Číselné soustavy

Dříve než zadáme příklady této série, musíme učinit několik dohod. Zřejmě nikdo z vás nepochybuje o tom, že každé přirozené číslo se dá jednoznačně vyjádřit v desítkové soustavě, tj že se dá psát ve tvaru

$$a_n.10^n + \cdots + a_1.10 + a_0 \tag{$*$}$$

kde $a_i \in \{0, 1, \ldots, 9\}$ a $a_n \neq 0$.

Laskavý čtenář též snadno nahlédne, že každé přirozené číslo můžeme vyjádřit jednoznačně v libovolné r-adické soustavě (kde přirozené $r > 1$), tj. psát ve tvaru

$$a_n.r^n + \cdots + a_1.r + a_0,$$

kde a_i jsou nezáporná celá čísla, které nepřevyšují číslo $r - 1$ (budeme jim říkat číslice r-adické soustavy) a $a_n \neq 0$.

V desítkové soustavě místo tvaru ($*$) většinou píšeme pouze $a_n a_{n-1} \ldots a_1 a_0$. Stejnou dohodu učiníme i pro jiné číselné soustavy. Tedy číslo 1997_{10} (v desítkové soustavě) můžeme v osmičkové soustavě psát jednoduše 3715_8. Vpravo dole od zápisu uvádíme číselnou soustavu, ve které je uvedené číslo zapsáno. Jinak bychom vlastně nevěděli, o jaké číslo jde. Pro přehlednost budeme v každé r-adické soustavě používat číslice $0, 1, \ldots, r - 1$ vyjádřené v soustavě desítkové. Bude-li číslice v desítkové soustavě víceciferná (zřejmě takové případy nastanou pro $r > 10$) dáme ji v příslušném zápise do závorek. Tedy $(25)8(1977)_{1997}$ znamená $25.1997^2 + 8.1997 + 1977$, tj. jedná se o trojciferné číslo v 1997-adické soustavě.

A ještě jedna dohoda. Mějme číslo n zapsané v r-adickém zápise ve tvaru ${a_k a_{k-1} \ldots a_1 a_0}_r$. Pro přirozené $z < k$ pak nazveme z-ciferným součtem čísla n číslo

$$s_z = \sum_{j=0}^{f} (a_{z \cdot j+z-1} \ldots a_{z \cdot j+1} a_{z.j})_r + (a_k a_{k-1} \ldots a_{z.f+z+1} a_{z.f+z})_r,$$

kde $f + 1$ je celočíselný podíl k děleno z. Posledním z-číslím pak budeme značit $a_{z-1} \ldots a_1 a_0$. Tedy například dvojciferný součet čísla 2581977_r je $s_2 = 77_r + 19_r + 58_r + 2_r$ a poslední čtyřčíslí tohoto čísla je 1977_r v libovolné r-adické soustavě (zřejmě však $r \geq 10$).

3. série

Téma: Číselné soustavy

Datum odeslání: 12. prosince 1996

Rozcvička (nebodovaná)
Rozhodněte, zda existuje takové r, aby r-adický zápis čísla π byl tvaru $3.1997\ldots$.

1. úloha (5 bodů)
Určete poslední číslici čísla $1997_{10}!$ v
(a) 2003-adické soustavě;
(b) 20003-adické soustavě.

2. úloha (5 bodů)
Označme počet čísel menších než n, které ve svém r-adickém zápise neobsahují číslici $(r-1)$ symbolem $\Upsilon(n)$. Dokažte, že pak platí[1]

$$\lim_{n\to\infty} \frac{\Upsilon(n)}{n} = 0,$$

tj. že „téměř všechna" čísla zapsaná v r-adické soustavě obsahují číslici $(r-1)$.

3. úloha (5 bodů)
Najděte všechny r-adické číselné soustavy takové, ve kterých je řešitelný algebrogram

$$SKALA + SKALA + SKALA = LASKA.$$

To znamená: každé písmeno lze nahradit číslicí (různé různou) r-adické číselné soustavy, aby naznačené sečtení tří stejných čísel dávalo správný výsledek.

