MATEMATICKO-FYZIKÁLNY ČASOPIS SAV, 15, 1, 1965

O DĚLITELNOSTI FAKTORIÁLU $n!$

JOSEF METELKA, Olomouc

V článku se nejprve řeší otázka: Kterou nejvyšší mocninou čísla $m > 1$ je dělitelný faktoriál $n!$? V druhé části je otázka v jistém smyslu obrácena: Které přirozené číslo n má faktoriál $n!$ dělitelný mocninou m^k, nikoli však mocninou m^{k+1} daného přirozeného čísla $m > 1$?

§ 1

Úmluva. Všecka malá latinská písmena v celé práci značí vždy přirozená čísla. Výjimkou je jen exponent k, který může být též roven nule. Ostatní odchylky budou vždy udány.

Položme si problém:

Kterou nejvyšší mocninou čísla $m > 1$ je dělitelný faktoriál $n!$?

A

Nechť je m prvočíslo, tj. $m = p > 1$.

Věta 1. *Je-li p prvočíslo, je faktoriál $n!$ dělitelný číslem p^k, kde*

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

a není dělitelný číslem p^{k+1}.

Důkaz věty je uveden skoro ve všech učebnicích teorie čísel, např. [1, str. 46; 2, str. 24; 3, str. 25].

Příklad. Číslo 131! je dělitelno 5^{32} a není dělitelno 5^{33}, neboť

$$\left[\frac{131}{5}\right] + \left[\frac{131}{25}\right] + \left[\frac{131}{125}\right] = 26 + 5 + 1 = 32.$$

Věta 2. *Nechť je p^{k_n} nejvyšší mocnina prvočísla p, jíž je dělitelný faktoriál $n!$, pak platí*

$$\lim_{n\to\infty} \frac{k_n}{n} = \frac{1}{p-1}.$$

Důkaz. Budeme předpokládat, že n je již větší než p. Označme $i_n = [\log_p n]$, pak máme

$$\lim_{n\to\infty} \frac{i_n}{n} = 0\,. \tag{1}$$

Pro libovolné j platí

$$1 > \frac{n}{p^j} - \left[\frac{n}{p^j}\right] \geqq 0\,.$$

Sčítáme-li tyto nerovnosti pro $j = 1, 2, \ldots, i_n$, dostáváme

$$i_n > n\,\frac{\left(\frac{1}{p}\right)^{i_n} - 1}{1 - p} - k_n \geqq 0\,. \tag{2}$$

Dělíme číslem n a limitujeme pro $n \to \infty$, čímž dostáváme

$$\lim_{n\to\infty} \frac{i_n}{n} \geqq \frac{1}{p-1} - \lim_{n\to\infty} \frac{k_n}{n} \geqq 0$$

a to dává vzhledem ke vztahu [1] tvrzení věty.

Pro první odhad lze tedy v některých případech psát

$$k_n = \left[\frac{n}{p-1}\right]. \tag{3}$$

Např. pro $n = 131$, $p = 5$ dostaneme tak $k_{131} = \left[\frac{131}{4}\right] = 32$ v úplné shodě s přesným výsledkem získaným podle věty 1. Přehled o přesnosti vztahu (3) podává věta:

Věta 3. *Má-li k_n týž význam jako ve větě 2 a je-li $i_n = [\log_p n]$, platí*

$$\left[\frac{n}{p-1}\right] \geqq k_n \geqq \left[\frac{n}{p-1}\right] - (i_n + 1)\,.$$

Důkaz: Z nerovností (2) plyne jednak

$$k_n \leqq \frac{n}{p-1} - \frac{n}{p^{i_n}(p-1)} < \frac{n}{p-1},$$

což lze psát

$$k_n \leqq \left[\frac{n}{p-1}\right],$$

jednak

$$(4)\qquad k_n > \frac{n}{p-1} - \frac{n}{p^{i_n}(p-1)} - i_n\,.$$

Odhadněme výraz

$$u = \frac{n}{p^{i_n}(p-1)}\,.$$

Pro $p = 2$ je $u = \dfrac{n}{2^{i_n}} < 2$ vzhledem k volbě čísla i_n. Pro $p > 2$ je

$$2\,.\,p^{i_n}\,.\,(p-1) > p^{i_n+1} > n$$

a tedy opět $u < 2$. Nerovnost (4) pak dává

$$k_n > \frac{n}{p-1} - (i_n + 1) - 1\,,$$

což lze psát dále

$$k_n \geqq \left[\frac{n}{p-1}\right] - (i_n + 1)\,.$$

Poznámka. Pro $p > 2$ se obou hranic, udaných ve větě 3, skutečně dosahuje. Jestliže je $n = p^s$, je podle věty 1

$$k_n = \frac{p^s - 1}{p-1} = \frac{n}{p-1} - \frac{1}{p-1} = \left[\frac{n}{p-1}\right].$$

