Emil Schönbaum

Několik kapitol z nauky o číslech

Časopis pro pěstování mathematiky a fysiky, Vol. 34 (1905), No. 3, 265--300

Persistent URL: http://dml.cz/dmlcz/121164

Několik kapitol z nauky o číslech.

Napsal

Emil Schönbaum.

I.

V nauce o číslech hraje velmi důležitou úlohu funkce, kterou Legendre ve svém Theorie de nombres označuje $E(x)$, kdežto Gauss zavádí pro ni označení $[x]$. Definice je velmi jednoduchá: Pro necelé číslo x značí podle Gausse $[x]$ největší celistvé číslo menší než x. Tato definice platí i pro negativní x a sice jest na př. $\left[\frac{5}{4}\right] = 1$, $\left[-\frac{5}{4}\right] = -2$. Pro celistvá a jest ovšem $[a] = a$.

Funkci té příbuzná jest jiná, kterou označujeme $\{x\}$ = nejbližší celistvé číslo k x. Tedy $\left\{\frac{5}{4}\right\} = 1$, $\left\{-\frac{5}{4}\right\} = -1$. Rozdílu $x - \{x\} = R(x)$ užívá ve svých pracích Riemann.

Povaha funkce $[x]$ jest jednoduchá a vysvítá nejlépe z grafického znázornění. Na místech $x = 0, \pm 1, \pm 2, \pm 3 \ldots$, skočí vždy funkce o 1.

Některé vlastnosti jsou samozřejmé

1. $x + [-x] = -1$.
2. $[x] + a = [x + a]$. je-li a celé.
3. $[x] + [h - x] = h - 1$, neboť

$$x = [x] + \varepsilon, \quad 0 \leqq \varepsilon < 1,$$
$$h - x = h - [x] - \varepsilon$$

a tedy

$$[h - x] + [x] = h - 1.$$

4. $[x]+[y] \leqq [x+y]$, neboť

$$x = [x] + \varepsilon, \quad 0 \leqq \varepsilon < 1,$$
$$y = [y] + \eta, \quad 0 \leqq \eta < 1,$$
$$x + y = [x] + [y] + \varepsilon + \eta$$

a protože $\varepsilon + \eta \geqq 0$, po případě též $\geqq 1$, jest

$$[x+y] \geqq [x] + [y].$$

5. Obecněji jest

$$[x_1 + x_2 + \ldots + x_n] \geqq [x_1] + [x_2] + \ldots + [x_n]$$

a odtud pro $x_1 = x_2 = \ldots = x_n = x$

$$[nx] \geqq n\,[x].$$

6. Jest též lehko dokázati, že $\left[\frac{\left[\frac{x}{y}\right]}{z}\right] = \left[\frac{x}{yz}\right]$; jest totiž

$\frac{x}{y} = \left[\frac{x}{y}\right] + \varepsilon$, kdež $0 \leqq \varepsilon < 1$, tedy $\frac{x}{yz} = \frac{\left[\frac{x}{y}\right]}{z} + \frac{\varepsilon}{z}$ a

$\left[\frac{x}{yz}\right] = \left[\frac{\left[\frac{x}{y}\right]}{z}\right]$, neboť $\frac{\varepsilon}{z} < \frac{1}{z}$.

7. Značí-li x libovolné ne celé positivní číslo, mezi jehož násobky x, $2x$, $3x$, ... nx se nevyskytá žádné celistvé číslo, pak platí totéž o $\frac{1}{x}$, $\frac{2}{x}$, $\frac{3}{x}$, ... $\frac{h}{x}$, při čemž $h = [nx]$. Dále jest

$$[x] + [2x] + \ldots + [nx] + \left[\frac{1}{x}\right] + \left[\frac{2}{x}\right] + \ldots + \left[\frac{h}{x}\right] = nh.$$

Prvá část této věty je evidentní. Kdyby totiž bylo pro nějaké číslo a z řady 1, 2, ... h, $\frac{a}{x} = b$, b číslo celé, tedy by muselo býti $b \leqq n-1$, neboť $a \leqq h = [nx] < nx$, tudíž $bx = a$, což odporuje předpokladu o povaze čísla x. Druhá část věty se dokáže takto: V řadě $[x] + [2x] + \ldots + [nx]$ mají všechny členy až po $\left[\frac{1}{x}\right]$-tý hodnotu 0. Následující až

k $\left[\frac{2}{x}\right]$-tému jsou rovny 1, od $\left[\frac{2}{x}\right]$-tého až po $\left[\frac{3}{x}\right]$-tý člen mají hodnotu 2 atd.; jest tedy

$$[x]+[2x]+[3x]+\ldots+[nx]=0\cdot\left[\frac{1}{x}\right]+1\left\{\left[\frac{2}{x}\right]-\left[\frac{1}{x}\right]\right\}$$
$$+2\cdot\left\{\left[\frac{3}{x}\right]-\left[\frac{2}{x}\right]\right\}+\ldots+(h-1)\left\{\left[\frac{h}{x}\right]-\left[\frac{h-1}{x}\right]\right\}$$
$$+h\left\{n-\left[\frac{h}{x}\right]\right\}.$$

Odtud obdržíme, zjednodušíme-li pravou stranu, větu.

Jakožto důsledek plyne následující poučka: Jsou-li p, k čísla nesoudělná, lichá, jest

$$\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\ldots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]+\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\ldots$$
$$+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]=\frac{1}{4}(k-1)(p-1).$$

Je-li totiž $k<p$, jest

$$\frac{\frac{1}{2}(p-1)k}{p}<\frac{1}{2}k,\text{ ale }>\frac{1}{2}(k-1),\left[\frac{\frac{1}{2}(k-1)p}{p}\right]=\frac{1}{2}(k-1).$$

Stačí tudíž položiti v předešlé poučce

$$\frac{k}{p}=x,\quad\frac{1}{2}(p-1)=n,\quad\frac{1}{2}(k-1)=h.$$

Tato věta, jejíž důkaz jsme zde podali dle Gaussa (Werke. Bd. II., str. 3.), jest základem slavného třetího důkazu Gaussova reciproční věty o kvadratických zbytcích.

8. V číselné theorii jsou to v prvé řadě součty největších celků, které se vyskytují, a jest prací sem spadajících veliké množství.*)

*) Viz na př. *Jac. Hacks*: Über Summen von grössten Ganzen. Acta math. 1887, I. — *M. Stern*: Sur la valeur de quelques series etc. Acta math. T. 10. — *Lerch*: Rozpravy č. ak. třída II. roč. VII. č. 6. a 7. atd.

Při tom jest užitečno míti pro $[x]$ výraz, s nímž se dá pohodlněji manipulovati. Nechybí ani na takových výrazech.

Velice pohodlná jest následující forma pro $[x]$, které ve svých pracích a přednáškách užíval Kronecker (Crelle Journ. sv. 104 a 106),

$$[x] = \frac{1}{2} \sum_{h=1}^{h=r-1} (1 + sgn\,(x - h)). \qquad (1)$$

K vysvětlení této formule třeba podotknouti, že $sgn x$ značí positivní nebo negativní jedničku, dle toho, je-li $x > 0$, nebo $x < 0$, pro $x = 0$, jest $sgn x = 0$. Sčítání provádí se od $h = 1$ až po $h = r - 1$, kdež r je *libovolné* celé číslo větší než x.

Že potom jest výrazem na pravo stojícím $[x]$ vyjádřeno, jest zřejmo, neboť pro všechna $h > x$ jsou členové součtu $= 0$. Jen třeba ještě poznamenati, že, je-li x celistvé. neshoduje se tato definice funkce $[x]$ s obyčejnou. V tomto případě jest totiž pro jedno h $sgn\,(x - h) = sgn\,0 = 0$, a tedy $[x] = x - \frac{1}{2}$. Kdybychom definovali $sgn\,0 = 1$, bylo by $[x] = x$ pro celistvé x.

Pomocí formule (1) lze dokázati velmi snadno mnoho vět, jichž důkazy jinak vyžadují značné námahy.

Dokažme podle Kroneckera, že

$$\sum_{k=1}^{\frac{n-1}{2}} \left[\frac{km}{n} + \frac{1}{2}\right] = \sum_{k'=1}^{\frac{m-1}{2}} \left[\frac{k'n}{m} + \frac{1}{2}\right],$$

kdež m, n značí libovolná lichá čísla.

Jest totiž

$$\left[\frac{km}{n} + \frac{1}{2}\right] = \sum_{k'=1}^{\frac{1}{2}(m-1)} \left(1 + sgn\left(\frac{k}{n} - \frac{k'}{m} + \frac{1}{2m}\right)\right)$$

pro všechna $k = 1, 2, \ldots, \frac{n-1}{2}$.

V součtu lze ale klásti místo $k' \frac{1}{2}(m + 1) - k'$, neboť tím se změní jen pořádek sčítanců, takže jest

$$\left[\frac{km}{n}+\frac{1}{2}\right]=\sum_{k'=1}^{\frac{1}{2}(m-1)}\left(1+sgn\left(\frac{k}{n}+\frac{k'}{m}-\frac{1}{2}\right)\right).$$

Dále jest

$$\left[\frac{k'n}{m}+\frac{1}{2}\right]=\frac{1}{2}\sum_{k=1}^{\frac{n-1}{2}}\left(1+sgn\left(\frac{k'}{m}-\frac{k}{n}+\frac{1}{2n}\right)\right)$$

pro $k'=1, 2, 3, \ldots, \frac{m-1}{2}$, neboť r můžeme tu patrně klásti $=\frac{n+1}{2}$. Zaměníme-li zase součtový index za $\frac{n+1}{2}-k$, čímž se nic nezmění, bude

$$\left[\frac{k'n}{m}+\frac{1}{2}\right]=\frac{1}{2}\sum_{k=1}^{\frac{n-1}{2}}\left(1+sgn\left(\frac{k}{n}+\frac{k'}{m}-\frac{1}{2}\right)\right).$$

Srovnáme-li s výrazem pro $\left[\frac{km}{n}+\frac{1}{2}\right]$ a sečteme-li všechny identity pro $k=1, 2, \ldots \frac{n-1}{2}$

$k'=1, 2, \ldots \frac{m-1}{2}$, obdržíme

$$\sum_{k=1}^{\frac{n-1}{2}}\left[\frac{km}{n}+\frac{1}{2}\right]=\sum_{k'=1}^{\frac{m-1}{2}}\left[\frac{k'm}{n}+\frac{1}{2}\right].$$