4. úloha (5 bodů)
(a) Mějme přirozené číslo n vyjádřené v r-adické soustavě ve tvaru

$$n = (r-1)(r-2)(r-3)\ldots 321_r.$$

Napíšeme-li r-adický zápis čísla n r-krát za sebou, získáme r-adický zápis čísla, které označíme m. Rozhodněte, pro která r je číslo m dělitelné číslem 11_r.
(b) Určete jednu číslici před a jednu číslici za desetinnou čárkou v šestnáctkovém zápise čísla

$$\left(\frac{\pi^2}{\pi^1} + \sqrt{\frac{\pi^4}{\pi^3}}\right)^{1997_{16}},$$

kde symbol π^i označuje i-tou číslici za desetinnou čárkou v šestnáctkovém zápise čísla π (π je Ludolfovo číslo).

[1] Poznamenejme, že zápis $\lim_{n\to\infty} \frac{\Upsilon(n)}{n} = 0$ znamená, že $(\forall \varepsilon > 0)(\exists n_0)(\forall n > n_0)\ \frac{\Upsilon(n)}{n} < \varepsilon$

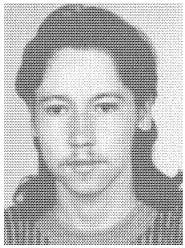
Upozornění: Nedoporučuji snažit se o hledání souvislosti mezi částmi (a) a (b) (pozn. zodpovědného redaktora).

5. ÚLOHA (5 BODŮ)

Nechť přirozené $r > 1$, nechť dále x, y, z, n jsou přirozená čísla taková, $x|(r^z - 1)$ a $y|r^z$ a r-adický zápis čísla n je tvaru ${a_k a_{k-1} \dots a_1 a_0}_r$ $(k > z)$. Dokažte, že pak

a) Přirozené číslo n je dělitelné číslem x právě tehdy, když jeho z-ciferný součet je dělitelný číslem x.
b) Přirozené číslo n je dělitelné číslem y právě tehdy, když jeho poslední z-číslí je dělitelné číslem y.

Řešení 3. série



Radek Erban

Rozcvička (nebodovaná). *Rozhodněte, zda existuje takové r, aby r-adický zápis čísla π byl tvaru* $3{,}1997\dots$.

Rozcvičku řešila jen jedna řešitelka (Lenka Zdeborová). Zde je řešení:
Využijeme vyjádření $\pi = 3{,}1415\dots$ a také pro $r > 7$ platných nerovností

$$(3{,}1998)_{r+1} < (3{,}1997)_r < (3{,}1998)_r.$$

Naší úlohou je nalézt takové $r \in \mathbb{N}$, že

$$(3{,}1997)_r \leq \pi < (3{,}1998)_r.$$

To však není možné, neboť

$$(3{,}1997)_{12} = 3{,}1513\dots,$$
$$(3{,}1998)_{13} = 3{,}1345\dots.$$

A vzhledem k výše uvedeným nerovnostem nemůže číslo π pro žádné $r \in \mathbb{N}$ ležet v požadovaném intervalu. Hledané r tedy neexistuje.

Pokud by se nejednalo pouze o rozcvičku, bylo by samořejmě ještě nutné zdůvodnit oprávněnost použitých numerických odhadů.

1. úloha

Určete poslední číslici čísla $1997_{10}!$ v

(a) 2003-adické soustavě;

(b) 20003-adické soustavě.

Lemma. *(Wilson) Nechť $p \in N$ je prvočíslo. Pak platí*

$$(p-1)! \equiv -1 \pmod p,$$

přičemž, že vztah $a \equiv b \pmod p$ znamená, že číslo p dělí rozdíl $(a-b)$. Čteme „a je kongruentní s b podle modulu p“; uvedený vztah nazýváme kongruencí. Poznamenejme, že platí i opačná implikace, tj. platí-li uvedená kongruence pro $p > 1$, pak p je prvočíslo.

Důkaz: Pro $p = 2$ a $p = 3$ tvrzení zřejmě platí, předpokládejme tedy, že $p > 3$. Uvažujme množinu $M = \{1, 2, 3, \dots, p-1\}$. Je-li $x \in M$, pak lze snadno dokázat (zkuste si to), že číslo xy probíhá pro $y \in M$ všechny prvky M. Existuje tedy právě jedno $y \in M$ takové, že $xy \equiv 1 \pmod p$.