Naproti tomu pro $n = p^s - 1$ je $i_n = s - 1$ a $\left[\dfrac{n}{p^j}\right] = p^{s-j} - 1,\, j = 1, \ldots, s$

a tedy

$$k_n = \frac{p^s - 1}{p-1} - s = \frac{n}{p-1} - s = \left[\frac{n}{p-1}\right] - (i_n + 1).$$

Je-li $p = 2$, není možné dosáhnout horní hranice z věty 3. Snadno se zjistí, že v tomto případě platí $k_n \leqq n - 1$.

B

Nechť je m číslo složené $m = p_1^{r_1}\,.\,p_2^{r_2} \ldots p_s^{r_s}$.

Věta 4. *Číslo $n!$ je dělitelné mocninou m^k, kde*

$$k = \min\left\{\left[\frac{1}{r_1}\sum_{i=1}^{\infty}\left[\frac{n}{p_1^i}\right]\right], \ldots, \left[\frac{1}{r_s}\sum_{i=1}^{\infty}\left[\frac{n}{p_s^i}\right]\right]\right\}.$$

a není dělitelné mocninou m^{k+1}.

Důkaz. Označme k_j exponent nejvyšší mocniny prvočísla p_j, kterou je dělitelné číslo $n!$. Podle věty 1 je $k_j = \sum_{i=1}^{\infty}\left[\dfrac{n}{p_s^i}\right]$. Faktoriál $n!$ lze tedy psát $n! = p_1^{k_1} \ldots p_s^{k_s}\,.\,z$, kde přirozené číslo z už není dělitelné žádným z prvočísel p_j a tedy také ne číslem m. Jestliže faktoriál $n!$ je dělitelný m^r, $r \geqq 0$, platí $\dfrac{n!}{m^r} = p_1^{k_1 - rr_1} \ldots p_s^{k_s - rr_s}\,.\,z$. Musí ovšem být $k_j - rr_j \geqq 0$ pro všecka j a tedy $r \leqq \left[\dfrac{k_j}{r_j}\right]$. Největší přípustný exponent $r = k$ dostaneme jako minimum všech čísel $\left[\dfrac{k_j}{r_j}\right]$, což dokazuje naši větu.

Poznámka. Číslo k z předešlé věty lze počítat také takto

$$k = \left[\min_j\left\{\frac{1}{r_j}\sum_{i=1}^{\infty}\left[\frac{n}{p_j^i}\right]\right\}\right], \quad 1 \leqq j \leqq s\,.$$

Příklady. Faktoriál 16! je dělitelný 8^5, číslo 4 000 000! končí 999 999 nulami, číslo 10! je dělitelno 120^2, ale jen první mocninou čísla 7 atd.

§ 2

Další otázka je v jistém smyslu obrácená k předešlé:
Které přirozené číslo n má faktoriál $n!$ dělitelný k-tou mocninou čísla m, nikoli však mocninou m^{k+1}?

A

Nechť je opět nejprve m prvočíslem, $m = p > 1$. Podle výsledku věty 1 jde o řešení rovnice

$$(5)\qquad \sum_{i=1}^{\infty}\left[\frac{x}{p^i}\right] = k$$

přirozenými čísly x.

Pro dané p a k nemusí mít rovnice (5) vůbec kořen. Volme např. $p = 5$, $k = 5$. Pro $x = 24$ je $\sum_{i=1}^{\infty}\left[\frac{24}{5^i}\right] = 4$ a tím spíše není dělitelný 5^5 faktoriál žádného čísla menšího než 24. Pro $x = 25$ je $\sum_{i=1}^{\infty}\left[\frac{25}{5^i}\right] = 6$ a tím spíše je faktoriál každého čísla většího než 25 dělitelný aspoň 5^6. Rovnice $\sum_{i=1}^{\infty}\left[\frac{x}{5^i}\right] = 5$ nemá tedy žádný kořen.

