# Kongruence

3. PODZIMNÍ SÉRIE — TERMÍN ODESLÁNÍ: 8. PROSINCE 2014

*Poznámka: Nulu za přirozené číslo nepovažujeme.*

ÚLOHA 1. (3 BODY)
Když si Kuba hrál se svým oblíbeným přirozeným číslem, zjistil zajímavou věc. Nejenže dané číslo bylo palindrom[1] a dávalo po dělení čtyřmi zbytek 1 a po dělení dvaceti pěti zbytek 22, ale dokonce bylo nejmenším číslem, které všechny předchozí body splňuje. Které číslo to bylo?

ÚLOHA 2. (3 BODY)
Nalezněte všechny čtveřice nezáporných celých čísel $a$, $b$, $c$, $d$, které řeší rovnici

$$10^a + 5^b = 3^c + 7^d.$$

ÚLOHA 3. (3 BODY)
Dokažte, že pro každé přirozené číslo $a$ existuje přirozené číslo $n > 1$ takové, že $n \mid a^n + 1$.

ÚLOHA 4. (5 BODŮ)
Nalezněte přirozené $n$ takové, že

$$11^{n+1} + 10^{12n+6} + 11^{4n+2} \equiv 1 \pmod{1000121}.$$

Prozradíme, že 1000121 je prvočíslo.

ÚLOHA 5. (5 BODŮ)
Dokažte, že $1^1 + 11^{11} + \cdots + 1111111111^{1111111111}$ (sčítanců je deset) je dělitelné 100.

ÚLOHA 6. (5 BODŮ)
Sedmiciferné přirozené číslo nazveme *spořádané*, pokud je každá z číslic 1, 2, 3, 4, 5, 6, 7 v jeho desítkovém zápisu obsažena právě jednou. Existují dvě různá spořádaná čísla taková, že jedno dělí druhé?

ÚLOHA 7. (5 BODŮ)
Nalezněte všechny posloupnosti přirozených čísel $(a_n)_{n=1}^{\infty}$, které pro každé prvočíslo $p$ a každé přirozené číslo $n$ splňují vztah

$$a_n^p \equiv n \pmod{a_p}.$$

ÚLOHA 8. (5 BODŮ)
Mějme libovolné prvočíslo $p \geq 7$. Dokažte, že pak existuje přirozené číslo $n$ a celá čísla $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_n$ nesoudělná s $p$ taková, že

$$\begin{aligned} x_1^2 + y_1^2 &\equiv x_2^2 \pmod{p}, \\ x_2^2 + y_2^2 &\equiv x_3^2 \pmod{p}, \\ &\vdots \\ x_n^2 + y_n^2 &\equiv x_1^2 \pmod{p}. \end{aligned}$$

[1] Palindromem rozumíme číslo, které se v desítkové soustavě čte stejně zepředu jako zezadu, např. 226747622.

# Kongruence

3. PODZIMNÍ SÉRIE — VZOROVÉ ŘEŠENÍ

## Úloha 1. (111; 107; 2,81; 3,0)

*Když si Kuba hrál se svým oblíbeným přirozeným číslem, zjistil zajímavou věc. Nejenže dané číslo bylo palindrom*[1] *a dávalo po dělení čtyřmi zbytek 1 a po dělení dvaceti pěti zbytek 22, ale dokonce bylo nejmenším číslem, které všechny předchozí body splňuje. Které číslo to bylo?*

*(Kuba Krásenský)*

ŘEŠENÍ:

Kubovo oblíbené přirozené číslo dávalo zbytek 22 po dělení dvaceti pěti, tudíž jeho poslední dvojčíslí bylo 22, 47, 72 nebo 97. Protože zbytek po dělení čtyřmi závisí pouze na posledním dvojčíslí, hledané číslo musí končit na 97, jenž jediné z uvedených dvojčíslí dává zbytek 1 po dělení čtyřmi. Proto Kubovo oblíbené číslo bylo nejmenší palindrom končící na 97, což je 797.

