se kombinuje s členy řádků ostatních, že tu

$$S_2(N) = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \dots \tag{23}$$

Jestli N číslo kmenné, jest patrně

$$S_2(N) = a + 1 = 1 + N.$$

Podle toho jest na př. součet dělitelů čísla

$$N = 60 = 2^2 . 3 . 5$$

$$S_2(60) = \frac{2^3-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{5^2-1}{5-1} = 7 . 4 . 6 = 168.$$

Sestavíme-li si $S_2(N)$ pro prvních 50 čísel, obdržíme:

N	$S_2(N)$	N	$S_2(N)$	N	$S_2(N)$	N	$S_2(N)$	N	$S_2(N)$
1	1	11	12	21	32	31	32	41	42
2	3	12	28	22	36	32	63	42	96
3	4	13	14	23	24	33	48	43	44
4	7	14	24	24	60	34	54	44	84
5	6	15	24	25	31	35	48	45	78
6	12	16	31	26	42	36	91	46	72
7	8	17	18	27	40	37	38	47	48
8	15	18	39	28	56	38	60	48	124
9	13	19	20	29	30	39	56	49	57
10	18	20	42	30	72	40	90	50	93

Jak patrno, nejeví tu součty S_2 žádnou pravidelnost, ba zdá se, že se neřídí žádným zákonem; a předc vyzpytoval bystrý mathematický zrak Eulerův i v tomto zdánlivém neladu rekurrentní pravidlo, jakým se dá $S_2(n)$ vyjádřiti pomocí součtů čísel předcházejících. Jestiť tu

$$\begin{aligned} S_2(N) = {} & S_2(N-1) + S_2(N-2) - S_2(N-5) - S_2(N-7) \\ & + S_1(N-12) + S_2(N-15) - S_2(N-22) - S_2(N-26) \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \tag{24}$$

při čemž však značí $S_2(0) = N$.

Řada čísel, jež se tu vyskytují, představuje rozšířenou řadu čísel *pentagonálních* *) a těmito čísly řídí se tudíž součet všech dělitelů čísla N.

*) Viz *Studnička* „O řadách součtových vůbec a číslech obrazcových zvlášť" Časopis pro pěstování mathm. a fysiky IV. pag. 78.

Podlé vzorce (24) jest tedy pro $N = 24$

$$S_2(24) = S_2(23) + S_2(22) - S_2(19) - S_2(17) + S_2(12) + S_2(9) - S_2(2)$$
$$= 24 + 36 - 20 - 18 + 28 + 13 - 3 = 60,$$

jakž v seznamu našem též stojí.

Znajíce vzorec (23), snadno ustanovíme i pro číslo N_1

$$S_2(N_1) = \frac{a_1^{\alpha_1+1}-1}{a_1-1} \cdot \frac{b_1^{\beta_1+1}-1}{b_1-1} \cdot \frac{c_1^{\gamma_1+1}-1}{c_1-1} \cdots$$

a taktéž i pro číslo $N N_1$

$$S_2(N N_1) = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdots \frac{a_1^{\alpha_1+1}-1}{a_1-1} \cdot \frac{b_1^{\beta_1+1}-1}{b_1-1} \cdots,$$

z čehož pak poznáváme, že o součtu dělitelů dvou čísel N a N_1 platí

$$S_2(N)\, S_2(N_1) = S_2(N N_1) \tag{25}$$

a tudíž o součtu dělitelů n čísel *nesoudělných*

$$\prod_{k=1}^{n} S_2(N_k) = S_2\left(\prod_{k=1}^{n} N_k\right), \tag{26}$$

tedy totéž pravidlo, jako o počtu dělitelů.

§. 6.

O číslech nesoudělných.

Poněvadž při některých vyšetřováních nutno jest znáti počet čísel menších nežli dané číslo N a zároveň s ním nesoudělných, musíme i tento počet, jejž budeme značiti symbolem $S_3(N)$, všeobecně ustanoviti a vzorcem vyjádřiti.