Zavedeme-li tu ještě funkci dříve označenou $\{x\}$ a uvážíme-li, že jest dle definice $\{x\}=\left[x+\frac{1}{2}\right]$, což lze lehko dokázati, máme jednodušší relaci

$$\sum_{n=1}^{\frac{1}{2}(n-1)}\left\{\frac{km}{n}\right\}=\sum_{k'=}^{\frac{m-1}{2}}\left\{\frac{k'm}{n}\right\}.$$

Snadno lze též odvoditi následující relaci Buscheovu:

Značí-li opět m, n libovolná lichá čísla, jest

$$\sum_{k=1}^{\frac{n-1}{2}} {}_k \left[\frac{2km}{n}\right] + \sum_{k'=1}^{m-1} {}_{k'} \left[\frac{k'n}{2m}\right] = \frac{1}{2}(m-1)(n-1).$$

Jest totiž opět pro $k = 1, 2, \ldots \frac{n-1}{2}$

$$\left[\frac{2km}{n}\right] = \frac{1}{2}\sum_{k=1}^{m-1} {}_{k'} \left(1 + sgn\left(\frac{k}{n} - \frac{k'}{2m}\right)\right), \text{ neboť } r \text{ lze tu voliti } = m.$$

$$= \frac{m-1}{2} + \frac{1}{2}\sum_{k'=1}^{m-1} {}_{k'}\, sgn\left(\frac{k}{n} - \frac{k'}{2m}\right)$$

a tedy

$$\sum_{k=1}^{\frac{n-1}{2}} {}_k \left[\frac{2km}{n}\right] = \frac{(m-1)(n-1)}{4} + \frac{1}{2}\sum_{k,\,k'} sgn\left(\frac{k}{n} - \frac{k'}{2m}\right)$$

$$k = 1, 2. \ldots \frac{n-1}{2},$$

$$k' = 1, 2, \ldots m - 1.$$

Právě tak jest ale přímo

$$\sum_{k'=1}^{m-1} {}_{k'} \left[\frac{k'n}{2m}\right] = \frac{(m-1)(n-1)}{4} + \frac{1}{2}\sum_{k,\,k'} sgn\left(\frac{k'}{2m} - \frac{k}{n}\right),$$

takže věta tvrzená jest dokázána.

9. Jiné vyjádření funkce $[x]$ obdržíme pomocí elementárných trigonometrických řad. Již grafické vyjádření funkce $[x]$ samo upomíná na grafické znázornění elementárných funkcí definovaných Fourierovými řadami, a podobné vyjádření pro $[x]$ jest si snadno zjednati.

Vyjděme od známých vzorců (viz na př. *Studnička*: Monoperiodické funkce str. 163)

$$\text{I.} \quad \frac{1-x}{2} = \frac{\sin \pi x}{\pi} + \frac{1}{2\pi}\sin 2\pi x + \frac{1}{3\pi}\sin 3\pi x + \ldots$$

$$= \sum_{k=1}^{\infty} \frac{\sin k\pi x}{k\pi}.$$

$$\text{II.} \qquad \frac{x}{2} = \frac{\sin \pi x}{\pi} - \frac{1}{2\pi} \sin 2\pi x + \frac{1}{3\pi} \sin 3\pi x - \ldots$$

$$= \sum_{k=1}^{\infty} (-1)^{k-1} \frac{\sin k\pi x}{k\pi}.$$

Oba vzorce platí původně jen pro $0 < x < 1$. Abychom platnost jich rozšířili, kladme na pravé straně I. $x = 1 + \xi$; tím obdržíme dle II

$$-\frac{\sin \pi\xi}{\pi} + \frac{1}{2\pi} \sin 2\pi\xi - \frac{1}{3\pi} \sin 3\pi\xi + \ldots = -\frac{\xi}{2}$$

$$\text{pro } 0 < \xi < 1$$

a tedy

$$\frac{\sin \pi x}{\pi} + \frac{1}{2\pi} \sin 2\pi x + \frac{1}{3\pi} \sin 3\pi x + \ldots = \frac{1-x}{2}$$

$$\text{pro } 1 < x < 2.$$

Klademe-li ale na pravé straně I. $x = 2 + \xi$, obdržíme

$$\sum_{k=1}^{\infty} \frac{\sin k\pi\xi}{k\pi} = \frac{1-\xi}{2} \quad \text{pro } 0 < \xi < 1$$

a tedy vrátíme-li se ku x

$$\sum_{k=1}^{\infty} \frac{\sin k\pi x}{k\pi} = \frac{3-x}{2} \quad \text{pro } 2 < x < 3,$$

obdobně jest

$$\sum_{k=1}^{\infty} \frac{\sin k\pi x}{k\pi} = \frac{3-x}{2} \quad \text{pro } 3 < x < 4,$$

a obecně

$$\sum_{k=1}^{\infty} \frac{\sin k\pi x}{k\pi} = \frac{2n+1-x}{2} \quad \text{pro } 2n < x < 2(n+1),$$

t. j. hodnota řady jest rovna poloviční rozdílu nejbližšího lichého čísla a čísla x.

Stejným způsobem lze odvoditi ze II. obecně

$$\sum_{k=1}^{\infty} (-1)^{k-1} \frac{\sin k\pi x}{k\pi} = \frac{x-2n}{2} \quad \text{pro } 2n-1 < x < 2n+1,$$

t. j. hodnota řady rovná se poloviční rozdílu argum. x a nejbližšího sudého čísla. Z obou posledních vzorců plyne odečtením

$$2\sum_{k=1}^{\infty}{}^{k}\frac{\sin 2k\pi x}{2k\pi} = 2n - x + \frac{1}{2} \quad \text{pro } 2n < x < 2n+1,$$

tedy

$$2n = [x] = x - \frac{1}{2} + \sum_{k=1}^{\infty}{}^{k}\frac{\sin 2k\pi x}{k\pi}.$$

Poznamenati dlužno ovšem, že pro celistvé x dlužno zde bráti $[x] = x - \frac{1}{2}$. Tato formule je účelná při vyšetřování celé řady vztahů mezi $[x]$ a jinými číselně theoretickými funkcemi, na př. Legendreovým znaménkem,*) funkcí $\mu(x)$ atd.

Jiné vztahy mezi součty největších celků pramení ve vyšších partiích nauky o číslech. Tak lze z nauky o počtu tříd binárních kvadratických forem odvoditi mnohé identity, na př. vztah Liouvilleův **)

$$\sum_{s}(-1)^{\frac{s-1}{2}}\left[\frac{m}{s}\right] = \sum_{\vartheta}[\sqrt{m-\vartheta^2}], \quad \text{kdež } s = 1, 3, 5, \ldots$$
$$\vartheta = 0, 1, 2, \ldots [\sqrt{m}].$$

10. Veliké množství formulí dostaneme, kombinujeme-li funkci $[x]$ s funkcí $\mu(x)$, zvanou obyčejně Mertensovou a definovanou následovně

$\mu(x) = (-1)^{\nu}$, obsahuje-li x ν vesměs různých prvočinitelů,
$\mu(x) = 0$, obsahuje-li x kvadratického dělitele,
$\mu(1) = 1$.

Této funkce $\mu(x)$ dá se užíti s velkým prospěchem ve všech partiích theorie čísel, zvláště při vyšetřování asymptotických zákonů a frequence prvočísel.***)

---

*) Viz *Lerch*: Rozpr. č. akad. l. c.

**) Liouville Journal de math. pur. e. appl. 1860; viz též *Lerch*: Arithmetické odvození Lejeune Dirichl. výsledků atd. Rozpr. č. akad. str. 13.

***) Viz *Mertens*: Ein Beitrag zur anal. Zahlentheorie, Crelle Journ. Bd. 78. Über eine zahlentheoretische Function. Sitzgsber. d. ak. Wien. Nov. 1897. *Landau*: Über die zahlentheor. Function $\mu(k)$. Sitzgsber. d. akad. d. Wiss. Wien 1904.

My chceme ještě odvoditi dvě jednoduché věty:

Předem je známo, že, utvoříme-li z libovolného počtu elementů všechny možné kombinace, je počet kombinací sudých tříd = počtu kombinací tříd lichých. Z toho plyne ihned:

$$\sum_{(d)} \mu(d) = 0,$$

kdež se součet vztahuje na všechny dělitele čísla daného m. Neboť je právě tolik dělitelů se sudým počtem prvočinitelů, jako s lichým, počítáme-li 1 k prvým.

Pouze pro $m = 1$ jest $\sum_{(d)} \mu(d) = 1$. Napíšeme-li všechny tyto součty pro $m = 1, 2, 3, \ldots n$ a sečteme-li, obdržíme tak formuli Lipschitzovu

$$\mu(1)\left[\frac{n}{1}\right] + \mu(2)\left[\frac{n}{2}\right] + \ldots + \mu(n)\left[\frac{n}{n}\right] = \sum_{k=1}^{n} \mu(k)\left[\frac{n}{k}\right] = 1.$$

K poučce té druží se celá řada jiných Jonquièrova, Cesarova (Bachmann: Anal. Zahlentheorie str. 309 a násl.)

Známá funkce $\varphi(x)$ definovaná co počet čísel nepřevyšujících x a nesoudělných s x,

$$\varphi(x) = x\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\ldots,$$

je-li $x = p_1^{\alpha_1} p_2^{\alpha_2} \ldots$, dá se též psáti

$$\varphi(x) = x - \sum_{p} \frac{x}{p_1} + \sum_{p_1 p_2} \frac{x}{p_1 p_2} - \ldots = \sum_{(d)} \mu(d) \frac{x}{d},$$

kdež se součet vztahuje na všechny dělitele čísla x.

Odtud se snadno obdrží

$$2F(x) - 1 = \sum_{k=1}^{\infty} \mu(k) \left[\frac{x}{k}\right]^2,$$

kde $F(x)$ značí počet členů řady Fareyovy, jichž čítatel ni jmenovatel nepřevyšují čísla x.

II.

1. Zodpovězme předem známou elementárnou otázku: Která jest nejvyšší mocnina prvočísla p obsažená v součinu n za sebou jdoucích prvých čísel, tedy ve faktorielle $n!$?

Odpověď poskytuje formule, kterou nalézáme poprvé u Legendrea a již chceme zváti jeho jménem.