Naproti tomu, je-li rovnice řešitelná pro $k > 0$, má právě p kořenů, jak ukazuje věta:

Věta 5. *Je-li p prvočíslo a $k > 0$ celé číslo, pak rovnice (5) buď nemá vůbec žádný kořen nebo její kořeny tvoří posloupnost p po sobě následujících přirozených čísel.*

Důkaz: Je-li n kořenem rovnice (5), musí pro $k > 0$ zřejmě být $n \geqq p$. Uvažujme posloupnost p po sobě následujících přirozených čísel $n = rp$, $n + 1, \ldots, n + p - 1$. Je-li kterékoliv z nich kořenem rovnice (5), jsou všecka ostatní též kořeny, neboť platí $\left[\frac{n+j}{p^i}\right] = \left[\frac{r}{p^{i-1}}\right]$, $0 \leqq j \leqq p - 1$ a tedy také $\sum_{i=1}^{\infty}\left[\frac{n+j}{p^i}\right] = \sum_{i=1}^{\infty}\left[\frac{r}{p^{i-1}}\right]$. Avšak pro $n + s$, $s \geqq p$, platí $\left[\frac{n+s}{p}\right] > \left[\frac{n}{p}\right]$ a $\left[\frac{n+s}{p^i}\right] \geqq \left[\frac{n}{p^i}\right]$, $i = 2, 3, \ldots$ a tedy $\sum_{i=1}^{\infty}\left[\frac{n+s}{p^i}\right] > k$. Obdobně se ukáže, že pro $n - t$, $t > 0$, je $\sum_{i=1}^{\infty}\left[\frac{n-t}{p^i}\right] < k$.

Poznámka. Pro $k = 0$ má rovnice (5) zřejmě $p - 1$ kořenů $x = 1, \ldots, p - 1$. Případ $k = 0$ můžeme tedy v dalším — právě tak, jako jsme to učinili ve větě 5 — vylučovat.

Náš problém zní nyní takto: Určete, pro která p a $k > 0$ je rovnice (5) řešitelná, a udejte metodu řešení. Obou cílů dosáhneme konstrukcí zajímavé číselné soustavy, které nebylo — pokud je mi známo — dosud použito.

Definice 1. *Je-li možné napsat číslo $k > 0$ ve tvaru*

(6) $$k = d_1A_{1,p} + d_2A_{2,p} + \ldots + d_rA_{r,p},$$

kde $A_{j,p} = 1 + p + \ldots + p^{j-1}$, $0 \leqq d_j \leqq p - 1$, $j = 1, 2, \ldots, d_r \neq 0$, říkáme, že číslo k je psáno v neúplné p-adické soustavě.

Věta 6. *Existuje-li vyjádření čísla $k > 0$ v neúplné p-adické soustavě, je jednoznačné.*

Důkaz. Jednoznačnost se dokazuje zcela obdobně, jako jednoznačnost vyjádření čísla v úplné p-adické soustavě, tj. opírá se o fakt, že

$$(p - 1)A_{1,p} + (p - 1)A_{2,p} + \ldots + (p - 1)A_{j,p} < A_{j+1,p}.$$

Věta 7. *V neúplné p-adické soustavě nelze vyjádřit všecka přirozená čísla. V polouzavřeném intervalu $\langle 1, A_{j+1,p})$ je právě $A_{j,p}$ přirozených čísel, pro něž se nedá najít vyjádření (6).*

Důkaz. Pro přirozená čísla k z intervalu $\langle 1, A_{j+1,p})$ musí být ve vyjádření (6) $d_{j+1} = d_{j+2} = \ldots = 0$. Volíme-li za koeficienty d_s, $1 \leqq s \leqq j$, všecky přípustné číselné hodnoty, dostaneme p^j vyjádření ve tvaru (6), tedy podle věty 6 p^j různých přirozených čísel, která jsou vesměs menší než $A_{j+1,p}$, neboť

$$d_1A_{1,p} + \ldots + d_jA_{j,p} \leqq (p - 1)(A_{1,p} + \ldots + A_{j,p}) =$$
$$= (p - 1) + (p^2 - 1) + \ldots + (p^j - 1) = A_{j+1,p} - (j + 1) < A_{j+1,p}.$$

V intervalu $\langle 1, A_{j+1,p})$ nelze tudíž vyjádřit ve tvaru (6) $A_{j+1,p} - p^j = A_{j,p}$ čísel.