K tomu cíli třeba jen z řady N čísel

$$1, 2, 3, \ldots, a, (a+1), \ldots, N,$$

v níž jsou všechna čísla menší nežli N obsažena, vyloučiti čísla taková, která obsahují některého dělitele čísla N aneb čísla s N soudělná. A tu patrno, že v ní především obsažena jsou čísla

$$1a, 2a, 3a, \ldots, \frac{N}{a} \cdot a,$$

jež mají s N faktor a společný a jichž jest na počet $\frac{N}{a}$, takže odečteme-li tato čísla soudělná od N, obdržíme

$$N - \frac{N}{a} = N\left(1 - \frac{1}{a}\right). \tag{27}$$

V řadě těchto zbývajících čísel obsažena dále čísla

$$1b,\ 2b,\ 3b,\ \ldots,\ \frac{N}{b}.b\,,$$

jež mají s N faktor b společný a jichž jest na počet $\frac{N}{b}$; a z těch neobsahuje faktor a podlé vzorce (27) počet

$$\frac{N}{b}\left(1 - \frac{1}{a}\right),$$

takže odečteme-li od výrazu (27) i tato čísla podlé b soudělná, zbude nám jen

$$N\left(1 - \frac{1}{a}\right) - \frac{N}{b}\left(1 - \frac{1}{a}\right) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right). \tag{28}$$

V řadě čísel zbývajících a výrazem (28) zahrnutých vyskytují se dále čísla

$$1c,\ 2c,\ 3c,\ldots,\ \frac{N}{c}.c\,,$$

jež mají s N faktor c společný a jichž jest na počet $\frac{N}{c}$, a z těch neobsahuje ani a ani b co faktor podlé vzorce (28) počet

$$\frac{N}{c}\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right),$$

takže odstraníme-li z výrazu (28) i tato čísla podle c soudělná, zbude nám jen

$$N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right).$$

Pokračujeme-li takto dále, obdržíme konečně pro *počet* nesoudělných čísel menších nežli N vzorec

$$S_3(N) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right)\ldots, \tag{29}$$

aneb zavedeme-li za N původní význam (17) a zkrátíme-li,

$$S_3(N) = a^{\alpha-1}(a-1)\, b^{\beta-1}(b-1)\, c^{\gamma-1}(c-1)\ldots \tag{30}$$

Jestli tedy N číslo kmenné, bude

$$S_3(N) = a - 1 = N - 1.$$

Zároveň tu sluší poznamenati, že k těmto číslům nesoudělným se vždy počítá 1 a že tudíž i

$$S_3(1) = 1,$$
$$S_3(2) = 1,$$

což představuje jaksi výminku, kterou i na dále nutno míti na zřeteli.

Počet $S_3(N)$ vyjadřuje vždy číslo *sudé*, jelikož čísla kmenná jsou, vyjmouc 2, lichá a tudíž činitelové vzorce (30)

$$a-1, \quad b-1, \quad c-1, \ldots$$

čísla sudá; zároveň tu platí pravidlo, že polovice těchto čísel jest menší a polovice větší nežli $\frac{N}{2}$. a že se vždy dvě doplňují na N.

Jestli totiž $A < N$ a A s N číslo nesoudělné, budou též čísla N, $(N-A)$ nesoudělná; neb kdyby bylo vedlé

$$N = aq \quad \text{též} \quad (N-A) = ap,$$

bylo by $$A = a(q-p),$$

tedy by mělo s číslem N faktor a společný, což jest proti podmínce položené, z čehož tedy jde, že i $(N-A)$ není číslo soudělné a že s prvním dohromady činí

$$A + (N-A) = N,$$

jakž bylo praveno.

Číslo $60 = 2^2 . 3 . 5$ obsahuje na př. čísel nesoudělných $2(3-1)(5-1) = 16$ a sice, spořádáme-li je podlé velikosti pod sebe,

$$\begin{array}{cccccccc} 1, & 7, & 11, & 13, & 17, & 19, & 23, & 29, \\ 59, & 53, & 49, & 47, & 43, & 41, & 37, & 31. \end{array}$$

Jak později seznáme, jest číslo $S_3(N)$ velmi důležité pro řešení neurčitých rovnic stupně prvního pomocí poučky Fermatovy, pročež klademe tuto i tabulku pro tato čísla od 1 až do 50.