Ptejme se nyní, kdy může být $x = y$. Řešíme rovnici $x^2 \equiv 1 \pmod p$, což je ekvivalentní se zápisem $p \mid x^2 - 1 = (x-1)(x+1)$. Dostáváme tedy jen dvě řešení v oboru množiny M a to $x = 1$, $p-1$. Ostatní čísla z množiny $M \setminus \{1, p-1\}$ se rozpadají na dvojice $x_1, y_1; x_2, y_2; \dots; x_k, y_k$, pro které platí $x_1y_1 \equiv 1, x_2y_2 \equiv 1, \dots, x_ky_k \equiv 1 \pmod p$. Čísla $x_1, y_1, x_2, y_2, \dots x_k, y_k$ jsou až na pořadí čísla $2, 3, 4, \dots, (p-2)$, proto vynásobením uvedených kongruencí máme $x_1y_1x_2y_2 \cdots x_ky_k \equiv 1 \pmod p$, tj.

$$2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2) \equiv 1 \pmod p$$

a násobíme-li poslední vztah konguencí $p - 1 \equiv -1 \pmod p$, dostáváme

$$(p-1)! \equiv -1 \pmod p,$$

což jsme chtěli.[2]

(a) Nyní použijeme lemma pro prvočíslo $p = 2003$ a jednoduchými úpravami dostáváme

$$-1 \equiv 2002! = 1997! \cdot 1998 \cdot 1999 \cdot 2000 \cdot 2001 \cdot 2002 \equiv 1997!(-5)(-4)(-3)(-2)(-1) \pmod{2003}$$

$$1997!(-5)(-4)(-3)(-2)(-1) = 1997!(-120).$$

Vynásobením -217 a užitím toho, že $(-120)(-217) = 26040 \equiv 1 \pmod{2003}$ zjišťujeme, že

$$1997! \equiv 217 \pmod{2003}.$$

A tedy 217 je poslední číslice čísla $1997_{10}!$ v 2003-adické soustavě.

(b) Jelikož číslo $20003 = 83 \cdot 241$ dělí číslo $1997_{10}!$, je poslední číslice čísla $1997_{10}!$ v 20003-adické soustavě 0.

Poznámky k došlým řešením: Řešitele bylo možno rozdělit do pěti skupin:

(1) špatně si přečetli zadání — buď si faktoriál představili v dolním indexu, nebo ho vynechali úplně $(0 + 0i)$.
(2) dokázali druhou (jednodušší) část $(2 + 0i)$.
(3) dokázali obě tvrzení, druhé však s použitím Wilsonovy věty, kterou použili bez důkazu $(3 + 0i)$.
(4) dokázali obě tvrzení, při důkazu Wilsonovy věty se odvolali na literaturu $(5 + 0i)$.
(5) dokázali obě tvrzení i Wilsonovu větu $(5 + 2i)$.

---

[2] Analogické tvrzení platí v každém *konečném tělese*. Zkuste tuto analogii zformulovat (a případně i dokázat). Tělesem se zde míní jisté zobecnění racionálních čísel. Je to množina objektů (čísel), které můžeme sčítat a násobit, přičemž tyto operace splňují několik přirozených požadavků (asociativita, distributivita, …). Příklady (nekonečných) těles jsou racionální, reálná, komplexní čísla, příklad konečného tělesa jsou například „celá čísla modulo p", pro tento příklad dostáváme právě dokázané lemma.

2. úloha
Označme počet čísel menších než n, které ve svém r-adickém zápise neobsahují číslici $(r-1)$ symbolem $\Upsilon(n)$. Dokažte, že pak platí[3]

$$\lim_{n\to\infty} \frac{\Upsilon(n)}{n} = 0,$$

tj. že „téměř všechna" čísla zapsaná v r-adické soustavě obsahují číslici $(r-1)$.