Označme M_{jp} množinu přirozených čísel z intervalu $\langle 1, A_{j+1,p})$, jež nelze vyjádřit ve tvaru (6), a označme dále $\overline{M}_{jp}$ množinu přirozených čísel z téhož intervalu, pro něž nemá rovnice (5) řešení.

Věta 8. a) $\overline{M}_{jp} \subset M_{jp}$; b) *je-li číslo $k > 0$ psáno ve tvaru (6), má rovnice (5) kořeny $x = \sum_{j=0}^{r} d_jp^j$, $0 \leqq d_0 \leqq p - 1$.*

Důkaz. Stačí dokázat tvrzení b), neboť tvrzení a) je jednoduchým důsledkem. Nechť tedy $x = \sum_{j=0}^{r} d_jp^j$, pak

$$\left[\frac{x}{p^i}\right] = \sum_{j=i}^{r} d_jp^{j-i}, \quad i = 1, 2, \ldots$$

a tedy

$$\sum_{i=1}^{\infty}\left[\frac{x}{p^i}\right] = \sum_{i=1}^{\infty}\sum_{j=i}^{r} d_jp^{j-i} = \sum_{j=1}^{r} d_j \sum_{i=1}^{j} p^{i-1} = \sum_{j=1}^{r} d_jA_{j,p} = k.$$

Věta 9. *Do množiny $\overline{M}_{jp}$ patří každé číslo tvaru*

(9) $$k = A_{j+1,p} - g_jA_{j,p} - g_{j-1}A_{j-1,p} - \ldots - g_2A_{2,p} - mA_{1,p},$$

kde koeficienty g_s, $2 \leqq s \leqq j$, nabývají nezávisle na sobě hodnot $0, 1, \ldots, p - 1$

a m je přirozené číslo z intervalu $\langle j - r + 2, j\rangle$, přičemž r znamená index prvního nenulového prvku v posloupnosti $g_2, g_3, \ldots, g_{j+1} = 1$.

Důkaz. Ukážeme nejprve, že k je číslem intervalu $\langle 1, A_{j+1,p})$. Vztah $k < A_{j+1,p}$ je zřejmý; dále $k \geqq A_{j+1,p} - (p-1)(A_{j,p} + \ldots + A_{2,p}) - jA_{1,p} = A_{j+1,p} - (p-1)(A_{j,p} + \ldots + A_{2,p} + A_{1,p}) + (p - j - 1)A_{1,p} = A_{j+1,p} - A_{j+1,p} + j + 1 + (p - j - 1) = p > 1$. Nyní je třeba rozeznávat dva případy:

a) $g_2 = \ldots = g_j = 0$. (Tento případ nastává mimo jiné vždy, když $j = 1$.) Pak číslo $k = A_{j+1,p} - mA_{1,p}$, kde m je v intervalu $\langle 1, j\rangle$. Zvolme dvě čísla $x_1 = p^{j+1}$ a $x_2 = p^{j+1} - 1$.

Pak máme
$$\sum_{i=1}^{j+1}\left[\frac{x_1}{p^i}\right] = \sum_{i=1}^{j+1} p^{j-i+1} = A_{j+1,p} > k,$$
$$\sum_{i=1}^{j}\left[\frac{x_2}{p^i}\right] = \sum_{i=1}^{j} p^{j-i+1} - j = A_{j+1,p} - (j+1) < k.$$

Rovnice (5) tedy nemá řešení.

b) Aspoň jeden z koeficientů $g_2, \ldots, g_j$ je různý od nuly. V tomto případě je vždy $j > 1$ a číslo k má tvar
$$k = A_{j+1,p} - g_jA_{j,p} - \ldots - g_rA_{r,p} - mA_{1,p},$$
kde $j \geqq r \geqq 2$, $g_r \neq 0$ a tedy m je číslo z intervalu $\langle j - r + 2, j\rangle$. Zvolme dvě přirozená čísla
$$x_1 = (p - g_j - 1)p^j + \ldots + (p - g_{r+1} - 1)p^{r+1} + (p - g_r)p^r,$$
$$x_2 = (p - g_j - 1)p^j + \ldots + (p - g_{r+1} - 1)p^{r+1} + (p - g_r)p^r - 1.$$