N	$S_3(N)$	N	$S_3(N)$	N	$S_3(N)$	N	$S_3(N)$	N	$S_3(N)$
1	1	11	10	21	12	31	30	41	40
2	1	12	4	22	10	32	16	42	12
3	2	13	12	23	22	33	20	43	42
4	2	14	6	24	8	34	16	44	20
5	4	15	8	25	20	35	24	35	24
6	2	16	8	26	12	36	12	46	22
7	6	17	16	27	18	37	36	47	46
8	4	18	12	28	12	38	18	48	16
9	6	19	18	29	28	39	24	49	42
10	4	20	8	30	8	40	16	50	20

Dále poznáváme i tu, že podlé vzorce (30) bude pro číslo N_1

$$S_3(N_1) = a_1^{\alpha_1-1}(a_1-1)\,b_1^{\beta_1-1}(b_1-1)\,c_1^{\gamma_1-1}(c_1-1)\ldots$$

a taktéž pro součin $N\,N_1$

$$S_3(N N_1) = a^{\alpha-1}(a-1)\,b^{\beta-1}(b-1)\ldots a_1^{\alpha_1-1}(a_1-1)\,b_1^{\beta_1-1}(b_1-1)\ldots$$

takže snadno i pro tento pojem S_3 si zjednáme pravidlo

$$S_3(N)\,S_3(N_1) = S_3(N N_1) \qquad (31)$$

a podle něho i všeobecný vzorec sestavíme

$$\prod_{k=1}^{n} S_3(N_k) = S_3\left(\prod_{k=1}^{n} N_k\right). \qquad (32)$$

Určíme-li konečně pro všechny dělitele čísla N součty S_3, bude *součet* těchto S_3, jejž označíme symbolem $S_4(N)$, rovnati se číslu N.

Jestli v jednodušším případě

$$M = a^{\alpha},$$

jsou tu dělitelové, jak patrno,

$$a^0,\ a^1,\ a^2,\ \ldots,\ a^\alpha$$

a tudíž platí pro a^k podlé vzorce (30)

$$S_3(a^k) = a^{k-1}(a-1),$$

z čehož jde, dosadíme-li za k po sobě 0, 1, 2, . , α,

$$\begin{aligned} S_3(a^0) = 1,\quad S_3(a^1) &= a-1,\\ S_3(a^2) &= a(a-1),\\ S_3(a^3) &= a^2(a-1),\\ &\vdots\\ S_3(a^\alpha) &= a^{\alpha-1}(a-1), \end{aligned}$$

a sečteme-li, tedy

$$\begin{aligned} \sum_{k=0}^{\alpha} S_3(a^k) &= 1 + (a-1)(1 + a + a^2 + \ldots + a^{\alpha-1})\\ &= 1 + (a-1)\frac{a^\alpha-1}{a-1} = a^\alpha = M; \end{aligned}$$

podlé toho jest tedy

$$\sum_{k=0}^{\alpha} S_3(a^k) = a^\alpha, \tag{33}$$

jakž bylo svrchu všeobecným pravidlem vyjádřeno.

A poněvadž podlé předešlého všechny dělitele čísla N obsahuje součin

$$\sum_{k=1}^{\alpha} a^k \sum_{k=0}^{\beta} b^k \sum_{k=0}^{\gamma} c^k \ldots,$$

bude, jak patrno, součet S_4 všech S_3, vztahujících se k těmto dělitelům,

$$S_4(N) = \Sigma S_3(a^k)\, \Sigma S_3(b^k)\, \Sigma S_3(c^k) \ldots,$$

aneb použijeme-li přiměřeně vzorce (33),

$$S_4(N) = a^\alpha b^\beta c^\gamma \ldots = N, \tag{34}$$

z čehož i všeobecné pravidlo svrchu vyslovené jde na jevo.

Jestli tedy na př. $N = 60$ a dělitelové tudíž

	1,	2,	3,	4,	5,	6,	10,	12,	15,	20,	30,	60,
jest S_3:	1,	1,	2,	2,	4,	2,	4,	4,	8,	8,	8,	16,

tedy $\Sigma S_3 = 60.$

Že i v tomto případě platí o dvou číslech našich

$$S_4(N)\,S_4(N_1) = S_4(NN_1) \tag{35}$$

a tudíž i všeobecně o n číslech *nesoudělných*

$$\prod_{k=1}^{n} S_4(N_k) = S_4\left(\prod_{k=1}^{n} N_k\right), \tag{36}$$

není třeba ani zvláště odůvodniti.