Jest patrno především, že mezi čísly 1, 2, 3, ... n prvočíslo p jakožto činitele obsahují čísla

$$1p,\ 2p,\ 3p,\ \ldots\ \left[\frac{n}{p}\right]p,$$

tedy v celku $\left[\frac{n}{p}\right]$ čísel. Čtvercem prvočísla p budou dělitelna čísla

$$1p^2,\ 2p^2,\ 3p^2,\ \ldots\left[\frac{n}{p^2}\right].p^2,$$

tedy $\left[\frac{n}{p^2}\right]$ čísel, číslem p^3 bude dělitelno $\left[\frac{n}{p^3}\right]$-čísel a tak to jde dále. Hledaná mocnina prvočísla p, která jest ještě v $n!$ obsažena, bude míti tudíž mocnitele

$$\alpha(n) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right],$$

kdež k jest určeno podmínkou $\left[\frac{n}{p^{k+1}}\right] = 0$. Pro různé applikace odporučuje se užívati pro $\alpha(n)$ tvaru

$$(1) \qquad \alpha(n) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right],$$

což je dovoleno, protože pro všechna $i > k$ jest $\left[\frac{n}{p^i}\right] = 0$.

Jinou cestou lze dojíti téhož výsledku takto:

Mezi čísly 1, 2, 3, ... n jsou číslem p dělitelna čísla

$$1.p,\ 2.p,\ 3.p\ \ldots\ \left[\frac{n}{p}\right].p$$

a součin $n!$ je tudíž dělitelný součinem

$$1 . 2 . 3 \ldots \left[\frac{n}{p}\right] p^{\left[\frac{n}{p}\right]}.$$

V součinu $\left[\frac{n}{p}\right]!$ jsou ale číslem p zase dělitelna čísla

$$1 . p . \; 2 . p, \; 3 . p \ldots \left[\frac{\left[\frac{n}{p}\right]}{p}\right] . p,$$

tedy jest součin ten dělitelný součinem

$$p^{\left[\frac{n}{p^2}\right]} . 1 . 2 . 3 \ldots \left[\frac{n}{p^2}\right], \text{ neboť jest } \left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{n}{p^2}\right].$$

Je-li posléze opět p^k nejvyšší mocnina, pro niž $\left[\frac{n}{p^k}\right] > 0$ obdržíme co výsledek $n!$ je dělitelno číslem

$$p^{\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right]} = p^{\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]}.$$

Tato formule je velmi výhodná při řešení různých otázek týkajících se dělitelnosti.

2. Užijeme jí k dokázání známé věty: Součin m za sebou jdoucích čísel celých je dělitelen součinem m prvých čísel.

Stačí dokázati, že libovolné prvočíslo p jest v čítateli podílu

$$\frac{(a+1)(a+2) \ldots (a+m)}{1 . 2 . 3 \quad \ldots \quad m} = \frac{(a+m)!}{a!\, m!}$$

obsaženo nejméně tak často jako v jmenovateli. Použitím Legendreovy formule jest ale

$$\alpha (a+m) = \sum_{i=1}^{\infty} \left[\frac{a+m}{p^i}\right]$$

a obdobně

$$\alpha (a) = \sum_{i=1}^{\infty} \left[\frac{a}{p^i}\right],$$

$$\alpha(m) = \sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right].$$

Protože jest ale

$$\left[\frac{a+m}{p^i}\right] \geqq \left[\frac{a}{p^i}\right] + \left[\frac{m}{p^i}\right].$$

jest též a fortiori

$$\alpha(a+m) \geqq \alpha(a) + \alpha(m).$$

Věta tato jakož i obecnější věta, již lze týmž způsobem dokázati,

$$\frac{(a_1 + a_2 + \ldots + a_m)!}{a_1!\ a_2!\ \ldots\ a_m!} = \text{celému číslu},$$

odvozuje se obyčejně z kombinatoriky, neboť zde značí podíl $\frac{(a_1 + a_2 + \ldots a_m)!}{a_1!\ a_2!\ \ldots\ a_m!}$ počet permutací z $(a_1 + \ldots + a_m)$ prvků, mezi nimiž je a_1, a_2, $\ldots$ a_m stejných. Poněvadž věty se často v theorii čísel užívá (jeden z důkazů Fermatovy věty je na ní založen), jest dobře dokázati ji pomůckami čistě číselně theoretickými.

3. Značí-li a_1, a_2, $\ldots$ a_m celá čísla positivní, jest podíl

$$\frac{(ma_1)!\ (ma_2)!\ \ldots\ (ma_m);}{a_1!\ a_2!\ \ldots\ a_m!\ (a_1 + a_2 + \ldots + a_m)!}$$ celým číslem.

Pro $m = 2$ obdržíme větu Catalanovu, kterou tento původně vyvodil z theorie elliptických funkcí. Dle věty té jest

$$\frac{(2a_1)!\ (2a_2)!}{a_1!\ a_2!\ (a_1 + a_2)!}.$$

Důkaz obecné věty jest snadný. Musí býti zase pro libovolné prvočíslo

$$\alpha(ma_1) + \alpha(ma_2) + \ldots + \alpha(ma_m) \geqq \alpha(a_1) + \alpha(a_2) + \ldots + \alpha(a_m) + \alpha(a_1 + a_2 + \ldots + a_m).$$

Ale jest patrně vždy

$$\left[\frac{ma_1}{p^i}\right]+\left[\frac{ma_2}{p^i}\right]+\ldots+\left[\frac{ma_m}{p^i}\right]\geqq\left[\frac{a_1}{p^i}\right]+\ldots$$
$$+\left[\frac{a_m}{p^i}\right]+\left[\frac{a_1+a_2+\ldots+a_m}{p^i}\right]$$

a tím je věta dokázána.

4. Mnohem obecnější nežli předešlé tvary jest podíl součinů faktoriell, jejž vyšetřoval E. Landau v Nouvelles Annales de Mathématiques r. 1900 a jehož speciellními případy jsou podíly dříve uvedené.

Jedná se o stanovení nutných a dostačujících podmínek, za kterých je celým číslem podíl

$$P=\frac{X_1!\ X_2!\ \ldots\ X_m!}{Y_1!\ Y_2!\ \ldots\ Y_n!}=\frac{\prod_{\nu=1}^{m} X_\nu!}{\prod_{\nu=1}^{n} Y_\nu!},$$

při tom jsou X_ν a Y_ν homogenní lineárné funkce r proměnných $u_1, u_2, \ldots u_r$ s koefficienty $a_i^{(\nu)}$, $b_i^{(\nu)}$ celými a positivními (z nichž mohou býti libovolné $=0$), takže jest tedy

$$X_\nu=a_1^{(\nu)}u_1+a_2^{(\nu)}u_2+\ldots+a_r^{(\nu)}u_r=\sum_{i=1}^{r} a_i^{(\nu)}u_i,\quad \nu=1,\ 2,\ \ldots\ m,$$

$$Y_\nu=b_1^{(\nu)}u_1+b_2^{(\nu)}u_2+\ldots+b_r^{(\nu)}u_r=\sum_{i=1}^{r} b_i^{(\nu)}u_i,\quad \nu=1,\ 2,\ \ldots\ n.$$

Jde tedy o vyšetření podmínek, jimž musí hověti $(m+n)r$ koefficientů a, b, aby podíl

$$P=\frac{\prod_{\nu=1}^{m}\left(\sum_{i=1}^{r} a_i^{(\nu)}u_i\right)!}{\prod_{\nu=1}^{n}\left(\sum_{i=1}^{r} b_i^{(\nu)}u_i\right)!}$$

byl číslem celým pro všechna celistvá a posit. u.

Chceme podati ve zjednodušené formě Landauovo vyšetřování. Pro libovolné prvočíslo p musí býti dle Legendreovy formule

$$(2)\qquad \sum_{i=1}^{\infty}\sum_{\nu=1}^{m}\left[\frac{X_\nu}{p^i}\right]\geqq\sum_{i=1}^{\infty}\sum_{\nu=1}^{n}\left[\frac{Y_\nu}{p^i}\right].$$

Patrně ale stačí, je-li pro všechna p a i

$$(3) \qquad \sum_{\nu=1}^{m} \left[\frac{X_\nu}{p^i}\right] \geqq \sum_{\nu=1}^{n} \left[\frac{Y_\nu}{p^i}\right]$$

neboť součtem všech podobných nerovností obdržíme a fortiori nerovnost (2). Podmínka (3) tedy pro dělitelnost stačí. Jiná otázka je ovšem, je-li nutná. Lze ukázati, že ano.

Supponujme, že by bylo pro určitou soustavu proměnných $v_1, v_2, \ldots v_r$

$$\sum_{\nu=1}^{m} \left[\frac{X_\nu}{p^i}\right] < \sum_{\nu=1}^{n} \left[\frac{Y_\nu}{p^i}\right]$$

a položme ještě $p^i = N$.

Pak lze vždy určiti číslo ϱ takové, aby

$$(4) \qquad \begin{aligned} \varrho X_\nu(v) &< (\varrho N - N)^2 \quad \text{pro } \nu = 1, 2, 3, \ldots m, \\ \varrho Y_\nu(v) &< (\varrho N - N)^2 \quad \text{pro } \nu = 1, 2, 3, \ldots n, \end{aligned}$$

neboť je-li $\frac{\alpha}{\beta}$ libovolný zlomek, lze vždy stanoviti číslo ξ tak, aby $\alpha\xi < (\xi\beta - \beta)^2$ čili, aby $\frac{\alpha}{\beta^2} < \frac{(\xi-1)^2}{\xi}$; stačíť zvoliti na př. $\xi = \frac{\alpha + 2\beta^2}{\beta^2}$, načež bude

$$\alpha\xi = \frac{\alpha^2 + 2\alpha\beta^2}{\beta^2}, \qquad (\beta\xi - \beta)^2 = \frac{\alpha^2 + 2\alpha\beta^2 + \beta^4}{\beta^2}$$

a tedy vskutku $\alpha\xi < (\xi\beta - \beta)^2$. Platí-li nerovnost ta pro určité ξ, platí i pro každé větší ξ. Stanovíme-li tudíž pro zlomky

$$\frac{X_1(v)}{N}, \frac{X_2(v)}{N}, \ldots \frac{X_m(v)}{N}, \frac{Y_1(v)}{N}, \frac{Y_2(v)}{N}, \ldots \frac{Y_n(v)}{N}$$

příslušná čísla ξ a nazveme největší z nich ϱ, pak jsou splněny pro toto ϱ nerovnosti (4). Obdobným způsobem lze dokázati, že dá se vždy vyhledati číslo σ takové, že platí relace

$$(5) \qquad \left[\frac{\sigma X_\nu(v)}{\sigma N - N}\right] = \left[\frac{\sigma X_\nu(v)}{\sigma N}\right], \quad \left[\frac{\sigma Y_\nu(v)}{\sigma N - N}\right] = \left[\frac{\sigma Y_\nu(v)}{\sigma N}\right]$$

pro všechna $\nu = 1, 2, \ldots m$, resp. $\nu = 1, 2, \ldots n$.

