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

*Časopis pro pěstování mathematiky a fysiky*, Vol. 4 (1875), No. 3, 97--115

Persistent URL: http://dml.cz/dmlcz/122563

# Základové nauky o číslech.

Podává

Dr. F. J. Studnička.*)

## Úvod.

### §. 1.

### O čísle vůbec.

Hledíme-li klidně před sebe, vytvoří se v oku našem obraz všeho, co může v té době do oka našeho paprsky světelné poslati a tu k platnosti přivésti; berouce pak obraz tento u vědomost pravíme, že *vidíme.*

*) V prvním článku tohoto ročníku vyložil jsem zcela stručně původ a rozvoj nauky o číslech a s ní těsně souvislé neurčité analytiky a poukázal ku konci k některým spisům, z nichž možná čerpati poučení *o vlastnostech čísel, jež nezakládají se v soustavě číselné* a jež jsou předmětem nauky o číslech vůbec. Poněvadž ale spisy tyto, jsouce cizojazyčnými, všem čtenářům našim nejsou zajisté stejně přístupny, odhodlal jsem se k tomu v listech těchto, věnovaných pěstování mathematiky a fysiky *se zvláštním zřetelem k studujícím,* vyložiti aspoň základní rysy této nauky vůbec a poučky týkající se *dělitelnosti a shodnosti čísel* zvlášť, aby pak každý s touto propravou mohl se obrátiti k studiím spisů obšírných, kdo by s tímto předmětem chtěl blíže se seznámiti, aneb aspoň tolik vědomostí si pohodlným spůsobem v tomto oboru zjednal, kolik jich třeba k doplnění toho, co s této strany se vykládá na středních školách našich. Zároveň pak bude toto pojednání vyplňovati příslušnou mezeru v naší literatuře mathematické tak dlouho, pokud se samostatný spis o theorii čísel neobjeví, což aby se brzy stalo, jest zajisté vřelým přáním všech, jimž záleží na rozvoji mathematických věd v lůně národa našeho, vynikajícího nadáním mathematickým již od dávných dob.

Omezujeme-li pak v duchu na tomto obraze jisté části co *celky*, vytvořujeme *jednotlivé* předměty, *jednotky určitého druhu*, rozeznávajíce je od jiných celků co jednotek druhů jiných. Jednotky tyto, závislé jsouce pouze na libovolném omezení v duchu našem, nedají se arci všeobecně určitěji vyměřiti, nýbrž postačí, představujeme-li si a poznáváme-li je *vždy co takové*.

Máme-li před sebou jednotek stejného druhu více a chceme-li *určiti*, *kolik* jich tu jest aneb chceme-li věděti, kolikráte tu jednotka téhož druhu vedle sebe jest položena, musíme k označení této *určité kolikosti* míti zvláštní vyjádření, jež nazýváme *číslem* a při psaní znázorňujeme číslicemi.

Vidíme-li na př. les před sebou, můžeme v něm rozeznávati stromy co jednotky; chceme-li pak určiti, kolik jich na jisté ploše stojí, musíme k tomu cíli znáti příslušné vyjádření, číslo, které takový počet jednotek v naší řeči vyznačuje, dejme tomu *stodvacet*, 120.

Vidíme-li u pekaře v koši stejné části bochníků, které povstaly tím, že každý bochník byl rozpůlen a každá tato půlka opět byla rozpůlena, budeme tu rozeznávati čtvrtiny bochníků co jednotky a udáme-li určitě, kolik takovýchto jednotek v košíku tomto se rozeznává, vyslovíme opět číslo, dejme tomu *dvacet* (20), totiž čtvrtek bochníku.

Základem čísla jest tudíž *jednotka* jistého druhu, kteráž sama jest číslem *prvním* neb *původním*, jelikož přidáváním dalších jednotek téhož druhu k ní povstává celá řada čísel větších jako jedna a jedna co *dvě* (2), jedna a jedna a ještě jedna co *tři* (3) atd., kterážto řada čísel jde do nekonečna. Neb kdyby byla konečnou, bylo by jedno číslo a sice poslední největším; poněvadž ale nic nám nebrání, abychom k tomuto číslu největšímu nepřidali opět jednotku a tudíž si nezjednali číslo ještě větší, tož patrno, že zvětšování čísel stálým přikládáním stejných jednotek nemá konce, že tedy *řada čísel jde do nekonečna*.

Při tom rozeznáváme řadu *čísel celistvých*, kdež základní jednotka nejmenuje se dílem celku jiného, tedy řadu

$$1, 2, 3, 4, 5, \ldots, \qquad (1)$$

již nazýváme tudíž *přirozenou* řadou číselnou, a pak řadu čísel

podílových neb *lomených*, kdež základní jednotka jest jmenována co několikátý neb $n$-tý díl celku jiného, tedy řadu

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}, \frac{n+1}{n}, \ldots, \quad (2)$$

již nazýváme tudíž i *odvozenou* řadou číselnou.

Řada tato jest všeobecnější nežli předešlá, jelikož jest první v druhé obsažena, což dvojím spůsobem lze vytknouti; píšeme-li v řadě (2) místo $n$ jednotku, obdržíme co zvláštní případ řadu (1) aneb vytkneme-li v řadě (2) členy

$$\frac{n}{n}, \frac{2n}{n}, \frac{3n}{n}, \frac{4n}{n}, \ldots,$$

obdržíme taktéž řadu (1).