Snadno najdeme vztahy
$$\left[\frac{x_1}{p}\right] = (p - g_j - 1)p^{j-1} + \ldots + (p - g_{r+1} - 1)p^r + (p - g_r)p^{r-1}; \quad \left[\frac{x_2}{p}\right] = \left[\frac{x_1}{p}\right] - 1,$$

....

$$\left[\frac{x_1}{p^r}\right] = (p - g_j - 1)p^{j-r} + \ldots + (p - g_{r+1} - 1)p + (p - g_r); \quad \left[\frac{x_2}{p^r}\right] = \left[\frac{x_1}{p^r}\right] - 1,$$
$$\left[\frac{x_1}{p^{r+1}}\right] = (p - g_j - 1)p^{j-r-1} + \ldots + (p - g_{r+1} - 1); \quad \left[\frac{x_2}{p^{r+1}}\right] = \left[\frac{x_1}{p^{r+1}}\right],$$

....

$$\left[\frac{x_1}{p^j}\right] = (p - g_j - 1); \quad \left[\frac{x_2}{p^j}\right] = \left[\frac{x_1}{p^j}\right].$$

Sčítáním dostaneme
$$S = \sum_{i=1}^{\infty}\left[\frac{x_1}{p^i}\right] = (p - g_j - 1)A_{j,p} + \ldots + (p - g_{r+1} - 1)A_{r+1,p} + (p - g_r)A_{r,p}.$$

Upravujeme-li postupně od posledního sčítance s použitím vztahu $p \cdot A_{s,p} = A_{s+1,p} - 1$, dostaneme
$$S = A_{j+1,p} - g_j \cdot A_{j,p} - \ldots - g_r \cdot A_{r,p} - (j - r + 1) > k;$$
$$\sum_{i=1}^{\infty}\left[\frac{x_2}{p^i}\right] = S - r = A_{j+1,p} - g_j \cdot A_{j,p} - \ldots - g_r \cdot A_{r,p} - (j+1) < k.$$

Rovnice (5) tedy nemá pro žádné k tvaru (9) kořeny.

Věta 10. *Množina $\overline{M}_{jp}$ má právě $A_{j,p}$ prvků.*

Důkaz. Množina $\overline{M}_{jp}$ nemůže mít více než $A_{j,p}$ prvků v důsledku vět 8a) a 7. Ukážeme nyní, že čísel k ve vyjádření (9) je $A_{j,p}$. Důkaz má dvě části:

a) Jednoznačnost vyjádření (9):

Předpokládejme, že číslo k lze psát ve tvaru (9) dvojím způsobem

(10a) $$k = A_{j+1,p} - g_jA_{j,p} - \ldots - g_rA_{r,p} - mA_{1,p}, \quad g_r \neq 0, \quad m \in \langle j - r + 2, j\rangle,$$

(10b) $$k = A_{j+1,p} - g'_jA_{j,p} - \ldots - g'_sA_{s,p} - m'A_{1,p}, \quad g'_s \neq 0, \quad m' \in \langle j - s + 2, j\rangle$$

a že $r \geqq s > 1$, přičemž není vyloučen případ, že $r = j + 1$ (pak zní (10a) takto: $k = A_{j+1,p} - mA_{1,p}$, $m \in \langle 1, j\rangle$). Je-li $r > s$, doplníme vyjádření (10a) formálně členy $-g_{r-1}A_{r-1,p} - \ldots - g_sA_{s,p}$, kde $g_{r-1} = \ldots = g_s = 0$. Odčítáním (10b) — (10a) dostáváme

(11) $$0 = (g_j - g'_j)A_{j,p} + \ldots + (g_s - g'_s)A_{s,p} + (m - m')A_{1,p}.$$
$$|(g_{j-1} - g'_{j-1})A_{j-1,p} + \ldots + (g_s - g'_s)A_{s,p} + (m - m')A_{1,p}| \leqq$$
$$\leqq |g_{j-1} - g'_{j-1}|A_{j-1,p} + \ldots + |g_s - g'_s|A_{s,p} + |m - m'|A_{1,p} \leqq$$
$$\leqq (p-1)(A_{j-1,p} + \ldots + A_{s,p}) + |m - m'| < (p-1)(A_{j-1,p} + \ldots + A_{1,p}) + r - 2 = A_{j,p} - (j - r + 2) < A_{j,p}.$$