Neboť jest možno zase ukázati, že dá se nalézti číslo η takové, že pro libovolný zlomek $\frac{\alpha}{\beta}$ a pro všechna $k < \eta$ platí

$$\left[\frac{\alpha}{\beta - k}\right] = \left[\frac{\alpha}{\beta}\right] \qquad 0 \leqq k < \eta.$$

Stačí totiž vzíti $\eta = \beta - \frac{\alpha}{\left[\frac{\alpha}{\beta}\right] + 1}$, načež pro každé $k = \beta - \frac{\alpha}{\left[\frac{\alpha}{\beta}\right] + 1 - \varepsilon}$ jest vztah žádaný splněn. Hodnotě $\varepsilon = \left[\frac{\alpha}{\beta}\right] + 1 - \frac{\alpha}{\beta}$ odpovídá $k = 0$.

Relace (5) lze tedy vskutku splniti, což je hned patrno, píšeme-li je ve tvaru

$$\left[\frac{X_\nu}{N - \frac{N}{\sigma}}\right] = \left[\frac{X_\nu}{N}\right], \quad \left[\frac{Y_\nu}{N - \frac{N}{\sigma}}\right] = \left[\frac{Y_\nu}{N}\right],$$

kdež jen třeba určiti σ z podmínky $\frac{N}{\sigma} = \eta$, takže relace ty budou platiti pro čísla σ větší než $\frac{N}{\eta}$. Stanovíme-li takto σ pro všechna $\nu = 1, 2, 3, \ldots m$, resp. $\nu = 1, 2, 3, \ldots n$, a zvolíme σ maximální, budou relace (5) platiti. Shrneme-li tudíž relace (4) a (5), vidíme, že lze vždy určiti číslo τ_1 tak, aby pro všechna $\tau > \tau_1$ bylo

$$\tau X_\nu(v) < (\tau N - \mu)^2, \qquad \tau Y_\nu(v) < (\tau N - \mu)^2$$

$$\nu = 1, 2, 3, \ldots m, \text{ resp. } \nu = 1, 2, 3, \ldots n,$$

$$\left[\frac{\tau X_\nu(v)}{\tau N - \mu}\right] = \left[\frac{X_\nu(v)}{N}\right], \quad \left[\frac{\tau Y_\nu(v)}{\tau N - \mu}\right] = \left[\frac{Y_\nu(v)}{N}\right]$$

$$\mu = 0, 1, 2, \ldots N.$$

Určíme-li ještě prvočíslo q tak, aby $\tau N - \mu = q$, bude patrně

(4a) $$X_\nu(\tau v) < q^2, \qquad Y_\nu(\tau v) < q^2,$$

$$(5a)\qquad \left[\frac{X_\nu(v)}{N}\right]=\left[\frac{X_\nu(\tau v)}{q}\right],\quad \left[\frac{Y_\nu(v)}{N}\right]=\left[\frac{Y_\nu(\tau v)}{q}\right].$$

Ze supposice

$$\sum_{\nu=1}^{m}{}^{\nu}\left[\frac{X_\nu(v)}{N}\right]<\sum_{\nu=1}^{n}{}^{\nu}\left[\frac{Y_\nu(v)}{N}\right]$$

plyne tudíž

$$\sum_{\nu=1}^{m}{}^{\nu}\left[\frac{X_\nu(\tau v)}{q}\right]<\sum_{\nu=1}^{n}{}^{\nu}\left[\frac{Y_\nu(\tau v)}{q}\right]$$

a z relace (4*a*) posléze

$$\sum_{k=1}^{\infty}{}^{k}\sum_{\nu=1}^{m}{}^{\nu}\left[\frac{X_\nu(\tau v)}{q^k}\right]<\sum_{k=1}^{\infty}{}^{k}\sum_{\nu=1}^{n}{}^{\nu}\left[\frac{Y_\nu(\tau v)}{q^k}\right],$$

neboť vymizí všechny členy až na první.

Jest tedy dokázáno: podmínka (3) je dostačující a nutná.

Píšeme-li v ní ještě $\frac{u_1}{p^k}=t_1, \frac{u_2}{p^k}=t_2, \ldots \frac{u_r}{p^k}=t_r$, bude pro dělitelnost nutnou a dostačující podmínka

$$(3)\qquad \sum_{\nu=1}^{m}{}^{\nu}[X_\nu(t)]\geqq\sum_{\nu=1}^{n}{}^{\nu}[Y_\nu(t)],$$

kdež t jsou čísla právě určená, tedy rationální.

Tato restrikce je ale zbytečná a lze lehko ukázati, že podmínka (3) musí pak platiti pro všechna reálná u.

Neboť kdyby bylo pro určitý systém proměnných (reálných) $u_1, u_2, \ldots u_r$, pro něž $X_\nu(u), Y_\nu'(u)\geqq 0$.

$$\sum_{\nu=1}^{m}{}^{\nu}[X_\nu(u)]<\sum_{\nu=1}^{n}{}^{\nu}[Y_\nu(u)],$$

bylo by též pro určitý systém *rationálných* t tvaru dříve uvedeného

$$(3^*)\qquad \sum_{\nu=1}^{m}{}^{\nu}[X_\nu(t)]<\sum_{\nu=1}^{n}{}^{\nu}[Y_\nu(t)].$$

Lze totiž vždy najíti takové δ, že pro $0\leqq h<\delta$,

$$\left[\frac{X_\nu(u)}{1-h}\right] = [X_\nu(u)], \quad \left[\frac{Y_\nu(u)}{1-h}\right] = [Y_\nu(u)].$$

(Plyne to z věty pro zlomek $\frac{\alpha}{\beta}$ odvozené, klademe-li $\beta = 1$). Tuto relaci možno též psáti

$$\left[X_\nu\left(\frac{u}{1-h}\right)\right] = [X_\nu(u)], \quad \left[Y_\nu\left(\frac{u}{1-h}\right)\right] = [Y_\nu(u)]$$

a tedy též

$$\sum_{\nu=1}^{m}{}^{\nu}\left[X_\nu\left(\frac{u}{1-h}\right)\right] < \sum_{\nu=1}^{n}{}^{\nu}\left[Y_\nu\left(\frac{u}{1-h}\right)\right].$$

Ale h dá se tak voliti, aby číslo $\frac{u}{1-h}$ (kde u jest reálné číslo), bylo číslem rationálným, nebo dokonce někdy celistvým. (Je-li na př. $u_1 = \sqrt{5}$, lze voliti $h = 1 - \frac{\sqrt{5}}{3}$, $1 - \frac{\sqrt{5}}{4}$, ... při čemž třeba ovšem ještě splniti podmínku $h < \delta = 1 - \frac{X_\nu(u)}{[X_\nu] - 1}$.)

Byla by tedy vskutku i pro t relace (3*) splněna, což je proti podmínce (3). Vidíme tedy: Nutnou a dostatečnou podmínkou, aby podíl P byl celým číslem, jest

$$\sum_{\nu=1}^{m}{}^{\nu}[X_\nu(u)] \geqq \sum_{\nu=1}^{n}{}^{\nu}[Y_\nu(u)]$$

pro všechna reálná u, pro něž X_ν, $Y_\nu \geqq 0$.

Pro praktická vyšetřování jest záhodno zkoumati, zda tato podmínka nedá se nahraditi jinou, při níž obor reálných čísel, pro něž nerovnost (5) má platiti, je sůžen na vhodně volený intervall.

Ukážeme snadno, že jest tomu tak a že stačí, platí-li vztah (5) pro všechna reálná čísla intervallu 0 — až — 1 (0, 1, inclusive), pro něž X_ν, Y_ν jsou positivní nebo rovny nulle $\left\{\begin{matrix}\nu = 1, 2, \ldots m\\ \nu = 1, 2, \ldots n\end{matrix}\right\}$. Že koefficient $a_k^{(\nu)}$, $b_k^{(\nu)}$ v lineárných homogenních funkcích

$$X_\nu = a_1^{(\nu)} u_1 + a_2^{(\nu)} u_2 + \ldots + a_r^{(\nu)} u_r,$$
$$Y_\nu = b_1^{(\nu)} u_1 + b_2^{(\nu)} u_2 + \ldots + b_r^{(\nu)} u_r,$$

musí býti positivní, jak jsme předpokládali, jest patrno hned, položíme-li na př. $u_1 = u_2 = \ldots = u_r = 0$, $u_k = 1$. Pak musí být $a_k^{(\nu)}$, $b_k^{(\nu)}$ positivní. Mimo to jsou ovšem celistvé.

Supponujme tedy, že jest pro všechna reálná u_i intervallu $(0 \leqq u_i \leqq 1)$, pro něž X_ν, $Y_\nu \geqq 0$

$$(6) \qquad \sum_{\nu=1}^{m} {}^{\nu} [X_\nu (u)] \geqq \sum_{\nu=1}^{n} {}^{\nu} [Y_\nu (u)].$$

Z toho plyne především pro

$$u_1 = u_2 = \ldots = u_{i-1} = u_{i+1} \ldots = u_r = 0, \quad u_i = 1,$$
$$a_i^{(1)} + a_i^{(2)} + \ldots + a_i^{(\nu)} + \ldots + a_i^{(m)} \geqq b_i^{(1)} + b_i^{(2)} + \ldots + b_i^{(n)}$$

čili

$$\sum_{\nu=1}^{m} {}^{\nu} a_i^{(\nu)} \geqq \sum_{\nu=1}^{n} {}^{\nu} b_i^{(\nu)},$$

pro všechna $i = 1, 2, \ldots r$. Jest tedy též pro pos. celé k_i

$$\sum_{\nu=1}^{m} {}^{\nu} a_i^{(\nu)} k_i \geqq \sum_{\nu=1}^{n} {}^{\nu} b_i^{(\nu)} k_i$$

a sečtením r těchto vztahů pro $i = 1, 2, \ldots r$ obdržíme

$$\sum_{\nu=1}^{m} {}^{\nu} X_\nu (k) \geqq \sum_{\nu=1}^{n} {}^{\nu} Y_\nu (k).$$

pro celistvá a positivní $k_1, k_2, \ldots k_r$.