Lemma. *Nechť $(a_n)_{n=1}^{\infty}$, $(b_n)_{n=1}^{\infty}$ jsou posloupnosti reálných čísel, pro které platí*[4]

$$\lim_{n\to\infty} b_n = 0, \qquad \forall n \in \mathbb{N}: \quad 0 \le a_n \le b_n.$$

Pak existuje též limita posloupnosti a_n a je rovna nule.

Důkaz: přenecháváme laskavému čtenáři.

Nechť $k \in N$. Ptejme se kolik je v r-adické číselné soustavě nejvýše k-ciferných čísel, která nebsahují číslici $(r-1)$. Bude jich zřejmě stejně jako všech nejvýše k-ciferných čísel v $(r-1)$-adické soustavě, to jest $(r-1)^k$.

Nechť n je $(k+1)$-ciferné číslo. Pak zřejmě platí

$$n \ge r^k, \qquad \Upsilon(n) \le \Upsilon(r^{k+1}) = (r-1)^{k+1}.$$

Odtud dostáváme nerovnost $\Upsilon(n)/n \le (r-1)\cdot((r-1)/r)^k$. Užijeme lemmatu pro $a_n = \Upsilon(n)/n$ a $b_n = (r-1)\cdot((r-1)/r)^k$. Jde-li nyní n do nekonečna jde i jeho počet cifer k do nekonečna. Avšak $(r-1)/r < 1$, proto

$$\lim_{k\to\infty} (r-1)\left(\frac{r-1}{r}\right)^k = (r-1)\cdot \lim_{k\to\infty}\left(\frac{r-1}{r}\right)^k = 0.$$

Dle lemmatu jsme hotovi.

3. úloha
Najděte všechny r-adické číselné soustavy takové, ve kterých je řešitelný algebrogram

$$SKALA + SKALA + SKALA = LASKA.$$

To znamená: každé písmeno lze nahradit číslicí (různé různou) r-adické číselné soustavy, aby naznačené sečtení tří stejných čísel dávalo správný výsledek.

Uvažováním prvního místa zprava v našem algebrogramu vidíme, že $2\cdot A$ je dělitelné číslem r. Tedy buď je $A = 0$, nebo $A = r/2$ (to samozřejmě pouze pro sudé r).

Zabývejme se nejprve případem $A = r/2$. Ze třetího místa zjišťujeme, že $S \ge r/2$ (Přenos nemůže být moc velký. Výjimku tvoří $r = 4$, kdy je třeba zvážit možnost $A = 2$, $L = 3$, $S = 0$.

[3] Poznamenejme, že zápis $\lim_{n\to\infty}\frac{\Upsilon(n)}{n} = 0$ znamená, že $(\forall\varepsilon > 0)(\exists n_0)(\forall n > n_0)\ \frac{\Upsilon(n)}{n} < \varepsilon$

[4] Definice limity posloupnosti nám říká $\lim_{n\to\infty} a_n = A$ právě tehdy, když pro každé $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ takové, že $\forall n > n_0: \quad |a_n - A| < \varepsilon$

Tato možnost selhává, neboť kvůli druhému místu by muselo být $K = 2 = A$.), ale z pátého místa vidíme, že $3 \cdot S \ \leq L \leq (r-1)$, tedy $r/2 \leq S \ \leq r/3$, což je *spor.*

Z předcházejícího tedy plyne, že $A = 0$ nezávisle na r. Nyní dostáváme následující rovnice:
Z druhého a třetího místa $\quad 3 \cdot L = rS + K$,
z čtvrtého a páteho místa $\quad 3 \cdot (rS + K) = rL + A = rL$.

Vynásobíme-li první rovnost třemi a přičteme druhou, dostaneme $9L = rL$, čili $r = 9$. Na druhé straně snadno nahlédneme, že pro $r = 9$ je uvedený algebrogram skutečně řešitelný, existují dokonce čtyři řešení: $SKALA = 13040, 16050, 23070, 26080$.

Poznámky k došlým řešením: Všichni (až na dvě výjimky, které sestavily rovnici 5. stupně pro r a nedořešily ji, za což obdržely $-i$.) řešili úlohu delším nebo kratším rozborem případů. Ta rychlejší řešení obdržela $+i$.

Několika řešitelům, kteří dokázali pouze to, že algebrogram nemůže mít řešení v žádné jiné, než devítkové soustavě, ale neuvedli příklad řešení jsem strhla jeden bod.