Sestavíme-li tedy výsledky, týkající se vlastností výrazů symbolem S označených, obdržíme konečně

$$\prod_{k=1}^{n} S_i(N_k) = S_i\left(\prod_{k=1}^{n} N_k\right), \tag{37}$$

kdež za i sluší klásti 1, 2, 3, 4.

Oddělení II.

O zbytcích lineárních.

§. 7.

O zbytcích vůbec.

Jak dříve již bylo vyloženo, značí symbol

$$Z\left(\frac{a}{p}\right) = \alpha, \quad \alpha < p,$$

že α jest zbytek, povstávající dělením čísla a číslem p, takže místo vzorce tohoto možná též psáti

$$\text{buď} \quad Z\left(\frac{a-\alpha}{p}\right) = 0,$$

$$\text{neb} \quad a = mp + \alpha,$$

kdež značí m, kolikrát jest p v a obsaženo.

O těchto zbytcích, které jsou výsledkem vlastností čísla a, p, platí celá řada pravidel, z nichž nejdůležitější tuto buďtež sestaveny.

Značí-li a, p čísla *nesoudělná* a jestli

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

musí tedy býti

$$Z\left(\frac{m}{p}\right)=0,$$

což samo o sobě jest dosti jasno a též plyne z poučky na konci §. 3. vyložené.

2. Pomocí této poučky snadno se dokáže, že pro *kmenné* číslo p jest binomický součinitel

$$\binom{p}{i}=\frac{p(p-1)(p-2)\ldots(p-i+1)}{i!}$$

dělitelný číslem p. Neb ze stejniny této jde

$$\binom{p}{i}i!=pQ,$$

kdež značí Q číslo celistvé, a tudíž bude

$$Z\left\{\frac{\binom{p}{i}i!}{p}\right\}=0;$$

poněvadž ale pro $i<p$ součin

$$i!=1.2.3\ldots i$$

neobsahuje v sobě kmenné číslo p a jest vůbec nesoudělný s p, jest podle předešlého pravidla

$$Z\left\{\frac{\binom{p}{i}}{p}\right\}=0. \tag{38}$$

3. Z téhož pravidla plyne dále, je-li p číslo kmenné a platí-li

$$Z\left(\frac{n_1+n_2+\ldots+n_a}{p}\right)=0$$

a tudíž podlé známé poučky též jest

$$Z\left(\frac{[n_1+n_2+\ldots+n_a]^p}{p}\right)=0,$$

že zároveň i platí

$$Z\left(\frac{n^p{}_1+n^p{}_2+\ldots+n^p{}_a}{p}\right)=0,$$

aneb spojíme-li oba vzorce,

$$Z\left(\frac{[n_1+n_2+\ldots+n_a]^p}{p}\right)=Z\left(\frac{n^p{}_1+n^p{}_2+\ldots+n^p{}_a}{p}\right). \tag{39}$$

Neb z předešlého vzorce jde pomocí polynomické poučky

$$(n_1+n_2+\ldots+n_a)^p = n^p{}_1 + n^p{}_2 + \ldots + n^p{}_a + p\,Q,$$

z kteréžto stejniny ihned plyne vzorec (39), jelikož levá strana jest číslem p dělitelna.

4. Značí-li a, b čísla nesoudělná s p a jestli

$$Z\left(\frac{a}{p}\right) = \alpha, \quad Z\left(\frac{b}{p}\right) = \beta,$$

bude, jakž i dříve bylo poznamenáno,

$$Z\left(\frac{a\,b}{p}\right) = \alpha\,\beta,$$

aneb jestli ve zvláštním případě $\alpha\beta > p$

$$Z\left(\frac{a\,b}{p}\right) = Z\left(\frac{\alpha\beta}{p}\right) = \gamma, \quad \gamma < p.$$

Neb podlé významu těchto symbolů jest

$$a = mp + \alpha,$$
$$b = np + \beta$$

a tudíž bude, znásobíme-li na obou stranách,

$$ab = p\,(mnp + m\beta + n\alpha) + \alpha\beta,$$

z čehož plyne pravidlo svrchu vyjádřené.