Vedle toho jest dle supposice pro u_i intervallu $(0 \ldots 1)$

$$\sum_{\nu=1}^{m} {}^{\nu} [X_\nu (u)] \geqq \sum_{\nu=1}^{n} {}^{\nu} [Y_\nu (u)]$$

a tedy součtem obou posledních nerovností, vzpomeneme-li, že pro celé α jest $[\alpha + \beta] = \alpha + [\beta]$,

$$\sum_{\nu=1}^{m} {}^{\nu} [X_\nu (u + k)] \geqq \sum_{\nu=1}^{n} {}^{\nu} [Y_\nu (u + k)].$$

Ale $k+u$ probíhá patrně všechna positivní reálná čísla, probíhá-li k všechna celá positivná čísla a u všechna čísla intervallu $0 \ldots 1$.

Tím je tedy dokázána věta:

Je-li pro všechny možné systémy realných čísel u $(0 \leqq u \leqq 1)$, pro něž $X_\nu(u) \geqq 0$, $Y_\nu(u) \geqq 0$,

$$\sum_{\nu=1}^{m} [X_\nu(u)] \geqq \sum_{\nu=1}^{n} [Y_\nu(u)],$$

pak jest podíl

$$P = \frac{\prod_{\nu=1}^{m} X_\nu(u)!}{\prod_{\nu=1}^{n} Y_\nu(u)!}$$

celým číslem.

Jakožto příklad dokažme, že $\dfrac{(5x+y)!\,(3y)!\,(x+5y)!\,(3x)!}{(x!)^3\,(y!)^3\,(x+2y)!^2\,(y+2x)!^2}$ jest celým číslem.

K tomu cíli nutno dokázati pro všechna x, y intervallu $(0, 1)$ platnost relace

$$[5x+y]+[x+5y]+[3x]+[3y] \geqq .3[x]+.3[y]+2[x+2y]+2[y+2x].$$

Pro 0,0 obdržíme na obou stranách 0. Pro 0,1 na levo 9 a na pravo rovněž 9.

Obdobně pro $x=1$, $y=0$. Pro $x=1$, $y=1$ na obou stranách 18.

Zbývá tedy dokázati platnost relace té pro

$$0<x<1, \quad 0<y<1.$$

Pro $x=y$ máme na levo $2[6x]+2[3x]$, na pravo $2[3x]+4[3x]$ a tedy relace splněna. Zbývá $x \lesssim y$. Vzhledem k symmetrii výrazu zvolme bez újmy všeobecnosti $x>y$. Pak jest

$$[5x+y]>[2x+y]+[3x]>[2x+y]+[2x+y]$$
$$[x+5y]>[x+2y]$$
$$[3x]>[x+2y],$$

tedy levá strana větší než

$$2[x+2y]+2[y+2x]$$

a větší než pravá strana, kde členy $3[x]+3[y]$ mají hodnotu 0.

Rovněž lze dokázati, že

$$\frac{(4x)!(4y)!}{x!y!(x+2y)!(y+2x)!}$$

jest číslem celým.

5. Jakožto další applikaci Legendreovy formule dokažme větu:

Jsou-li m a n čísla nesoudělná, jest

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

číslem celým.

Podíl ten lze psáti též ve tvaru

$$\frac{(m+n-1)!}{n!\,m!}.$$

Libovolné prvočíslo p bude obsaženo v čítateli s mocnitelem

$$\alpha(m+n-1)=\sum_{i=1}^{\infty}\left[\frac{m+n-1}{p^i}\right],$$

v jmenovateli s mocnitelem rovným

$$\alpha(n)+\alpha(m)=\sum_{i=1}^{\infty}\left[\frac{m}{p^i}\right]+\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right].$$

Třeba tudíž zase dokázati, že

$$\left[\frac{m+n-1}{p^i}\right]\geqq\left[\frac{m}{p^i}\right]+\left[\frac{n}{p^i}\right]$$

pro libovolné prvočíslo p a libovolné i.

To je ale hned viděti, píšeme-li $m=\mu p^i+r_1$, $n=\nu p^i+r_2$ kde r_1, r_2 jsou zbytky menší než p^i, takže $\left[\frac{m}{p^i}\right]=\mu$, $\left[\frac{n}{p^i}\right]=\nu$.

Máme tedy na levé straně relace

$$\left[\frac{m+n-1}{p^i}\right]=\mu+\nu+\left[\frac{r_1+r_2-1}{p^i}\right];$$

r_1, r_2 jsou ale celá čísla, která nemohou býti, vzhledem k nesoudělnosti čísel m, n, současně nullou. Na levo je v nejhorším případě $\mu + \nu$, nebo též $\mu + \nu + 1$, na pravo ale jen $\mu + \nu$. Relace tvrzená je tedy dokázána.

Ostatně lze tuto větu dokázati též přímo na základě věty: součin r za sebou jdoucích čísel je dělitelný součinem r prvých čísel.

Jest totiž jednak $\dfrac{(m+1)(m+2)\ldots(m+n-1)}{1.2\ldots(n-1)}$ celým číslem, jednak též

$$\frac{(m+1)(m+2)\ldots(m+n)}{1.2\ldots n} = \frac{(m+1)(m+2)\ldots(m+n-1)}{1.2\ldots(n-1)} \cdot \frac{m+n}{n}.$$

Vzhledem ale k tomu, že jest $[m, n]^*) = 1$, jest $(m+n)$ nedělitelno číslem n a tedy musí býti n obsaženo již v součinu $(m+1)(m+2)\ldots(m+n-1)$.

6. Buďtež m, n celá positivní čísla. Podíl

$$\frac{n(n+1)(n+2)\ldots(mn-1)}{m^n}$$

jest číslem celým, je-li m číslem složeným, zlomkem, je-li m prvočíslem.

a) Budiž m prvočíslem $= p$. Podíl lze psáti ve tvaru

$$\frac{(np-1)!}{p^n(n-1)!}$$

Pak bude obsaženo p v čítateli s mocnitelem

$$\alpha(np-1) = \sum_{i=1}^{\infty} \left[\frac{np-1}{p^i}\right].$$

Můžeme ale ukázati, že

$$\left[\frac{np-1}{p^i}\right] = \left[\frac{n-1}{p^{i-1}}\right],$$

neboť

*) Toto označení zavádí se nyní pro největšího společného dělitele čísel m, n.

$$\frac{np-1}{p^i} = \frac{n-1}{p^{i-1}} + \frac{p-1}{p^i} \quad \text{a} \quad \frac{p-1}{p^i} < \frac{1}{p^{i-1}}.$$

Následkem toho jest též

$$\alpha(np-1) = \left[\frac{np-1}{p}\right] + \sum_{i=2}^{\infty} \left[\frac{n-1}{p^{i-1}}\right].$$

V jmenovateli je naproti tomu obsaženo p s mocnitelem β

$$\beta = n + \sum_{i=1}^{\infty} \left[\frac{n-1}{p^i}\right] = n + \sum_{i=2}^{\infty} \left[\frac{n-1}{p^{i-1}}\right].$$

Poněvadž jest ještě $\left[\frac{np-1}{p}\right] = n-1$, jest patrně $\alpha(np-1) < \beta$ čímž věta tvrzená dokázána.

b) Budiž m číslo složené a tedy $m = p^\varrho q$, kdež p jest prvočíslo, p vyskýtá se pak v jmenovateli podílu

$$\frac{n(n+1)\ldots(mn-1)}{m^n}$$

jako činitel s exponentem $n\varrho$, kdežto v čítateli s mocnitelem

$$x = \alpha(nm-1) - \alpha(n-1) = \sum_{i=1}^{\infty} \left[\frac{np^\varrho q - 1}{p^i}\right] - \sum_{i=1}^{\infty} \left[\frac{n-1}{p^i}\right].$$

Jest ale hned patrno, že platí vztahy

$$\left[\frac{np^\varrho q - 1}{p^{\varrho+1}}\right] \geqq \left[\frac{n-1}{p}\right], \quad \left[\frac{np^\varrho q - 1}{p^{\varrho+2}}\right] \geqq \left[\frac{n-1}{p^2}\right]$$

a t. d. pro všechna $i > \varrho$ a tedy

$$x \geqq \left[\frac{np^\varrho q - 1}{p}\right] + \left[\frac{np^\varrho q - 1}{p^2}\right] + \ldots + \left[\frac{np^\varrho q - 1}{p^\varrho}\right]$$

$$x \geqq nq(1 + p + p^2 + \ldots + p^{\varrho-1}) - \varrho = nq\,\frac{p^\varrho - 1}{p-1} - \varrho.$$

Stačí tudíž dokázati, že

$$nq\,\frac{p^\varrho - 1}{p-1} - \varrho \geqq n\varrho.$$

Je-li $\varrho = 1$, musí býti $q \geqq 2$, a potom jest $nq - 1$ vskutku ne menší než n.

Je-li $\varrho > 1$ a píšeme-li $p = 1 + r$, kdež $r \geqq 1$, můžeme relaci, již máme dokázati, uvésti v tvar

$$nq\left((1+r)^{\varrho} - 1\right) \geqq (n+1)\,\varrho \,.\, r.$$

Levá strana jest ale větší než

$$nq\varrho r + nq\,\frac{\varrho(\varrho-1)}{2}\,r^2.$$

Pro $\varrho > 1$, $r \geqq 1$, $n > 1$ jest $(q \geqq 1)$

$$nq\varrho r \geqq n\varrho r$$
$$nq\,\frac{\varrho(\varrho-1)}{2}\,r^2 \geqq \varrho r$$

a tedy jest relace správná pro všechny případy.

Dlužno ještě podotknouti, že předpoklad $n > 1$ jest nutný, neboť jinak by nám bylo co činiti se vztahem

$$\frac{\varrho-1}{2}qr \geqq 1 \quad \text{čili} \quad (\varrho-1)qr \geqq 2 \quad \text{pro} \quad r \geqq 1,\ q \geqq 1,\ \varrho > 1.$$

Tato relace není ale splněna pro $\varrho = 2$, $q = 1$, $r = 1$, $p = 2$, $n = 1$. Vskutku podíl $\frac{1.2.3}{4}$ není celým číslem.

Pro $n = 1$ máme tedy větu: $\frac{1.2.3\ldots(m-1)}{m}$ jest číslem celým pro všechna složená m vyjma $m = 4$, zlomkem pro m prvočíselné a $m = 4$ (což je ostatně hned viděti).