4. úloha

(a) Mějme přirozené číslo n vyjádřené v r-adické soustavě ve tvaru

$$n = (r-1)(r-2)(r-3)\dots 321_r.$$

Napíšeme-li r-adický zápis čísla n r-krát za sebou, získáme r-adický zápis čísla, které označíme m. Rozhodněte, pro která r je číslo m dělitelné číslem 11_r.

(b) Určete jednu číslici před a jednu číslici za desetinnou čárkou v šestnáctkovém zápise čísla

$$\left(\frac{\pi^2}{\pi^1} + \sqrt{\frac{\pi^4}{\pi^3}}\right)^{1997_{16}},$$

kde symbol π^i označuje i-tou číslici za desetinnou čárkou v šestnáctkovém zápise čísla π (π je Ludolfovo číslo).
Upozornění: Nedoporučuji snažit se o hledání souvislosti mezi částmi (a) a (b) (pozn. zodpovědného redaktora).

(a) **Lemma.** *Nechť přirozené $r > 1$. Číslo $c = (a_k a_{k-1} \dots a_1 a_0)_r$ je dělitelné číslem 11_r právě tehdy, když číslo $\sum_{j=0}^{k} a_j(-1)^j$ („střídavý ciferný součet" čísla c, toto číslo označíme $\mathrm{scs}(c)$) je dělitelné číslem 11_r.*

Důkaz: Všimněme si, že $r^j = (r+1-1)^j = (11_r - 1)^j$, což po dělení 11_r dává zbytek $(-1)^j$ (užíjeme binomickou větu). Tudíž $\sum_{j=0}^{k} a_j r^j$ dává stejný zbytek, jako $\sum_{j=0}^{k} a_j(-1)^j = \mathrm{scs}(c)$. To, že číslo je dělitelné 11_r je totéž, jako že dává po dělení 11_r zbytek 0, jsme tedy hotovi.

Řešení nyní rozdělme na dva případy. Pokud je r sudé, tak z lemmatu 3 plyne, že číslo

$$x = (r-1)(r-2)(r-3)\dots 321(r-1)(r-2)(r-3)\dots 321_r$$

je dělitelné číslem 11_r a protože m lze psát jako $x \cdot 100\dots0100\dots\dots1$ s (v čísle je $r/2$ jedniček) je též dělitelné číslem 11_r. Pokud je číslo r liché, říká nám lemma, že číslo m je dělitelné číslem 11_r právě tehdy, když číslo $r((1+3+\dots+(r-2)) - (2+4+\dots+(r-1))) = -r(r-1)/2$ (stačí sečíst dvě aritmetické řady) je dělitelné číslem 11_r. Avšak $11_r = r+1$ nedělí $r(r-1)/2$ (protože

r a $r+1$ jsou nesoudělná, a $(r-1)/2$ je moc malé). Tedy pro žádné liché r není číslo m dělitelé číslem 11_r.

Dokázali jsme tedy: Číslo m je dělitelné číslem 11_r tehdy a jen tehdy, když r je sudé.

(b) Číslo π v šestnáctkové soustavě má tvar $\pi = 3,243(15)6\ldots$. Chceme tedy určit jednu číslici před a jednu číslici za desetinnou čárkou v šestnáctkovém zápisu čísla $\xi = \left(2+\sqrt{5}\right)^{1997_{16}}$. Uvažujme posloupnost $a_n = \alpha^n + \beta^n$, kde $\alpha = 2+\sqrt{5}$ a $\beta = 2-\sqrt{5}$. Umocněním podle binomické věty se snadno ověří, že a_n je celé číslo. Navíc se a_n a α^n liší velmi málo — méně než od $0,1_{16}$ ($|\beta| < 1/4$, tedy už $|\beta^2| < 0,1_{16}$). Pokud tedy a_n končí cifrou x_{16}, tak hledané cifry v ξ jsou $(\ldots x, 0\ldots)$ ($\beta^{1997_{16}} < 0$, proto je a_n o málo menší než $\alpha^{1997_{16}} = \xi$).