Rozdíl sousedních dvou členů řady (2) obnáší, jak patrno, $n$-tý díl jednotky a jest tudíž tím menší, čím větší jest $n$; přechod od jednoho člena řady této děje se tedy skokem velikosti $1/n$ a nechť zvolíme za $n$ číslo sebe větší, vždy bude mezi dvěma sousedními členy mezera nějaká, byť i sebe menší. Řada (2) jest podle toho *přetržitou* a nedá se pomocí *konečného n* přeměniti v řadu *spojitou*.

Během dalšího výkladu poznáme čísla jiného druhu, která nepřipadají ani do všeobecné řady (2), nechť zvolíme za $n$ číslo konečné jakékoli, nýbrž zůstávají vždy mezi určitými dvěma členy sousedními; čísla tato jsou *nesměrná* neb *irracionální*. Vedle nich pak sluší jmenovati čísla, která vůbec ani do řady (2) nelze uvésti, která připadají mimo ni; čísla tato jsou *imaginární* neb *laterální*. Ba s formálního stanoviska možná celou řadu rozličných druhů číselných rozeznávati.

Poněvadž se však k těmto jakož i dříve jmenovaným číslům nepřichází podobnou cestou přímou, nýbrž jen zvláštními obraty početními, zmíníme se blíže o nich, až se příležitost vhodná k tomu vyskytne.

Mluvíce o číslech vůbec, mějme tedy v tomto pojednání na mysli jen čísla řady (1) neb čísla celistvá.

§. 2.

## O úkonech početních.

Ze dvou neb více daných čísel vyvésti nové, neznámé, jest úkolem počítání. *Jakým způsobem* se neznámé číslo vyvádí ze známých, sluje *způsob* neb *úkon početní*, a těch jest *šestero:*

1. Ustanovíme-li pro dvě čísla $a$, $b$ třetí $c$, které obsahuje tolik jednotek, co $a$ a $b$ dohromady, *sečítáme;* $a$ i $b$ jsou tu *sčítanci* (summand), $c$ *součet* (summa), symbol neb znak tohoto úkonu $+$. Podlé toho jest tedy

$$a + b = c.$$

Poněvadž jest výsledek tentýž, připojím-li $b$ jednotek k $a$ jednotkám aneb naopak, jest patrně

$$a + b = b + a,$$

z čehož jde, že *úkon sečítání jest záměnným* neb *kommutativním.*

2. Ustanovíme-li pro dvě čísla $a$, $b$ třetí $c$, které obsahuje tolik jednotek, o kolik jest $a$ větší nežli $b$, *odčítáme;* $a$ jest tu *odčítanec* neb *menšenec* (minuend), $b$ *odčítatel* neb *menšitel* (subtrahend), $c$ pak *rozdíl* (difference), symbol neb znak tohoto úkonu $-$. Podle toho jest tedy

$$a - b = c.$$

Poněvadž v tomto případě platí

$$a - b = -(b - a),$$

patrno, že výměnou veličin $a$ a $b$ se změní výsledek, jelikož obdržel rozdíl znamení odčítavé; *úkon odčítání jest střídavým* neb *alternujícím.*

3. Ustanovíme-li pro dvě čísla $a$, $b$ třetí $c$, které obsahuje počet jednotek $a$ tolikrát, kolik jednotek obsahuje $b$, *násobíme; a* jest tu *násobenec* (multiplikand), $b$ *násobitel* (multiplikator), $c$ *násoba* (produkt), znak tohoto úkonu $\times$ neb . . Podle toho jest tedy

$$a \times b = a \,.\, b = c.$$

A poněvadž jest výsledek tentýž, obsahuje-li $c$ tolikrát $a$, kolikrát $b$ jednotku neb tolikrát $b$, kolikrát $a$ jednotku, platí

$$a \,.\, b = b \,.\, a,$$

z čehož jde, že *úkon násobení jest záměnným* neb *kommutativním*,[1]) za kteroužto příčinou nerozeznává se obyčejně násobitel a násobenec, nýbrž oběma říká se *činitel* (faktor), násobě pak podlé toho *součin.*

4. Ustanovíme-li pro dvě čísla $a$, $b$ třetí $c$, které obsahuje tolik jednotek, kolikrát jest $a$ větší nežli $b$, *dělíme;* $a$ jest tu *dělenec* (dividend), $b$ *dělitel* (divisor), $c$ *podíl* (quotient), znak tohoto úkonu : aneb čárka, napíše-li se dělenec nad ní, dělitel pod ní. Podle toho jest tedy

$$a : b = \frac{a}{b} = c.$$

A poněvadž tu, jak známo

$$a : b = \frac{1}{b : a},$$

---

*) Poněvadž záměnnost při násobení, ač dosti jasná, přec tak zřejmě a názorně nejde na jevo jako při sečítání, podáno několik důkazů o tom, z nichž nejdůkladnější jest tento:

Jestli $a > b$, bude $a = b + c$,
tedy $a.b = b.b + c.b$;
mimo to jest $b = b$,
tedy $b.a = b.a = b(b+c) = b.b + b.c$.