7. Abychom také ukázali, jak lze s výhodou užiti kombinatoriky při vyšetřování dělitelnosti čísel, dokážeme, že číslo celé $\frac{(na)!}{(a!)^n} = Q$ je dělitelno ještě faktoriellou $n!$ Že jest Q číslem celým, plyne ihned z toho, že $\frac{(a_1 + a_2 + \ldots + a_n)!}{a_1!\,a_2!\ldots a_n!}$ jest číslem celým. Položíme-li tu $a_1 = a_2 = \ldots = a_n = a$, jest ihned celistvost čísla Q patrna.

Mějmež nyní $N = na$ elementů. Tvořme všechny možné formace z těchto na elementů a sice tak, aby každá formace

čítala n skupin po a prvcích; za různé platí jen ty formace, při kterých se od sebe liší skupiny aspoň jedním prvkem. Jest otázka, kolik různých formací lze z N prvků vytvořiti.

Zvolme libovolnou formaci a permutujme v ní předem prvky v jednotlivých skupinách o sobě; tak obdržíme $(a!)^n$ útvarů. Vedle toho lze ještě skupiny navzájem permutovati a sice $n!$-kráte. Tak obdržíme v celku z této jediné $n!(a!)^n$ formací, jež platí za jedinou. Je-li tedy x počet různých formací, bude $x \,.\, n!(a!)^n$ patrně značiti počet všech permutací z $N = an$ prvků a tedy

$$x = \frac{N!}{n!(a!)^n} = \frac{(an)!}{n!(a!)^n} = \text{jakožto počet číslo celé.}$$

Téže methody lze užiti, abychom ukázali, že $\dfrac{N!}{b!(a!)^n n!}$ jest celým číslem, kdež $N = b + an$.

Ostatně jest to patrné, neboť $(b + an)!$ je dělitelno součinem $b!(an)!$ a $(an)!$ je dělitelno $(a!)^n n!$

Obecně jest $N!$ dělitelno součinem

$$b_1!\, b_2! \ldots b_r!\, (a_1!)^{n_1} (a_2!)^{n_2} \ldots (a_s!)^{n_s} n_1! \ldots n_s!,$$

je-li $N = b_1 + b_2 + \ldots + b_r + a_1 n_1 + a_2 n_2 + \ldots + a_s n_s$.

Je-li dále $N = a_1 a_2 a_3$, jest $N!$ dělitelno součinem $(a_2 a_3)!\,(a_1!)^{a_2 a_3}$ a tedy

$$\frac{N!}{(a_1!)^{a_2 a_3} (a_2!)^{a_3} a_3!}$$

celým číslem; podobně pro $N = a_1 a_2 a_3 a_4$ jest

$$\frac{N!}{(a_1!)^{a_2 a_3 a_4} \,.\, (a_2!)^{a_3 a_4} \,.\, (a_3!)^{a_4} \,.\, a_4!}$$

celým číslem. Je-li ještě $a_1 = a_2 = a_3 = a_4$, jest

$$\frac{a^4!}{(a!)^{a^3 + a^2 + a + 1}}$$

číslem celým a obecně

$$\frac{a^n!}{(a!)^{a^{n-1} + a^{n-2} + \ldots a + 1}} = \frac{a^n!}{(a!)^{\frac{a^n - 1}{a - 1}}}$$

číslem celým.

Podle toho jest ku př. $30!$ dělitelno $(3!)^{10}(5!)^2 2!$ a $25!$ jest dělitelno součinem $(5!)^6$. V jednotlivých případech lze ovšem meze dělitelnosti ještě značně rozšířiti.

Větu: $(an)!$ je dělitelno součinem $(a!)^n n!$ lze dokázati též přímo.

Stačí patrně, je-li pro libovolné prvočíslo p

$$\sum_{i=1}^{\infty} \left[\frac{an}{p^i}\right] \geqq \sum_{i=1}^{\infty} n\left[\frac{a}{p^i}\right] + \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right].$$

Není-li a dělitelno číslem p, dá se tento vztah lehko dokázati, neboť v tomto případě jest $\left[\frac{a}{p^i}\right] = \left[\frac{a-1}{p^i}\right]$, takže pravá strana zní

$$n\sum_{i=1}^{\infty}\left[\frac{a-1}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right],$$

kdežto na levé straně

$$\left[\frac{an}{p^i}\right] = \left[\frac{(a-1)n}{p^i} + \frac{n}{p^i}\right] \geqq \left[\frac{(a-1)n}{p^i}\right] + \left[\frac{n}{p^i}\right] \geqq n\left[\frac{a-1}{p^i}\right] + \left[\frac{n}{p^i}\right]$$

Jest tedy vskutku relace správná.

Je-li ale a dělitelno prvočíslem p, lze klásti $a = p^\delta c$, kde p^δ je nejvyšší mocnina prvočísla p obsažená v a, takže c je číslem p nedělitelno.

Potom jest na levé straně

$$\sum_{i=1}^{\infty}\left[\frac{an}{p^i}\right] = p^{\delta-1}cn + p^{\delta-2}cn + \ldots pcn + cn + \sum_{i=1}^{\infty}\left[\frac{cn}{p^i}\right],$$

kdežto na pravé

$$n\sum_{i=1}^{\infty}\left[\frac{a}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right] = p^{\delta-1}cn + p^{\delta-2}cn + \ldots + cn + n\sum_{i=1}^{\infty}\left[\frac{c}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right];$$

zbývá tedy dokázati, že

$$\sum_{i=1}^{\infty}\left[\frac{cn}{p^i}\right] \geqq n\sum_{i=1}^{\infty}\left[\frac{a}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right],$$

kdež c je nedělitelno číslem p; to je ale právě předešlý dokázaný případ.

8. Některé z vět o dělitelnosti zakládají se na vyjadřování čísel v soustavách číselných, jichž základem jest prvočíslo. Především lze udati velmi jednoduchou formuli pro funkci $\alpha(n)$, je-li číslo n napsáno v soustavě číselné o základu p, kdež p jest prvočíslo, pro něž mocnitele $\alpha(n)$ vyšetřujeme.

Budiž tedy $n = a_0 + a_1 p + a_2 p^2 + \ldots + a_m p^m$, pak jest opět mocnitel $\alpha(n)$:

$$\alpha(n) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right].$$

$$\left[\frac{n}{p}\right] = a_1 + a_2 p + \ldots + a_m p^{m-1}$$

$$\left[\frac{n}{p^2}\right] = a_2 + a_3 p + \ldots + a_m p^{m-2}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\left[\frac{n}{p^{m-1}}\right] = a_{m-1} + a_m p$$

$$\left[\frac{n}{p^m}\right] = a_m,$$

tedy

$$\alpha(n) = a_1 + a_2 \frac{p^2 - 1}{p - 1} + a_3 \frac{p^3 - 1}{p - 1} + \ldots$$

$$+ a_m \frac{p^m - 1}{p - 1} = \frac{a_0 + a_1 p + \ldots + a_m p^m - a_0 - a_1 - \ldots - a_m}{p - 1}$$

$$\alpha(n) = \frac{n - \sigma(n)}{p - 1},$$

kdež $\sigma(n)$ značí cifferný součet čísla n.

Pro $p = 2$ obdržíme zvláště jednoduchý výsledek.

Této formule lze užiti při některých důkazech. Chceme pomocí vzorce toho ukázati, že za určitých okolností se dá podíl $\frac{(an)!}{(a!)^n n!}$ ještě dále beze zbytku děliti vyšší mocninou čísla $n!$

Bezprostředně jest patrna správnost relace

$$\sigma(a) + \sigma(n) = \sigma(a + n) + k(p - 1),$$

při čemž k značí počet jedniček, které se při sčítání z jednoho sloupce do druhého přenášejí.

Podobně jest pro součin ciffernych součtů

$$\sigma(a)\sigma(n) = \sigma(na) + (p-1)k,$$

kdež k nyní značí celkový počet jedniček přenesených při násobení v řádcích a při konečném sčítání.

Ku př. v 5-ové soustavě jest

$$\begin{array}{r} \underline{4\ 2} \times 23 \\ 2_2 3_1 1 \\ \underline{1_1 3\ 4} \\ 2_1 1_1 2\ 1 \end{array}$$

tedy

$$k = 6, \qquad \sigma(a)\sigma(n) = 30,$$
$$\sigma(an) + 4k = 6 + 24 = 30.$$

Nejvyšší mocnina prvočísla p obsažená ještě v podílu $\frac{(na)!}{(a!)^n n!}$ bude míti podle toho mocnitele:

$$\frac{na - \sigma(an) - na + n\sigma(a) - n + \sigma(n)}{p-1} = \varepsilon$$

$$\varepsilon = \frac{n\left(\sigma(a)-1\right) + \sigma(n) - \sigma(a)\sigma(n)}{p-1} + k = \frac{\left(\sigma(a)-1\right)\left(n - \sigma(n)\right)}{p-1} + k$$
$$= \alpha_p(n)\left(\sigma(a)-1\right) + k,$$

slovy vyjádřeno, p je v podílu tom obsaženo beze zbytku v mocnině téže jako v $(n!)^{\sigma(a)-1}$, při čemž vynecháme číslo $k \geqq 0$.

Z toho plyne, že, vyjádříme-li a ve všech číselných soustavách pro prvočíselná p menší nebo rovná a a je-li τ minimální hodnota číselné funkce $\sigma(a)$ pro různé ty soustavy, že podíl $\frac{(na)!}{(a!)^n n!}$ je dělitelný ještě mocninou $(n!)^{\tau-1}$.

V některých případech dá se rozhodnouti hned, je-li podíl ten dělitelen ještě mocninou $(n!)$; ku př. je-li a mocninou libovolného prvočísla, tedy $a = p^i$, bude pro soustavu číselnou o základě p, $\sigma(a) = 1$ a tedy $\varepsilon - k = 0$ a tedy též $\tau - 1 = 0$:

Je-li a mocninou nějakého prvočísla, pak není podíl $\frac{(na)!}{(a!)^n n!}$ dělitelný žádnou další mocninou $n!$

Co se týče čísla k, tu může toto někdy dělitelnost dalšími mocninami $(n!)$ rozšířiti, je-li $> \alpha_p(n) = \frac{n - \sigma(n)}{p-1}$ pro všechna prvočísla p od 2 až do většího z obou čísel a, n.