Kdyby tedy bylo ve výrazu (11) $g_j - g'_j \neq 0$, převážil by první člen vpravo v absolutní hodnotě nad součtem všech ostatních, což však není možné. Musí tudíž být $g'_j - g'_j = \ldots = g_s - g'_s = 0$ a ovšem také $m - m' = 0$. Vyjádření čísla k ve tvaru (9) je tedy jednoznačné.

b) Počet různých vyjádření tvaru (9):

Číslo m může nabýt své největší hodnoty j, ať jsou koeficienty $g_2, \dots, g_j$ jakékoli (v mezích 0 až $p-1$), tj. tedy u p^{j-1} čísel tvaru (9). Hodnoty $j-1$ může nabýt jen tehdy, je-li $g_2 = 0$ a ostatní koeficienty $g_3, \dots, g_j$ jsou libovolné, tj. u p^{j-2} čísel tvaru (9). Tak lze usuzovat dále; nejmenší hodnoty $m = 1$ lze použít jen v případě $g_2 = \dots = g_j = 0$, tj. u jediného čísla tvaru (9). Celkem je

$$p^{j-1} + p^{j-2} + \dots + p + 1 = A_{j,p}$$

možných vyjádření tvaru (9) a tedy také $A_{j,p}$ různých čísel k.

Důsledek. $\overline{M}_{jp} = M_{jp}$.

Tím je předložená otázka úplně zodpovězena pro $m = p$.

Příklad. Nechť je $p = 7$. Určíme nejprve čísla $A_{j,p}$ a to s pomocí rekurentního vztahu $A_{j+1,p} = p \cdot A_{j,p} + 1$, $A_{1,p} = 1$.

$$A_{1,7} = 1, \ A_{2,7} = 8, \ A_{3,7} = 57, \ A_{4,7} = 400, \dots$$

Existuje tedy např. 8 čísel množiny M_{27} a jsou to čísla $57 - 8g_2 - m$, kde může být

g_2	0	0	1	2	3	4	5	6
m	1	2	2	2	2	2	2	2

Máme tudíž:

$$M_{27} = \{7, 15, 23, 31, 39, 47, 55, 56\}.$$

Pro těchto osm čísel k nemá rovnice $\sum_{i=1}^{\infty} \left[\frac{x}{7^i}\right] = k$ řešení. Volme v intervalu $\langle 1, 57)$ číslo, pro něž řešení existuje, např. $k = 53$ a hledejme kořen rovnice. Číslo 53 vyjádříme v neúplné sedmičkové soustavě $53 = 5 \cdot A_{1,7} + 6 \cdot A_{2,7}$. A pak má rovnice vzhledem k větě 8 tyto kořeny

$$x = d_0 + 5 \cdot 7 + 6 \cdot 7^2, \quad 0 \leqq d_0 \leqq 6.$$

Jsou to kořeny 329, 330, 331, 332, 333, 334, 335.

Obdobným způsobem je např. pro $p = 11$, $k = 1\,999\,998$. $19\,999\,991 \leqq x \leqq 20\,000\,001$.

B

Nechť je m číslo složené $m = p_1^{r_1} \cdot \ldots \cdot p_s^{r_s}$. Nyní jde o řešení přirozenými čísly rovnice (věta 4.):

$$\text{(12)} \qquad \min_j \left\{ \left[\frac{1}{r_j} \sum_{i=1}^{\infty} \left[\frac{x}{p_j^i} \right] \right] \right\} = k, \quad 1 \leqq j \leqq s.$$

To znamená, že kořeny musí současně vyhovovat s nerovnostem

$$\text{(13)} \qquad \left[\frac{1}{r_1} \sum_{i=1}^{\infty} \left[\frac{x}{p_1^i} \right] \right] \geqq k, \dots, \left[\frac{1}{r_s} \sum_{i=1}^{\infty} \left[\frac{x}{p_s^i} \right] \right] \geqq k,$$

kde aspoň v jednom vztahu platí znaménko rovnosti. Nerovnosti (13) můžeme přepsat takto

$$\text{(14)} \qquad \sum_{i=1}^{\infty} \left[\frac{x}{p_1^i} \right] \geqq r_1 k, \dots, \sum_{i=1}^{\infty} \left[\frac{x}{p_s^i} \right] \geqq r_s k,$$

kde tentokrát nemusí platit rovnost ani v jednom vztahu, avšak aspoň pro jedno přirozené číslo j, $1 \leqq j \leqq s$, musí platit

$$\text{(15)} \qquad \sum_{i=1}^{\infty} \left[\frac{x}{p_j^i} \right] < r_j \cdot (k+1).$$