Jestli $b.c = c.b$, jest $a.b = b.a$; třeba tedy důkaz vésti dále.

Pro $b > c$ bude $b = c + d$,
tedy $b.c = c.c + d.c$;
mimo to jest $c = c$,
tedy $c.b = c.b = c.(c+d) = c.c + c.d$.

Jest-li $c.d = d.c$ bude $c.b = b.c$ a tudíž i $a.b = b.a$; třeba tedy ještě dále podobným spůsobem pokračovati, čímž přijdeme k číslům vždy menším a méně se lišícím, až konečně bude

$p > q$ a pak $p = q + 1$,
tedy $p.q = q.q + 1.q$;
mimo to jest $q = q$
tedy $q.p = q.p = q(q+1) = q.q + q.1$,
z čehož jde: poněvadž $1.q = q.1$, jest $p.q = q.p$, ...
a tudíž $c.d = d.c$,
$b.c = c.b$,
a konečně $a.b = b.a$,
což bylo dokázati.

patrno, že výměnou veličin se změní výsledek, jelikož podíl stal se jmenovatelem zlomku, jehož čítatel jest 1, kteryžto poměr nazýváme *převratným* (reciprok); *úkol dělení jest tedy převratným.*

5. Ustanovíme-li pro dvě čísla $a$, $b$ třetí $c$, které obsahuje $a$ co faktor tolikrát, kolikrát obsahuje v sobě $b$ jednotku, *mocníme; a* jest tu *mocněnec* (dignand), *b mocnitel* (exponent), *c mocnina* (potence), znamení tohoto úkonu vyšší postavení čísla $b$ s pravé strany k $a$. Podle toho jest tedy

$$a^b = c.$$

Poněvadž tu, jak známo,

$$b^a \leqslant c,$$

patrno, že výměnou veličin $a$ a $b$ se změní výsledek; *úkon mocnění není tedy záměnným.*

6. Ustanovíme-li pro dvě čísla $a$, $b$ třetí $c$, kteréž nutno položiti tolikrát co faktor, kolikrát obsahuje $b$ jednotku, aby se obdrželo číslo $a$, *odmocňujeme*; $a$ jest tu *odmocněnec* (radikand) *b odmocnitel* (exponent), *c odmocnina*, *kořen* (radix), znamení tohoto úkonu první tah písmene R tedy $\sqrt{}$, nad něž se píše odmocnitel, za něž pak se klade odmocněnec. Podle toho jest tedy

$$\sqrt[b]{a} = c,$$

při čemž opět, jako prvé, platí

$$\sqrt[a]{b} \leqslant c,$$

z čehož patrno, že *úkon odmocnění není záměnným.*

Srovnáme-li úkony tyto podlé podstaty, poznáme, že druhý, čtvrtý a šestý povstává obrácením úkonu prvního, třetího a pátého; i jmenujeme tyto úkony *skladné* (thetické), ony pak *rozkladné* (lytické).

Též co se tkne rázu výsledků, jež úkony tohoto neb onoho druhu obdržíme, vyskytují se tu podstatné rozdíly.

Jsou-li čísla $a$, $b$, o nichž jsme dříve jednali, čísla celistvá — a o těch jen platí výměry svrchu podané —, jest výsledek úkonu skladného $c$ taktéž číslo celistvé, vzaté z řady (1); jinak jest však při úkonech rozkladných.

Z výměru dřívějšího

$$a - b = c$$

jde především na jevo, že pro

$$b = a$$

nečítá číslo $c$ žádné jednotky, neb pak není mezi $a$ a $b$ rozdílu; abychom tento výsledek naznačili, musíme zavésti nový symbol, *nullu* neb *nicku* 0.

Jestli však v jiném případě

$$b > a,$$

pak nevyskytuje se v řadě čísel (1) žádné, které by úloze naší vyhovilo; nutno tedy položiti

$$b = a + \alpha,$$

načež odečtením čísla $(a + \alpha)$ od $a$ zbývá číslo $\alpha$ ještě odečísti, takže tu povstane, jak známo,

$$-\alpha = c.$$

Přicházíme tudíž k novému druhu čísel, které mají znamení odčetné před sebou, k číslům *odčetným*, *subtraktivním* neb, jak obyčejně slují, *negativním*, *záporným*.

Abychom vykázali jim místo v řadě přirozené (1), jděme od pravé strany k levé nazpět a pozorujme, že číslo na levo stojící jest o 1 menší nežli sousední číslo pravé; přijdeme tím od 3 k 2, od 2 k 1, od 1 pak k 0, načež bude číslo o 1 menší nežli 0 patrně — 1, o 1 menší nežli —1 číslo — 2 atd.; řada (1) bude tímto i na levou stranu do nekonečna rozšířena a obdrží tvar

$$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots, \quad (3)$$

podle něhož možná i řadu čísel lomených (2) podobně na levou stranu rozšířiti.

Má-li se tedy výsledek odčítání ve všech případech vyznačiti, nutno zavésti nový druh čísel, totiž čísla *záporná*, jež jsou pokračováním řady (1) směrem opačným, při čemž nazýváme, abychom protivu obou směrů naznačili, čísla řady (1) *kladnými* neb *positivními*, přidávajíce k nim, kde toho zapotřebí, symbol sčítání $+$.