Jindy je to nemožno a pak je $\tau - 1$ vskutku nejvyšším exponentem faktorielly $n!$, jejíž mocninou je podíl $\frac{(an)!}{(a!)^n n!}$ ještě dělitelný. Tak jest tomu ku př. pro $a \leqq n$, neboť pak jest $k < \frac{n - \sigma(n)}{p-1}$ aspoň pro jedno prvočíslo; pro $p = 2$ se to dá velmi jednoduše dokázati.

Příklad $60!$ jest dělitelno $(6!)^{10} . 10!$ Vyjádříme-li 6 v soustavě dvojkové, trojkové a pětkové, obdržíme resp.

$$6 = 110,\ 20,\ 11, \text{ tedy } \tau(6) = 2.$$

Jest tudíž ještě

$$\frac{60!}{(6!)^{10}(10!)^2}$$

celým číslem.

Z jiných vět sem patřících uvádíme ještě: Jsou-li a, n 2 libovolná celá čísla, napsaná v soustavě p-cifferné (p prvočíslo), jest nejvyšší mocnina čísla p obsažená v $n!$ $p^{\alpha(n)}$; pak bude součin $(a+1)(a+2)\ldots(a+n) = \frac{(a+n)!}{a!}$ dělitelný mocninou $p^{\alpha+k}$, kdež k značí opět počet jedniček přenesených při sčítání čísel a, n.

Důkaz jest snadný. Je totiž

$$\alpha(a) = \frac{a - \sigma(a)}{p-1},\ \alpha(n) = \frac{n - \sigma(n)}{p-1},\ \alpha(a+n) = \frac{n + a - \sigma(a+n)}{p-1}$$

a hledaný exponent $= \alpha(a+n) - \alpha(a)$

$$= \frac{n - \sigma(a+n) + \sigma(a)}{p-1} = \frac{n - \sigma(n)}{p-1} + k = \alpha(n) + k.$$

9. Zvolíme-li n různých celých čísel α_1, α_2, α_3, $\ldots$ α_n a utvoříme z nich součin:

$(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)\ldots(\alpha_1 - \alpha_n)(\alpha_2 - \alpha_3)\ldots(\alpha_2 - \alpha_n)\ldots(\alpha_{n-1} - \alpha_n)$,
bude součin ten dělitelný součinem faktoriell

$$(n-1)!(n-2)!\ldots 3!2!1!$$

Tedy:

$$\frac{\Pi(\alpha_i - \alpha_k)}{\Pi(i-k)}$$

jest celým číslem, při čemž $k > i$ a i probíhá řadu čísel $1, 2, 3, \ldots n-1$, kdežto $k = 2, 3, \ldots n$, neboť je patrno, že

$$\Pi(i-k) = (n-1)!(n-2)!\ldots 3!2!1!$$

Tuto zajímavou větu lze odvoditi snadno z nauky o determinantech a sice z theorie t. zv. mocninných determinantů.[1]) Vzhledem k důležitosti její podáváme zde důkaz od nauky o determinantech neodvislý.

Patrně stačí opět, dokážeme-li, že libovolné prvočíslo p jest obsaženo v čítateli podílu s mocninou nejméně tak vysokou jako v jmenovateli.

V jmenovateli $(n-1)!(n-2)!\ldots 3!2!1!$ je prvočíslo p obsaženo s mocnitelem

$$\alpha(n-1) + \alpha(n-2) + \ldots + \alpha(3) + \alpha(2) + \alpha(1)$$
$$= \sum_{i=1}^{\infty} \left\{ \left[\frac{n-1}{p^i}\right] + \left[\frac{n-2}{p^i}\right] + \ldots + \left[\frac{3}{p^i}\right] + \left[\frac{2}{p^i}\right] \right\}.$$

Označíme-li k vůli stručnosti $p^i = q$, jde o určení součtu

$$\left[\frac{n-1}{q}\right] + \left[\frac{n-2}{q}\right] + \ldots \left[\frac{3}{q}\right] + \left[\frac{2}{q}\right] + \left[\frac{1}{q}\right].$$

Položme ještě $n-1 = aq + \delta$, kdež $0 \leqq \delta < q$ a tedy $\left[\frac{n-1}{q}\right] = a$.
Pak jest možno součet ten rozložiti v částečné součty

$$\left[\frac{1}{q}\right] + \left[\frac{2}{q}\right] + \ldots + \left[\frac{q-1}{q}\right] = 0 \cdot q$$
$$\left[\frac{q}{q}\right] + \left[\frac{q+1}{q}\right] + \ldots + \left[\frac{2q-1}{q}\right] = 1 \cdot q$$

---

[1]) Viz *Studnička*: Úvod do nauky o determinantech str. 95. a násl.

$$\left[\frac{2q}{q}\right]+\left[\frac{2q+1}{q}\right]+\ldots+\left[\frac{3q-1}{q}\right]=2\,.\,q$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\left[\frac{(a-1)q}{q}\right]+\left[\frac{(a-1)q+1}{q}\right]+\ldots+\left[\frac{(a-1)q+q-1}{q}\right]$$
$$=(a-1)q$$

$$\left[\frac{aq}{q}\right]+\left[\frac{aq+1}{q}\right]+\ldots+\left[\frac{aq+\delta}{q}\right]=(\delta+1)a.$$

Sečtením obdržíme tedy

$$\left[\frac{n-1}{q}\right]+\left[\frac{n-2}{q}\right]+\ldots+\left[\frac{3}{q}\right]+\left[\frac{2}{q}\right]+\left[\frac{1}{q}\right]$$
$$=\frac{a(a-1)q}{2}+(\delta+1)a=\frac{a(a-1)q}{2}+(n-aq)a$$
$$=a\left(n-\frac{q}{2}\right)-\frac{a^2q}{2}\,.$$

Třeba podotknouti, že je $\left[\frac{n-1}{q}\right]=\left[\frac{n}{q}\right]=a$ ve všech případech až na ten, kdy n je dělitelno q a tedy $\frac{n}{q}$ celým číslem. V tomto případě je hodnota součtu jednodušší. Je tu totiž $\left[\frac{n-1}{q}\right]=a=\frac{n}{q}-1$; dosadíme-li a zjednodušíme, obdržíme $\frac{n}{2}\left(\frac{n}{q}-1\right)$. Podle toho bude mocnitel, s nímž je ještě obsaženo p v jmenovateli podílu:

$$\sum_{i=1}^{\infty}{}^{i}\,a\left(n-\frac{p^i}{2}\right)-\frac{a^2p^i}{2}=\sum_{i=1}^{\infty}{}^{i}\left\{\left[\frac{n-1}{p^i}\right]\left(n-\frac{p^i}{2}\right)-\frac{p^i}{2}\left[\frac{n-1}{p^i}\right]^2\right\}.$$

Při tom se pokračuje ve sčítání tak dlouho, až $\left[\frac{n-1}{p^k}\right]=0$.

Obraťme se nyní k čítateli. Zde si usnadníme práci tím, že zvolíme případ, který je pro větu naši nejnepříznivější, tedy ten, kdy v čítateli je co nejméně differencí čísel $\alpha_k-\alpha_i$ dělitelných číslem q. Abychom případ ten stanovili, dělme čísla $\alpha_1, \alpha_2, \ldots \alpha_n$ číslem q a všechna α_k o stejném zbytku shrňme vždy do jedné třídy. Tak obdržíme určitý počet tříd a v každé

určitý počet čísel α shodných (mod q). Tvoříme-li rozdíly v jednotlivých třídách, budou tyto vesměs dělitelny číslem q a sice, je-li v některé třídě obsaženo β elementů α_k, bude patrně počet rozdílů = počtu kombinací 2. třídy, tedy $\frac{\beta(\beta-1)}{2}$ rozdílů, které jsou vesměs dělitelny q. Při tom jest počet tříd nanejvýše roven q, neboť tolik jest nejvýše různých zbytků.

Lze nyní snadno nahlédnouti, že, čím méně bude tříd, tím více prvků bude v nich, a jak výraz $\frac{\beta(\beta-1)}{2}$ ukazuje, tím více rozdílů dělitelných číslem q. Dále, čím více se liší třídy počtem elementů α, tím více bude rozdílů dělitelných číslem q. Máme-li na př. 2 třídy s počty prvků β, γ, tož jest počet differencí dělitelných q ze 2 těchto tříd

$$x = \frac{\beta(\beta-1)}{2} + \frac{\gamma(\gamma-1)}{2} = \frac{\gamma^2+\beta^2-\beta-\gamma}{2}$$

$$= \gamma^2 + \frac{\eta^2}{2} + \eta\gamma - \frac{\eta+\gamma}{2},$$

klademe-li

$$\beta = \eta + \gamma.$$

Roste-li η, roste též x; minimum bude x míti pro $\eta = 0$ nebo $\eta = 1$.

V celku je tedy viděti: Nejnepříznivější případ je ten, když máme pokud možno nejvíce tříd, tedy q, a když třídy ty mají všechny stejný počet prvků anebo jich počty se liší pouze o 1.

Prvý případ je možný pouze, je-li n (počet všech α) dělitelno počtem všech různých zbytků q. Pak máme tedy q tříd o $\frac{n}{q}$ prvcích, takže počet všech differencí dělitelných q obnáší

$$q \cdot \frac{n}{2q}\left(\frac{n}{q}-1\right) = \frac{n}{2}\left(\frac{n}{q}-1\right);$$

to je zároveň exponent, s nímž je q obsaženo v čítateli.

Není li n dělitelno q, pak máme n prvků a různých zbytků (tříd) jen q, takže se aspoň jeden ze zbytků musí nejméně $\left[\frac{n}{q}\right]$krát opakovati.

V nepříznivém případě, jejž jsme zvolili, budeme míti tedy ξ tříd o $\left[\frac{n}{q}\right]$ prvcích a ξ tříd o $\left[\frac{n}{q}\right]+1$ prvcích, takže jest

$$\xi \cdot \left[\frac{n}{q}\right] + \xi \left(\left[\frac{n}{q}\right]+1\right) = n$$
$$\xi + \xi = q$$

a odtud, zavedeme-li opět

$$\left[\frac{n}{q}\right] = \left[\frac{n-1}{q}\right] = a.$$
$$\xi = q - n + aq, \qquad \xi = n - aq.$$

V tomto nejhorším případě jest tudíž počet differencí dělitelných číslem q

$$y = \frac{1}{2}(q - n + aq)(a-1)\,a + \frac{1}{2}(n - aq)\,a(a+1)$$
$$= a\left(n - \frac{q}{2}\right) - \frac{a^2 q}{2}.$$

Utvoříme-li součin

$$\begin{aligned}
&(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \ldots (\alpha_1 - \alpha_n)\\
&\qquad (\alpha_2 - \alpha_3) \ldots (\alpha_2 - \alpha_n)\\
&\ldots\ldots\ldots\ldots \qquad \ldots\ldots\ldots\\
&\qquad\qquad\qquad\qquad (\alpha_{n-1} - \alpha_n),
\end{aligned}$$

bude tento dělitelen tedy mocninou $q^{a\left(n-\frac{q}{2}\right)-\frac{a^2q}{2}}$ a protože totéž bylo by možno dokázati pro libovolnou jinou mocninu p^l prvočísla p, jest patrně mocnitel čísla p, s nímž je toto obsaženo v součinu, vyjádřen týmž součtem jako dříve. Tím je věta dokázána.