Jestli pak $\alpha = 1$, $\beta = 1$, bude

$$Z\left(\frac{\alpha\beta}{p}\right) = 1 \quad \text{a tudíž i} \quad Z\left(\frac{a\,b}{p}\right) = 1.$$

Poznámka. Pravidla tohoto možná užiti při násobení, chceme-li se přesvědčiti zdali nebylo pochybeno; zjednáme-li si totiž zbytky jednotlivých činitelů jakož i příslušného součinu pro dělitele 9, což podle známého pravidla dělitelnosti snadno se provede, a vyhovují-li zbytky tyto předešlému pravidlu, soudíme, že bylo dobře násobeno (*zkouška devítkou.*)

Na př. máme při součinu

$$5313 \,.\, 6014 = 31952382,$$

dělíme-li 9, zbytky 3, 2, 6, kteréž vyhovují podmínce

$$3 \,.\, 2 = 6,$$

což potvrzuje, že bylo dobře násobeno.

5. Značí-li všeobecně $a_1, a_2, a_3, \ldots, a_n$ čísla *nesoudělná* s p a jestli tu tedy

$$Z\left(\frac{a_1}{p}\right)=\alpha_1 \quad \text{neb} \quad a_1=m_1 p+\alpha_1,$$

$$Z\left(\frac{a_2}{p}\right)=\alpha_2 \quad \text{"} \quad a_2=m_2 p+\alpha_2,$$

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

$$Z\left(\frac{a_n}{p}\right)=\alpha_n \quad \text{"} \quad a_n=m_n p+\alpha_n,$$

obdržíme, znásobíme-li na obou stranách,

$$a_1\, a_2\, a_3 \ldots a_n=p\,Q+\alpha_1\, \alpha_2\, \alpha_3 \ldots \alpha_n,$$

kdež význam činitele Q jest patrný; i bude tudíž

$$Z\left(\frac{a_1\, a_2 \ldots a_n}{p}\right)=Z\left(\frac{\alpha_1\, \alpha_2 \ldots \alpha_n}{p}\right). \tag{40}$$

Jestli pak ve zvláštním případě

$$a_1=a_2=\ldots=a_n=a,$$

$$\alpha_1=\alpha_2=\ldots=\alpha_n=\alpha,$$

plyne z pravidla posledního

$$Z\left(\frac{a^n}{p}\right)=Z\left(\frac{\alpha^n}{p}\right) \tag{41}$$

a jestli konečně $\alpha=1$, též

$$Z\left(\frac{a^n}{p}\right)=1. \tag{42}$$

6. Značí-li a, p čísla *nesoudělná* a jestli

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

bude

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

"

$$Z\left(\frac{3a}{p}\right)=\alpha_3,$$

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

"

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

kdež α_1, α_2, α_3, $\ldots$, α_{p-1} značí vesměs zbytky nestejné. Neb kdyby dva z nich byly stejny, dejme tomu

$$\alpha_i=\alpha_k,$$

bylo by, jak patrno,

$$Z\left(\frac{ia}{p}\right)=Z\left(\frac{ka}{p}\right)$$

aneb podle významu tohoto symbolu

$$Z\left(\frac{(i-k)a}{p}\right)=0;$$

ale tu jest a nesoudělné s p a číslo

$$i-k<p$$

nemůže taktéž obsahovati v sobě p co faktor, nemůže býti tudíž poslední rovnici vyhověno, není tedy též podmínka za základ položená možná, nejsou tedy dva zbytky v oné řadě stejny.

Konečně platí o těchto zbytcích, že součet dvou stejně daleko od konců vzdálených jest p, což ze stejniny

$$Z\left(\frac{ka}{p}\right)+Z\left(\frac{p-k}{p}\right)=Z\left(\frac{k+p-k}{p}\right)=0$$

jde na jevo. A z tohoto pravidla plyne, zavedeme-li zbytky nejmenší, že součet dvou stejně daleko od konců vzdálených jest 0. Podlé toho jest tedy

$$\alpha_1+\alpha_{p-1}=p,$$
$$\alpha_2+\alpha_{p-2}=p,$$
$$\alpha_3+\alpha_{p-3}=p,$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\,,$$

takže známe-li polovici těchto zbytků, snadno druhou polovici si zjednáme pomocí tohoto pravidla. Při tom budiž ještě poznamenáno, že k-tý zbytek skládá se z prvního a $(k-1)$ho; neb jestli