Podobně vede druhý úkon rozkladný, totiž dělení, k číslům jiné řady nežli jest (1), totiž k číslům řady (2) neb k číslům lomeným; neb jestli v dřívějším výměru

$$\frac{a}{b} = c$$

$a$ číslo takové, které nepovstalo násobením čísla $b$ s nějakým číslem řady (1), nebude taktéž $c$ číslem řady (1), nýbrž bude patrně patřiti do řady (2), jak i symbol tento ukazuje.

Třetí úkon rozkladný, totiž odmocnění, vede konečně k dvěma novým druhům čísel a sice k *irracionálním* neb *nesměrným*, když $c$ nelze ani do řady (1) ani do řady (2), byť i na levou stranu byly rozšířeny, položiti, jako na př.

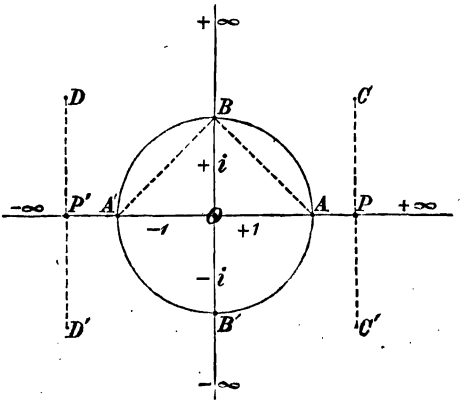
$$\sqrt[2]{2} = \sqrt{2} = 1{\cdot}41421356\ldots,$$

— obdržímeť tu zlomek do nekonečna jdoucí —, a pak k číslům *imaginárním* neb *laterálným*, *pomyslným*, když $b$ jest číslo *záporné* a $a$ číslo *sudé* a tudíž v žádné řadě nemá místa číslo

$$c = \sqrt[a]{-b}.$$

Jak odjinud známo, leží řada čísel laterálných zcela mimo řadu čísel dosud jmenovaných, jež slují *reálná*. Nejlépe pak poznáme poměr tento, znázorníme-li si řady obě.

Obr. 11.




Představme si, že přímka $P'P$ (obr. 11.) jde na obě strany do nekonečna a že směr od $O$ na *pravo* jest směrem *positivním*, směr *opačný* pak *negativním;* pak připadnou, zvolíme-li určitou délku $OA$ za 1, všechna čísla reálná do této přímky, pro niž znamení + a — jest *ukazovatelem směru*. Chceme-li pak věděti,

jaký ukazovatel platí pro směr k tomuto kolmý, veďme poloměrem 1 ze středu $O$ kruh $ABA'$, načež obdržíme podlé známé poučky v trojúhelníku $ABA'$

$$\overline{OB}^2 = i^2 = OA \,.\, OA' \,.$$

aneb zavedeme-li

$$OA = 1, \quad OA' = -1$$

a odmocníme-li,

$$OB = i = \sqrt{-1},$$

z čehož patrno, že *ukazovatel pro směr kolmý jest* $\sqrt{-1}$.

A poněvadž, jak známo,

$$\sqrt{-a} = \sqrt{-1}\,\sqrt{a} = i\,\sqrt{a},$$

tož patrno, že *čísla laterálná znázorňuje přímka stojící kolmo na přímce řadu čísel reálných znázorňující.*

Zároveň pak poznáváme, že body kdekoli v rovině položené znázorňují čísla, skládající se z části reálné a laterálné čili tak zvaná čísla *soujemná* (komplex), při čemž označení části reálné a laterálné ukazuje na kvadrant, v němž příslušný bod jest položen. Na obr. 11. jest na př.

$$OP = a, \quad CP = C'P = DP' = D'P' = b$$

a tudíž znázorňuje poloha bodu

$$\begin{aligned} C &\text{ číslo } +a+bi, \\ D &\quad\ \ " \ -a+bi, \\ C' &\quad\ \ " \ +a-bi, \\ D' &\quad\ \ " \ -a-bi. \end{aligned}$$

Čísla reálná i laterálná o sobě vyplňují takřka osu neb *přímku*, čísla soujemná pak *rovinu nekonečnou.* Jaká čísla vyplňují v tomto smyslu celý *prostor*?

Konečně sluší ještě vytknouti, že výsledky třetího úkonu rozkladného, totiž odmocnění, jsou tolikaznačné neb vlastně tolikaznamné, kolik jednotek odmocnitel $b$ obsahuje; neb tu platí

$$\sqrt[b]{a} = \sqrt[b]{1}\,\sqrt[b]{a} = c\,\sqrt[b]{1},$$

značí-li $c$ číslo reálné, při čemž

$$\sqrt[b]{1} = \varepsilon_1, \ \varepsilon_2, \ \varepsilon_3, \ldots, \ \varepsilon_n,$$

a $\varepsilon_k$ jest $k$-tá hodnota $b$-té odmocniny jednotky, již obdržíme řešením binomické rovnice

$$x^n - 1 = 0.$$

Na př. budiž tu uvedeno čtvero hodnot čtvrté odmocniny jednotky, totiž

$$\sqrt[4]{1} = +1, \quad -1, \quad +i, \quad -i,$$

což obdržíme i neodvisle od řešení binomických rovnic z rozkladu

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x - i)(x + i).$$

Jak z výsledků těchto patrno, liší se valně též *ráz* prvních čtyr úkonů od rázu úkonů posledních. Kdežto při prvních možná výsledek záměnou veličin $a$, $b$ povstávající naznačiti pomocí úkonů téhož druhu, nelze při úkonech posledních téhož cíle dosáhnouti, takže odůvodněno jest s této strany označení: úkony *algebraické* a úkony *transcendentní*, jakéhož se tu mnohdy užívá.