Budeme řešit za pomoci metody vyložené v oddíle A postupně nerovnosti (14). Jestliže tyto nerovnosti dávají kořeny

$$a_1 \leqq x, \dots, a_s \leqq x,$$

musí kořeny rovnice (12) splňovat vztah

$$\text{(16)} \qquad a \leqq x, \quad \text{kde} \quad a = \max(a_1, \dots, a_s).$$

Dále řešíme postupně nerovnosti (15); nechť kořeny jsou

$$x < b_1, \dots, x < b_s.$$

Pak musí kořeny rovnice (12) splňovat další vztah

$$\text{(17)} \qquad x < b, \quad \text{kde} \quad b = \max(b_1, \dots, b_s).$$

Rovnice (12) má tedy řešení právě tehdy, jestliže platí $a < b$.

Příklad. Nechť je $m = 2800$ a $k = 3$.

$2800 = 2^4 \cdot 5^2 \cdot 7$, je tedy $p_1 = 2$, $r_1 = 4$, $p_2 = 5$, $r_2 = 2$, $p_3 = 7$, $r_3 = 1$.

Nerovnosti (14) mají tvar

$$\sum_{i=1}^{\infty} \left[\frac{x}{2^i} \right] \geqq 12, \quad \sum_{i=1}^{\infty} \left[\frac{x}{5^i} \right] \geqq 6, \quad \sum_{i=1}^{\infty} \left[\frac{x}{7^i} \right] \geqq 3$$

a dávají

$$a_1 = 16 \leqq x, \quad a_2 = 25 \leqq x, \quad a_3 = 21 \leqq x,$$

odkud podle (16)

$$25 \leqq x.$$

Nerovnosti (15) mají tvar

$$\sum_{i=1}^{\infty}\left[\frac{x}{2^i}\right] < 16, \quad \sum_{i=1}^{\infty}\left[\frac{x}{5^i}\right] < 8, \quad \sum_{i=1}^{\infty}\left[\frac{x}{7^i}\right] < 4$$

a dávají

$$x < 18 = b_1, \quad x < 35 = b_2, \quad x < 28 = b_3,$$

odkud podle (17)

$$x < 35.$$

Existuje tedy deset čísel, a to

$$25, 26, 27, 28, 29, 30, 31, 32, 33, 34,$$

takových, že jejich faktoriál je dělitelný 2800^3 a ne 2800^4.

Příklad. Nechť je $m = 36$, $k = 52$.

$$36 = 2^2 . 3^2, \text{ tj. } p_1 = 2, \; r_1 = 2, \; p_2 = 3, \; r_2 = 2.$$

$$\sum_{i=1}^{\infty}\left[\frac{x}{2^i}\right] \geqq 104, \quad \sum_{i=1}^{\infty}\left[\frac{x}{3^i}\right] \geqq 104,$$

$$a_1 = 108 \leqq x, \quad a_2 = 216 \leqq x.$$

S druhé strany

$$\sum_{i=1}^{\infty}\left[\frac{x}{2^i}\right] < 106, \quad \sum_{i=1}^{\infty}\left[\frac{x}{3^i}\right] < 106,$$

$$x < 112 = b_1, \quad x < 216 = b_2.$$

V tomto případě nemá úloha vůbec řešení.

§ 3

Otázku, kterou jsme si položili v § 1, lze obrátit ještě jiným způsobem: *Najděte číslo $m > 1$ takové, aby daný faktoriál $n!$ byl dělitelný m^k a ne m^{k+1} při daném přirozeném čísle k.*

Při použití předešlých výsledků je úloha zcela snadná a neposkytuje nic zajímavého. Uvedeme prostě popis řešení.