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

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

a tudíž odečteme-li,

$$Z\left(\frac{a}{p}\right)=\alpha_k-\alpha_{k-1}=\alpha_1,$$

z čehož jde tedy

$$\alpha_k = \alpha_1 + \alpha_{k-1} \quad \text{neb} \quad \alpha_k = Z\left(\frac{\alpha_1 + \alpha_{k-1}}{p}\right). \tag{43}$$

7. Značí-li $a_1, a_2, a_3, \ldots, a_n$ čísla kmenná a jestli

$$Z\left(\frac{m}{a_1}\right) = \alpha,$$
$$Z\left(\frac{m}{a_2}\right) = \alpha,$$
$$\vdots$$
$$Z\left(\frac{m}{a_n}\right) = \alpha,$$

bude zároveň též

$$Z\left(\frac{m}{a_1 a_2 \ldots a_n}\right) = \alpha;$$

neb tu jest patrně rozdíl $m - \alpha$ dělitelný čísly kmennými, tedy i dělitelný jich součinem.

8. Značí-li a, p čísla nesoudělná a jestli p číslo kmenné, které vyhovuje podmínce

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

aneb $$a = 1 + mp,$$

obdržíme, uvedeme-li na obou stranách na p-tou mocninu,

$$a^p = 1 + p^2 Q,$$

kdež význam čísla Q jest patrný, z čehož pak jde

$$Z\left(\frac{a^p}{p^2}\right) = 1;$$

naložíme-li s rovnicí touto stejným spůsobem jako s předešlou, obdržíme dále

$$Z\left(\frac{a^{p^2}}{p^3}\right) = 1$$

a tudíž konečně všeobecně

$$Z\left(\frac{a^{p^{\alpha-1}}}{p^\alpha}\right) = 1. \tag{44}$$

9. Jestli $f(x)$ celistvá rationální funkce algebraická rozměru $(p-1)$ho a tudíž všeobecně

$$f(x)=x^{p-1}+A_{p-2}\,x^{p-2}+\ldots+A_1\,x+A_0$$

a platí-li tu pro $k=1, 2, 3, \ldots, p-1$

$$Z\left(\frac{f(\alpha_k)}{p}\right)=0, \tag{45}$$

bude, jakž snadno dělením se přesvědčíme,

$$f(x)=(x-\alpha_1)\,f_1(x)+R,$$

kdež značí f_1 funkci podobnou stupně $(p-2)$-ho a R zbytek, jehož hodnotu poznáme, dosadíme-li do posledního vzorce α_1 za x; obdržímeť tu

$$f(\alpha_1)=R$$

a tudíž zároveň

$$f(x)=(x-\alpha_1)f_1(x)+f(\alpha_1),$$

z čehož jde podlé podmínky (45)

$$Z\left(\frac{f}{p}\right)=(x-\alpha_1)\,f_1.$$

Podobně bude $\quad Z\left(\frac{f_1}{p}\right)=(x-\alpha_2)\,f_2,$

$$\vdots$$

$$Z\left(\frac{f_{p-3}}{p}\right)=(x-\alpha_{p-2})\,f_{p-2},$$

konečně $\quad Z\left(\frac{f_{p-2}}{p}\right)=(x-\alpha_{p-1})\,f_{p-1},$

kdež ale f_{p-1} jest funkce rozměru 0-tého a tudíž se redukuje na 1.

Z této soustavy rovnic obdržíme pak, znásobíme-li na obou stranách a zkrátíme-li,

$$Z\left(\frac{f}{p}\right)=(x-\alpha_1)\,(x-\alpha_2)\ldots(x-\alpha_{p-1}),$$

aneb což jest totéž,

$$f(x)=(x-\alpha_1)\,(x-\alpha_2)\ldots(x-\alpha_{p-1})+p\,Q, \tag{46}$$

kdež Q může značiti též funkci podobnou, rozměru ale nižšího nežli $f(x)$.

(Pokračování.)