Z věty té lze odvoditi různé speciální poučky.

Užijeme-li jí pro čísla a, $a+b$, $a+b^2, \ldots a+b^n$, bude zníti věta následovně:

Součin

$$(b^{n-1}-1)(b^{n-2}-1)^2(b^{n-3}-1)^3 \ldots (b-1)^{n-1}$$

násobený jistou mocninou čísla b, jest dělitelný součinem

$$n!\,(n-1)!\,(n-2)!\,\ldots\,3!\,2!\,1!$$

Je-li ještě b rel. prvočíslem vzhledem k $n, n-1, \ldots 3, 2, 1$, tož odpadne onen činitel.

Na př. pro $b=7, n=6, (7^5-1)(7^4-1)^2(7^3-1)^3(7^2-1)^4(7-1)^5$ je dělitelno $6!\,5!\,4!\,3!\,2!\,1$.

Je-li dále

$$\alpha_1 = a, \quad \alpha_2 = a + b_1, \quad \alpha_3 = a + b_2, \quad \ldots \quad \alpha_{n+1} = a + b_n,$$

kde a, b_1, b_2, $\ldots$ b_n jsou libovolná čísla, jest dle věty naší $b_1 b_2 \ldots b_n \Pi(b_k - b_i)$ dělitelno součinem $n!\,(n-1)!\ldots 3!\,2!\,1!$ a jsou-li b_1, b_2, $\ldots$ b_n rel. prvoč. vzhledem k

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

jest $\Pi(b_k - b_i)$ dělitelno přímo $n!\,(n-1)!\,\ldots\,3!\,2!\,1!$

10. Téměř všechny dosavadní úvahy zakládaly se na použití věty:

Nejvyšší mocnitel, s nímž prvočíslo p jest obsaženo v součinu $n!$, jest vyjádřen součtem:

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = \alpha(n),$$

při čemž se sčítá až po $i = \varrho$ takové, že $\left[\frac{n}{p^\varrho}\right] > 0$, $\left[\frac{n}{p^{\varrho+1}}\right] = 0$.

Tato věta nám dovoluje vyjádřiti faktoriellu $n!$ tvarem, který někdy prokazuje v číselné theorii dobré služby. Poněvadž věta platí patrně pro všechna $p \leqq n$, jest

$$n! = \Pi_p p^{\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]}$$

čili

$$\log(n!) = \sum_p \log p \,.\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots \left[\frac{n}{p^\varrho}\right]\right);$$

při tom součin (součet) se vztahuje na všechna prvočísla p.

Pro $\log(n!)$ lze ale obdržeti jiný výraz, který se obzvláště dobře hodí pro vyšetřování různých asymptotických zákonů na-

uky o číslech. Tento jednoduchý a zajímavý výraz je založen na funkci $\Theta(n)$ definované následovně:

$$\Theta(n) = \sum_{p} \tau \log p;$$

součet se vztahuje na všechna prvočísla p, která nepřevyšují čísla n, a τ je mocnitel nejvyšší mocniny čísla p, která není větší než n. Budiž podotčeno, že z této definice se dá lehko vyvoditi pro $\Theta(n)$ následující výraz [1])

$$\Theta(n) = -\Sigma\mu(k)\left[\frac{n}{k}\right]\log k, \quad k = 1, 2, \ldots n.$$

Věta, kterou chceme uvésti, je následující Čebyševova relace:

$$(1.) \quad \log(n!) = \Theta(n) + \Theta\left(\frac{n}{2}\right) + \Theta\left(\frac{n}{3}\right) + \ldots + \Theta\left(\frac{n}{n}\right).$$

Dosadíme-li na levo za $\log(n!)$ výraz svrchu napsaný a užijeme-li definice pro $\Theta(n)$, bude třeba dokázati, že

$$\sum_{p} \log p \cdot \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

$$= \sum_{p} \tau_n \log p + \sum_{p} \tau_{\frac{n}{2}} \log p + \ldots \sum_{p} \tau_{\frac{n}{n}} \log p.$$

Při tom na levo sčítá se přese všechna prvočísla $p \leqq n$, kdežto v prvém součtu na pravo přese všecka prvočísla, jež nepřevyšují n, v druhém přes prvočísla, která nepřevyšují $\frac{n}{2}$ a t. d.; τ_n má při tom význam nejvyššího mocnitele prvočísla d takového, že $p^{\tau_n} \leqq n < p^{\tau_n+1}$, obdobně jest $p^{\tau_{\frac{n}{2}}} \leqq \frac{n}{2} < p^{\tau_{\frac{n}{2}}+1}$ a t. d. Z toho plyne:

$$\tau_n = \left[\frac{\log n}{\log p}\right], \quad \tau_{\frac{n}{2}} = \left[\frac{\log \frac{n}{2}}{\log p}\right], \quad \ldots \tau_{\frac{n}{n}} = \left[\frac{\log \frac{n}{n}}{\log p}\right].$$

---

[1]) *Mertens:* Über eine zahlentheor. Function. Sitzungsber. d. k. Akad. Wien 1897.

Zvolme nyní libovolné prvočíslo p nepřevyšující n a ukažme, že výrazy, které na obou stranách obsahují $\log p$, jsou stejné.

Na levé straně má $\log p$ činitele $\sum_{i=1}^{\infty} i \left[\frac{n}{p^i}\right]$, kde se sečítá ale jen po $i = \varrho$.

Na pravé vyskytá se $\log p$ v členech

$$\left[\frac{\log n}{\log p}\right] \log p, \left[\frac{\log \frac{n}{2}}{\log p}\right] \log p, \ \ldots \left[\frac{\log \frac{n}{n}}{\log p}\right] \log p,$$

takže půjde opět jen o určení součtu

$$\sum_{k=1}^{n} \left[\frac{\log \frac{n}{k}}{\log p}\right]. \tag{2.}$$

Označme dále

$$\left[\frac{n}{p^\pi}\right] = n_\pi.$$

Potom je jasno, že v součtu (2.) mají hodnotu 0 následující členy

$$\left[\frac{\log \frac{n}{n}}{\log p}\right], \left[\frac{\log \frac{n}{n-1}}{\log p}\right], \ \ldots \left[\frac{\log \frac{n}{n_1+1}}{\log p}\right];$$

součet členů, v nichž $\left[\frac{\log \frac{n}{k}}{\log p}\right] = 1$, jest

$$\left[\frac{\log \frac{n}{n_1}}{\log p}\right] + \left[\frac{\log \frac{n}{n_1-1}}{\log p}\right] + \ \ldots \ + \left[\frac{\log \frac{n}{n_2+1}}{\log p}\right] = 1 \,.\, (n_1 - n_2),$$

součet členů, v nichž $\left[\frac{\log \frac{n}{k}}{\log p}\right] = 2$, jest

$$\left[\frac{\log \frac{n}{n_2}}{\log p}\right] + \left[\frac{\log \frac{n}{n_2-1}}{\log p}\right] + \ \ldots \ + \left[\frac{\log \frac{n}{n_3+1}}{\log p}\right] = 2 \,.\, (n_2 - n_3),$$

neboť jest $\frac{n}{n_2} = \frac{n}{\left[\frac{n}{p^2}\right]} \geqq \frac{n}{\frac{n}{p^2}} = p^2$ a tedy $\log \frac{n}{n_2} \geqq 2 \log p$. Po-

dobně jest součet členů, v nichž $\left[\frac{\log \frac{n}{k}}{\log p}\right] = 3$,

$$\left[\frac{\log \frac{n}{n_3}}{\log p}\right] + \left[\frac{\log \frac{n}{n_3 - 1}}{\log p}\right] + \ldots + \left[\frac{\log \frac{n}{n_4 + 1}}{\log p}\right] = 3 \,.\, (n_3 - n_4)$$

a t. d., až posléze

$$\left[\frac{\log \frac{n}{n_\varrho}}{\log p}\right] + \left[\frac{\log \frac{n}{n_\varrho - 1}}{\log p}\right] + \ldots + \left[\frac{\log \frac{n}{1}}{\log p}\right] = \varrho n_\varrho .$$

Součtem obdržíme

$$\sum_{k=1}^{n} {}_k \left[\frac{\log \frac{n}{k}}{\log p}\right] = 1 \,.\, (n_1 - n_2) + 2 \,.\, (n_2 - n_3) + 3 \,.\, (n_3 - n_4) +$$

$$\ldots + (\varrho - 1)(n_{\varrho - 1} - n_\varrho) + \varrho n_\varrho$$

$$= n_1 + n_2 + n_3 + \ldots + n_\varrho = \sum_{k=1}^{\infty} {}_k \left[\frac{n}{p^i}\right].$$

Tím je formule dokázána.

Klademe-li v ní místo n $\left[\frac{n}{2}\right]$, obdržíme

$$(3.) \quad \Theta\left(\frac{n}{2}\right) + \Theta\left(\frac{n}{4}\right) + \Theta\left(\frac{n}{6}\right) + \ldots + \Theta\left(\frac{n}{n}\right) = \log\left(\left[\frac{n}{2}\right]!\right)$$

a odečtením

$$\Theta(n) + \Theta\left(\frac{n}{3}\right) + \Theta\left(\frac{n}{5}\right) + \ldots = \log \frac{n!}{\left[\frac{n}{2}\right]!}$$

Odečteme-li ale dvojnásobnou rovnici (3.) od (1.), dostaneme

$$\Theta(n) - \Theta\left(\frac{n}{2}\right) + \Theta\left(\frac{n}{3}\right) - \Theta\left(\frac{n}{4}\right) + \ldots \pm \Theta\left(\frac{n}{n}\right)$$

$$= \log \frac{n!}{\left(\left[\frac{n}{2}\right]!\right)^2} .$$