---

## Oddělení I.

## O dělitelnosti čísel.

### §. 3.

### O vzájemnosti dvou čísel vůbec.

Předložena-li dvě nestejná čísla celistvá $a$, $b$, o nichž platí všeobecně

$$a > b$$

a ptáme-li se, jak se k sobě mají, tu mohou se vyskytnouti dva případy a sice jest buď číslo $b$ v čísle $a$ několikráte obsaženo, takže psáti můžeme

$$a = mb, \quad m > 1, \tag{4}$$

aneb není číslo $b$ v čísle $a$ tímto spůsobem obsaženo, takže

$$a = mb + c, \quad m \geqq 1, \quad b > c. \tag{5}$$

V prvním případě se praví, že $a$ jest *násobek* neb *multiplum* čísla $b$ neb že $a$ jest dělitelno číslem $b$, aneb že zbytek,

povstávající dělením čísla $a$ číslem $b$ jest 0, což označujeme symbolem

$$Z\left(\frac{a}{b}\right)=0. \tag{6}$$

V druhém případě se praví, že $a$ není násobkem čísla $b$, neb že $a$ není dělitelno číslem $b$ aneb že dělením čísla $a$ číslem $b$ povstává zbytek $c<b$, což označujeme stejným znakem, píšíce

$$Z\left(\frac{a}{b}\right)=c. \tag{7}$$

A v posledním tomto případě rozeznávati sluší opět dva zvláštní případy a sice jest buď $a$ i $b$ násobek jiného čísla $n$, takže

$$a=np, \quad b=nq,$$

z čehož jde, že $n>1$ jest *společným dělitelem* obou, načež čísla $a$, $b$ nazýváme *soudělná*, aneb neobsahuje $a$ násobek jiného čísla, kterýmž jest číslo $b$ dělitelno, nemají tedy čísla $a$, $b$ společného dělitele $n>1$ a jsou tudíž *nesoudělná*. Neb jestli za stejných podmínek současně

$$\begin{aligned} a &= m_1 b + c, \quad c<b, \\ b &= m_2 c + d, \quad d<c, \\ &\vdots \\ \text{bude konečně} \quad i &= m_{n-1} k + l, \quad l<k, \\ k &= m_n l, \end{aligned}$$

jelikož se tu zbytky stále menší, takže poslední musí býti 0; a tu jde z rovnice

$$\begin{aligned} \text{poslední} \quad & Z\left(\frac{k}{l}\right)=0, \\ \text{tedy z předposlední} \quad & Z\left(\frac{i}{l}\right)=0, \\ & \vdots \\ \text{z druhé} \quad & Z\left(\frac{b}{l}\right)=0, \\ \text{z první} \quad & Z\left(\frac{a}{l}\right)=0, \end{aligned}$$

z čehož patrno, že $l$ jest dělitelem čísla $a$ i $b$ a to zároveň *největším společným dělitelem* obou čísel; čísla $a$, $b$ jsou tudíž *soudělná*.

Jestli pak ve zvláštním případě

$$l = 1,$$

nemají čísla tato společného dělitele vyjmouc 1 a jsou tudíž *nesoudělná*.

A jestli konečně číslo $a$ nesoudělné se všemi čísly menšími nežli $a$, sluje *číslo kmenné* *) (numerus primus), což naznačiti možná symbolem

$$Z\left(\frac{a}{x}\right) = y, \quad a > x > 1. \tag{8}$$

Podlé této vzájemnosti možná tedy rozeznávati čísla druhu dvojího a sice *kmenná*, žádné jiné číslo co faktor neobsahující neb z jiných čísel násobením nesložená, a pak *složená*, obsahující co faktor jiné číslo jednou neb vícekráte, takže všeobecný jich tvar jest

$$N = a^{\alpha}\, b^{\beta}\, c^{\gamma} \ldots, \tag{9}$$

kdež značí $a$, $b$, $c$, ... čísla kmenná, $\alpha$, $\beta$, $\gamma$, ... pak ukazují, kolikrát které číslo jest v $N$ co faktor obsaženo.

Abychom se dozvěděli, jak číslo nějaké jest složeno, nutno, abychom vyzkoumali dělením, která čísla kmenná jsou v něm obsažena a kolikráte; počet možná tu vésti podlé tohoto příkladu:

$$N = 3960 \,|^{2}\, 1980 \,|^{2}\, 990 \,|^{2}\, 495 \,|^{3}\, 165 \,|^{3}\, 55 \,|^{5}\, 11 \,|^{11}\, 1;$$

jest tedy v tomto případě

$$N = 2^3 . 3^2 . 5 . 11.$$

Řada čísel složených jest nekonečná, což poznáváme i ze vzorce (9), v němž $\alpha$, $\beta$, $\gamma$, ... mohou míti hodnoty všechny od 0 až do $\infty$ jdoucí. Ale i řada čísel kmenných jest nekonečná, což *Euklid* již dokázal.