Faktoriál $n!$ rozložíme na prvočinitele

$$n! = p_1^{r_1} . p_2^{r_2} . \ldots . p_s^{r_s}.$$

Označme

$$\left[\frac{r_j}{k}\right] = u_j, \quad \left[\frac{r_j}{k+1}\right] = v_j, \quad 1 \leqq j \leqq s.$$

Označme dále M_k množinu čísel tvaru

$$(18) \qquad p_1^{y_1} . p_2^{y_2} . \ldots . p_s^{y_s}, \quad 0 \leqq y_j \leqq u_j.$$

Je-li $m \in M_k$, je $n!$ dělitelno nejméně m^k. Obdobně označíme M_{k+1} množinu čísel tvaru

$$(19) \qquad p_1^{z_1} . p_2^{z_2} . \ldots . p_s^{z_s}, \quad 0 \leqq z_j \leqq v_j.$$

Je-li $m \in M_{k+1}$, je $n!$ dělitelno nejméně m^{k+1}. Naší úloze tedy vyhovují všecka čísla množiny $M_k - M_{k+1}$. Podle (18) a (19) je to celkem

$$\prod_{j=1}^{s}(u_j + 1) - \prod_{j=1}^{s}(v_j + 1)$$

přirozených čísel m, které vyhovují předložené úloze.

Příklad. Nechť je $n = 25$ a $k = 3$.

$$25! = 2^{22} . 3^{10} . 5^6 . 7^3 . 11^2 . 13 . 17 . 19 . 23,$$

$$u_1 = 7, \; u_2 = 3, \; u_3 = 2, \; u_4 = 1, \; u_5 = \ldots = 0,$$

$$v_1 = 5, \; v_2 = 2, \; v_3 = 1, \; v_4 = \ldots = 0.$$

Čísla množin M_3, resp. M_4 jsou

$$2^{y_1} . 3^{y_2} . 5^{y_3} . 7^{y_4}, \quad 0 \leqq y_j \leqq u_j,$$

resp.

$$2^{z_1} . 3^{z_2} . 5^{z_3}, \quad 0 \leqq z_j \leqq v_j.$$

Existuje tedy celkem $8 . 4 . 3 . 2 - 6 . 3 . 2 = 156$ přirozených čísel takových, že $25!$ je dělitelno právě třetí mocninou každého tohoto čísla. Nejmenší z těchto čísel je $m_1 = 7$, největší je $m_{156} = 604\,800 = 2^7 . 3^3 . 5^2 . 7$.

LITERATURA

[1] Бухштаб А. А., *Теория чисел*, Москва 1960.
[2] Сушкевич А. К., *Теория чисел*, Харьков 1954.
[3] Виноградов И. М., *Основы теории чисел*, Москва 1952.

Došlo 10. 6. 1963.

Katedra algebry a geometrie
přírodovědecké fakulty
University Palackého,
Olomouc

ÜBER DIE TEILBARKEIT DES FAKTORIALS $n!$

Josef Metelka

Zusammenfassung

Zuerst behandelt man eingehender die bekannte Frage der höchsten Potenz der gegebenen Zahl $m > 1$, durch welche das Faktorial $n!$ teilbar ist. Dann wird die umgekehrte Frage betrachtet und zwar wird ein solches Faktorial $n!$ bestimmt, das durch m^k, nicht jedoch durch m^{k+1} teilbar ist, wo m und k gegebene Zahlen sind. Es handelt sich um die ganzzahligen nichtnegativen Lösungen der Gleichung (5), bzw. der Gleichung (12). Im Falle der Primzahl $m = p$ wird bewiesen, daß die Gleichung (5) für die und nur für die Exponente k lösbar ist, welche sich in der Form $k = \sum_{j=1}^{r} d_j A_{j,p}$ ausdrücken lassen, wo $A_{j,p} = 1 + p + \ldots + p^{j-1}$ und $0 \leqq d_j \leqq p - 1$. Es existieren dann genau p Lösungen der Gleichung (5), die man alle in der Form $x = \sum_{j=0}^{r} d_j p^j$, wo d_0 eine beliebige ganze Zahl $0 \leqq d_0 \leqq p - 1$ ist, schreiben kann. Das Verfahren gestattet es, das Problem auch für zusammengesetzte Potenzbasen m zu lösen. Die Gleichung (12) wird in diesem Falle auf ein System von Ungleichungen (13) bis (17) umgewandelt.