Vzhledem k rovnostem $\alpha^{n+2} = 4\cdot\alpha^{n+1} + \alpha^n$, $\beta^{n+2} = 4\cdot\beta^{n+1} + \beta^n$, platí rekurentní vztah $a_{n+2} = 4a_{n+1} + a_n$, přičemž $a_0 = 2$, $a_1 = 4$. Označme $b_n = a_n \mod 16$. Snadno spočteme první členy 2, 4, 2, 12, 2, 4. Protože b_n závisí jen na b_{n-1} a b_{n-2}, musí už platit $b_{n+4} = b_n$. Tím spíše $b_{n+16} = b_n$ a tedy $b_{1997_{16}} = b_{7_{16}} = b_{3_{16}} = 12$. Závěr: hledané číslice jsou $\ldots(12), 0\ldots$.

Poznámky k došlým řešením: V části a) byly možné asi dva přístupy. První je ten, který využívá vzorové řešení. Druhý spočívá ve vyjádření čísla m jako $n(r^{(r-1)(r-1)} + r^{(r-1)(r-2)} + \cdots + 1)$, sečtení geometrické řady a dalších úpravách.

V části b) byly postupy založené na jiné myšlence než vzorové řešení většinou nepřesné a chybné. Několik řešitelů po zcela přesně vyřešené úloze udělalo chybu ve znaménku $\beta^{1997_{16}}$ a vyšlo jim proto $(11),(15)$. Ztratili za to $1i$ (typický případ nevhodného použití imaginárních bodů, pozn. redaktora).

5. úloha

Nechť přirozené $r > 1$, nechť dále x, y, z, n jsou přirozená čísla taková, $x|(r^z-1)$ a $y|r^z$ a r-adický zápis čísla n je tvaru ${a_k a_{k-1}\ldots a_1 a_0}_r$ ($k > z$). Dokažte, že pak

a) Přirozené číslo n je dělitelné číslem x právě tehdy, když jeho z-ciferný součet je dělitelný číslem x.
b) Přirozené číslo n je dělitelné číslem y právě tehdy, když jeho poslední z-číslí je dělitelné číslem y.

Za nejúspornější řešení chválíme Eriku Ventlukovou.

(a) Zavedeme $a_i = 0$ pro $i > k$ a $f+1 = \lfloor\frac{k}{z}\rfloor$, stejně jako v úvodním textu k sérii.

$$n = \sum_{i=0}^{f+1} r^{zi}(a_{zi+0} + a_{zi+1}r + \cdots + a_{zi+z-1}r^{z-1}).$$

Vzhledem ke kongruenci $r^z \equiv 1 \pmod{x}$ platí také $r^{zi} \equiv 1^i \pmod{x}$, z čehož vyplývá

$$n \equiv \sum_{i=0}^{f+1}(a_{zi+0} + a_{zi+1}r + \cdots + a_{zi+z-1}r^{z-1}) \pmod{x}.$$

A to je požadované tvrzení — na pravé straně je z-ciferný sočet.

(b) Z $y \mid r^z$ plyne $y \mid a_z r^z + a_{z+1}r^{z+1} + \cdots + a_k r^k = u$. A tedy

$$y \mid n \iff y \mid n-u \iff y \mid a_0 + a_1 r + \cdots + a_{z-1}r^{z-1}, \text{ c.b.d.}$$

Poznámky k došlým řešením: Tato úloha Vám nedělala žádné problémy. Téměř všichni jste dostali plný počet (reálných) bodů. Rozhodl jsem se tedy, že se trochu „vyřádím“ na imaginární části hodnocení. Omlouvám se všem, pokud se jim imaginární hodnocení zdá nespravedlivé, již z jeho povahy musí být značně subjektivní.

Velmi mě potěšilo, že téměř nikdo z Vás neopoměl v úlohách dokazovat ekvivalenci. Co mě ale znechucuje, je odbývání důkazu ekvivalence poznámkou o ekvivalentnosti Vašich úprav. Chcete říci, že kongruence nějakých dvou čísel je ekvivalentní s tím, že jedno je z-ciferným součtem druhého? Lze jen konstatovat, že jste použili toto magické zaříkávadlo na špatném místě.