Neb kdyby počet čísel kmenných byl konečný, bylo by

---

*) Že jsem tu zavedl místo slova „*prvočíslo*“, jehož se u nás dosud užívá, pojmenování „*číslo kmenné*“, má své důvody i věcné i formálné, kteréž tuto nechci vykládati, maje za to, že nové toto jmeno bude každému vítané.

jedno z nich největší, dejme tomu $P$; sestavíme-li pak ze všech čísel kmenných násobením a jednotky připojením výraz

$$n = 2 . 3 . 5 . 7 \ldots P + 1,$$

tož patrno, že tu $n > P$ a zároveň pro které koli číslo kmenné a tudíž i z kmenných složené $p$ bude vždy

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

z čehož jde podlé výměru (8), že $n$ jest též číslo kmenné, ač jest větší nežli $P$, kteréž bylo v konečném počtu čísel kmenných největším; není tedy žádné konečné číslo kmenné největším a jde tudíž řada těchto čísel do nekonečna.

Avšak není možná celou tuto řadu zahrnouti vzorcem nějakým, zejména algebraickým; neb stane-li se

$$N = a + bx + cx^2 + \ldots$$

pro $x = m$ číslem kmenným $p$, bude pro

$$x = m + py$$

číslem dělitelným na $p$ a tudíž složeným, jakž snadno se možná přesvědčiti; dosadíme-li totiž tuto hodnotu do vzorce předešlého, obdržíme

$$N' = a + bm + cm^2 + \ldots + bpy + 2\,cmpy + cp^2y^2 + \ldots$$

aneb dosadíme-li hodnotu $p$ za první řadu,

$$N' = p\,(1 + by + 2\,cmy + cpy^2 + \ldots),$$

z čehož jde, že jest $N'$ číslem $p$ dělitelno, že není tedy číslem kmenným.

Určitý počet čísel kmenných možná však podobným vzorcem vyjádřiti, jakž *Euler* na př. ukázal vzorcem

$$N = 41 - x + x^2,$$

v němž obsaženo 40 čísel kmenných.

Ačkoli jest již veliký počet čísel kmenných v tabulky sestaven*) — rozklad v činitele veden až do 5 millionů —,

*) Kmenná čísla menší nežli 10000 sestavena jsou též v „neurčité analytice“ *Berkhanem* vydané, kdež ve dvou svazcích vyloženy nejdůležitější způsoby, jakými se řeší neurčité rovnice stupně prvního a druhého, a mnoho zajímavých sem připadajících sestaveno úkolů.

přec nutno někdy samostatně rozhodnouti, zda-li předložené číslo nějaké jest kmenným čili nic; a tu velmi prospívá poučka tato:

*Leží-li číslo $a$ mezi $r^2$ a $(r+1)^2$ a není-li dělitelno čísly kmennými menšími nežli $r$, jest samo číslem kmenným.*

Neb dejme tomu, že by bylo dělitelno číslem větším $r+s$, že by tedy platilo

$$a = (r+s)\,q,$$

bylo by tudíž i dělitelno číslem $q$, o němž víme, že

$$q = \frac{a}{r+s} < \frac{(r+1)^2}{r+s} < r+1,$$

jelikož zvětšením čitatele $a$ a zmenšením jmenovatele stane se hodnota zlomku větší; a z této nerovnice jde na jevo, že $a$ bylo by dělitelno číslem $q$ menším nežli $r$, což jest proti původní podmínce. Není tedy $a$ dělitelno číslem větším nežli $r$, není-li dělitelno kmenným číslem menším.

Abychom rozhodli, zda-li na př. 737 jest číslo kmenné, ustanovme z $\sqrt{737}$ hodnotu $r = 27$, načež postačí vyšetřiti, je-li číslo předložené dělitelno kmennými menšími nežli 27, při čemž se brzy sezná, že obsahuje 11 co činitele.

Konečně budiž tu poznamenáno, že násobením čísel neobsahujících kmenné číslo $p$ nelze vyvésti nové číslo, které by obsahovalo $p$ co faktor; neb jsou-li $a$, $p$ jakož i $b$, $p$ čísla nesoudělná, budou i $a \,.\, b$, $p$ čísla nesoudělná aneb použijeme-li našich symbolů, jestli

$$Z\left(\frac{a}{p}\right) = a_1, Z\left(\frac{b}{p}\right) = b_1$$

bude

$$Z\left(\frac{ab}{p}\right) = a_1 b_1 \text{ neb } Z\left(\frac{a_1 b_1}{p}\right) = \alpha.$$

Na příklad

$$Z\left(\frac{27}{11}\right) = 5, Z\left(\frac{8}{12}\right) = 8,$$

tedy

$$Z\left(\frac{27 \cdot 8}{11}\right) = 5 \cdot 8 \text{ neb } Z\left(\frac{5 \cdot 8}{11}\right) = 7.$$

Ač jest zákon tento zcela jasný, dostává se mu přece i zvláštního odůvodnění, jež pro důkladnost Euklidické methody tuto též podáváme ve formě poněkud změněné. Jestli

$$Z\left(\frac{a}{p}\right) = a_1, \quad \text{bude } a = pq + a_1,$$
$$Z\left(\frac{p}{a_1}\right) = a_2, \quad \text{„ } p = a_1 q_1 + a_2,$$
$$Z\left(\frac{p}{a_2}\right) = a_3, \quad \text{„ } p = a_2 q_2 + a_3,$$
$$\vdots$$
$$Z\left(\frac{p}{a_{n-1}}\right) = a_n, \text{ bude } p = a_{n-1} q_{n-1} + a_n,$$

při čemž $a_n$ nemůže býti $0$, poněvadž by pak podlé předešlého dělilo $p$ číslo $a$, což jest proti podmínce první; zároveň tu pak platí

$$p > a_1 > a_2 > a_3 > \ldots > a_n,$$

takže se konečně tímto spůsobem musí přijíti k

$$a_n = 1.$$

Násobíme-li tedy za touto podmínkou předešlé rovnice na obou stranách číslem $b$, obdržíme

$$ab = bpq + a_1 b,$$
$$pb = b\, a_1\, q_1 + a_2 b,$$
$$pb = b\, a_2\, q_2 + a_3 b,$$
$$\vdots$$
$$pb = b a_{n-1}\, q_{n-1} + b,$$

načež soudíme takto: Kdyby platilo

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

následovalo by nutně ze soustavy předešlé a sice z rovnice

první $\quad Z\left(\frac{a_1 b}{p}\right) = 0,$

tudíž z druhé $\quad Z\left(\frac{a_2 b}{p}\right) = 0,$

„ z třetí $\quad Z\left(\frac{a_3 b}{p}\right) = 0,$

„ z předposlední $\quad Z\left(\frac{a_{n-1} b}{p}\right) = 0,$

tudíž z poslední $$Z\left(\frac{b}{p}\right) = 0,$$

kteryžto poslední výsledek zřejmě odporuje podmínce druhé, z čehož jde, že neplatí ani výsledky předcházející a tudíž i není základ jich, totiž

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

pravým; není tedy součin $ab$ dělitelný kmenným číslem $p$, není-li ani $a$ ani $b$ číslem $p$ dělitelno.

Z čehož jde pak *Euklidova poučka*, že není součin $PQ$ dělitelný kmenným číslem $p$, platí-li

$$p > P, p > Q,$$

a konečně všeobecná poučka, že *součin*

$$N = a \,.\, b \,.\, c \,.\,.\,.\,.\, l$$

*není dělitelný kmenným číslem $p$, není-li žádný z činitelů jeho tímto číslem dělitelný*, z čehož jde pro

$$a = b = c = \ldots = l = n,$$

že současně platí

$$Z\left(\frac{n}{p}\right) = \alpha, Z\left(\frac{n^m}{p}\right) = \beta \qquad (10)$$

aneb *není-li číslo $n$ dělitelno kmenným číslem $p$, není jím dělitelna žádná mocnina jeho.*

§. 4.

**O pravidlech dělitelnosti.**

Dosud mluvili jsme o dělitelnosti jenom všeobecně, při čemž arci jsme nuceni byli zkouškou neb skutečným dělením se přesvědčiti, zda-li některé číslo v jiném co faktor jest obsaženo čili nic. Toto rozhodování značně se usnadní, známe-li pravidla, podlé nichž možná posouditi dělitelnost nějakým kmenným číslem, anižby se skutečně dělení provedlo; a s těmi jest nám nyní se zanášeti.

Značí-li $a, b, c, \ldots$ čísla kmenná, možná každé číslo $n$ vyjádřiti tvarem, jak dříve již bylo praveno,

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

Kdybychom tedy znali pro určité číslo $n$ tento vzorec, znali bychom i jeho dělitele; neznáme-li však tohoto tvaru, nutno jiným spůsobem vyšetřiti, které číslo jest v $n$ co faktor obsaženo aneb kterým číslem jest $n$ dělitelno.

Abychom příslušná pravidla vyvinuli pro jednotlivá čísla kmenná, dejmo číslu $n$ *tvar soustavný*

$$N = A^m x_m + A^{m-1} x_{m-1} + \ldots + A^2 x_2 + A_1 x_1 + x_0, \qquad (11)$$

kdež pro libovolnou hodnotu přípony $k$ platí

$$x_k < A$$

a značí $x_k$ *číslici*, $A_k$ *hodnotu místa*, na němž číslice tato stojí, takže pro

$$A = 2, 3, 4, \ldots, 10, 12, \ldots$$

obdržíme číselnou soustavu *dyadickou*, *) *triadickou*, *tetradickou*, . . . *dekadickou*, *dodekadickou*, . . .

Má-li tedy $A$ určitou hodnotu a chceme-li poznati dělitelnost čísla $n$ v této soustavě $A$ číselné, položme

$$nA = pq + r, \qquad (12)$$

kdež jsou $n$ a $p$ čísla *nesoudělná* neb

$$Z\left(\frac{n}{p}\right) = \alpha;$$

pak bude, zmocníme-li,

$$n^2 A^2 = pq_1 + r^2,$$
$$n^3 A^3 = pq_2 + r^3,$$
$$\vdots$$
$$n^m A^m = pq_{m-1} + r^m.$$

---

*) Soustava dyadická jest patrně nejjednodušší, jelikož pomocí číslic dvou a sice 0 a 1 vyjádřuje všechna čísla, spůsobem arci rozvláčným; *Leibnic*, který dle zpráv jednoho missionáře měl za to, že Číňané užívají soustavy dvoučíselné, obdivoval se jim velmi a vynášel zjev tento nanejvýš. Pro nás má soustava tato, jelikož tu $x_k$ jest buď 1 neb 0, jen tak dalece důležitosti, že vyjádřuje čísla pomocí mocnin čísla 2; neb ze vzorce (11) jde

$$N = 2^m x_m + 2^{m-1} x_{m-1} + \ldots + 2x_1 + x_0;$$

podle toho jest na př.

$$(63)_X = (111\,111)_{II} = 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0,$$
$$(75)_X = (100\,1011)_{II} = 2^6 + 2^3 + 2^1 + 2^0.$$

Znásobíme-li vzorec (11) na obou stranách mocninou $n^m$ a dosadíme li pak na pravou stranu za $n^k A^k$ příslušnou hodnotu ze soustavy předešlé, bude patrně

$$n^m N = p \sum_{k=0}^{m-1} n^k q_{m-k-1} x_{m-k} + \sum_{k=0}^{m} n^k r^{m-k} x_{m-k},$$

aneb zavedeme-li kratší označení,

$$n^m N = pQ + R, \tag{13}$$

kdež podlé předešlého platí

$$R = r^m x_m + n r^{m-1} x_{m-1} + n^2 r^{m-2} x_{m-2} + \ldots + n^m x_0. \tag{14}$$

Jestli tu $R$ dělitelno kmenným číslem $p$, bude jím dělitelno i $N$; neb jelikož za podmínkou dříve vyslovenou platí podlé pravidla (10)

$$Z\left(\frac{n^m}{p}\right) = \beta,$$

musí současně býti, je-li $R$ číslem $p$ dělitelno,

$$Z\left(\frac{R}{p}\right) = 0, \; Z\left(\frac{N}{p}\right) = 0,$$

poněvadž z rovnice (13) jde patrně

$$Z\left(\frac{n^m N}{p}\right) = Z\left(\frac{R}{p}\right).$$

Jestli pak ve zvláštním případě

$$n = 1,$$

promění se vzorec (14) v jednodušší

$$R_1 = r^m x_m + r^{m-1} x_{m-1} + \ldots + r x_1 + x_0, \tag{15}$$

načež bude buď $N$ dělitelno číslem $p$, je-li jím $R_1$, aneb bude v opačném případě

$$Z\left(\frac{N}{p}\right) = Z\left(\frac{R}{p}\right). \tag{16}$$

Vyšetřování dělitelnosti čísla $N$ uvedeno tudíž na vyšetřování dělitelnosti čísla $R$ neb $R_1$, kteréž jest jednodušší.

Př. 1. Abychom seznali pravidlo dělitelnosti pro číslo $p = 3$ v soustavě *desetinné*, položme ve vzorci (12)

$$n = 1, A = 10, q = 3, r = 1,$$

načež obdržíme ze vzorce (15)

$$R_1 = x_0 + x_1 + x_2 + \ldots + x_m;$$

a totéž obdrží se pro $p = 9$, $q = 1$, takže pravidlo v těchto dvou případech zní takto: *V desetinné soustavě jest číslo dělitelno 3 neb 9, je-li těmito čísly dělitelný součet číslic tohoto čísla*, a zároveň tu platí v opačném případě rovnice (16).

V soustavě *pentadické* by bylo

$$A = 5, n = 2, p = 3,\ 9,\ r = 1$$

a tudíž by se vzorec (14) proměnil v

$$R = x_m + 2\,x_{m-1} + 4\,x_{m-2} + 8\,x_{m-3} + \ldots;$$

podlé toho by se na př. vyšetřilo, že číslo

$$N = (13423)_5$$

jest dělitelno jen 3, nikoli 9, jelikož tu součet

$$R = 1 + 2.3 + 4.4 + 8.2 + 16.3 = 87$$

jest číslem 3 dělitelný.

Př. 2. Abychom poznali pravidla dělitelnosti pro čísla 7, 11, 13, položme ve vzorci (12) pro soustavu dekadickou

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

jelikož pak

$$\begin{aligned} 1001 &= 7.143, \\ &= 11.91, \\ &= 13.77, \end{aligned}$$

načež obdržíme ze vzorce (15)

$$R_1 = x_0 - x_1 + x_3 - \ldots \pm x_m,$$

kdež ale značí $x_k$ číslo trojčíslicové.

*Rozdělíme-li tedy číslo N v desetinné soustavě od pravé ruky k levé na třídy po třech číslicích a jestli rozdíl součtu sudých tříd a lichých dělitelný buď 7 neb 11 neb 13, jest i číslo N dělitelno buď 7 neb 11 neb 13;* v opačném případě platí pravidlo (16).

Číslo 723|501|357|614 poskytuje třídy na místě

lichém $614 + 501 = 1115$

sudém $357 + 723 = 1080$

rozdíl tedy $35 = 5.7$,

jest tedy dělitelno 7; dělíme-li 11, dá zbytek 2, dělíme-li 13, zbytek 9, jelikož

$$Z\left(\frac{35}{11}\right) = 2,\ Z\left(\frac{35}{13}\right) = 9.$$

(Pokračování.)