POZNÁMKY:

Líbila se mi řešení využívající Čínskou zbytkovou větu. Plný počet jsem udělovala samozřejmě také řešením, která procházela od nejmenších všechna čísla splňující některou z podmínek ze zadání, pokud nebyla některá čísla bez okomentování opomenuta. Zde bych chtěla upozornit, že existují i dvojciferné palindromy – na ně se často zapomínalo. *(Míša Hubatová)*

## Úloha 2. (86; 47; 1,95; 2,0)

*Nalezněte všechny čtveřice nezáporných celých čísel $a$, $b$, $c$, $d$, které řeší rovnici*

$$10^a + 5^b = 3^c + 7^d.$$

*(Štěpán Šimsa)*

ŘEŠENÍ:

Pokud $a > 0$, potom na levé straně rovnice máme liché číslo, zatímco na pravé straně vždy číslo sudé, takže rovnost nemůže nikdy nastat. Musí tedy být $a = 0$, rovnice se nám přepíše do tvaru

$$1 + 5^b = 3^c + 7^d.$$

Nyní předpokládejme, že $c > 0$, a podívejme se na rovnici modulo tři. Protože $7 \equiv 1 \pmod 3$, je i $7^d \equiv 1 \pmod 3$ a pravá strana dává vždy zbytek 1 po dělení třemi. Dále $5 \equiv -1 \pmod 3$, takže $5^b \equiv (-1)^b \pmod 3$. Levá strana může tedy dávat zbytky pouze 0 nebo 2, proto rovnost nenastává. Z toho plyne, že i $c = 0$. Dostáváme rovnici $5^b = 7^d$, která má řešení pouze $b = d = 0$.

[1] Palindromem rozumíme číslo, které se v desítkové soustavě čte stejně zepředu jako zezadu, např. 226747622.

Poznámky:
Kromě správných řešení, která byla většinou stejná jako vzorák, se vyskytlo několik skupin řešení špatných. Řešitelé z první skupiny pouze ukázali, že rovnice nemá řešení v $\mathbb{N}$, z čehož usoudili, že je nutně $a = b = c = d = 0$, což samozřejmě obecně není pravda. Další skupina se snažila úlohu vyřešit pomocí diskutování, jakou cifrou končí čísla na levé a pravé straně, nikdo to však správně nedotáhl do konce. Někteří řešitelé si neuvědomili, že 0 je nezáporné celé číslo, a po vyšetření sudosti/lichosti obou stran prohlásili, že rovnice nemá řešení. Dokonce se našel jeden řešitel, který správě ukázal, že $a = 0$, ale při vyšetřování rovnice modulo tři stejně napsal, že rovnost nenastává nikdy. *(Martin Čech)*

## Úloha 3. (72; 61; 2,58; 3,0)

*Dokažte, že pro každé přirozené číslo $a$ existuje přirozené číslo $n > 1$ takové, že $n \mid a^n + 1$.*
*(Anh Dung „Tonda“ Le)*

Řešení:

Pokud je $a$ liché, potom je $a^2$ liché a $a^2 + 1$ je sudé, číslo $n = 2$ tedy vyhovuje podmínce v zadání. Pokud je $a$ sudé, položíme $n = a + 1$. Potom platí

$$a^n = (n-1)^n \equiv (-1)^n = -1 \pmod{n},$$

neboť $n$ je liché. Pokud si tuto kongruenci přepíšeme podle definice, dostaneme $n \mid a^n + 1$, což jsme přesně chtěli.

Poznámky:
Většina zaslaných řešení byla správná, skoro vždy shodná se vzorovým. Někteří si navíc všimli, že zadané podmínce vyhovuje každý prvočíselný dělitel čísla $a+1$, a dokonce i každý lichý dělitel čísla $a + 1$. To sice úloha nijak nepožadovala, ale je to zajímavé pozorování. *(Tonda Češík)*

## Úloha 4. (46; 36; 3,76; 5,0)

*Nalezněte přirozené $n$ takové, že*

$$11^{n+1} + 10^{12n+6} + 11^{4n+2} \equiv 1 \pmod{1000121}.$$

*Prozradíme, že 1000121 je prvočíslo.* *(Kuba Krásenský)*

Řešení:
Nejdříve ukážeme, že výraz $10^{12n+6} + 11^{4n+2}$ je pro každé $n$ dělitelný prvočíslem 1000121. Můžeme totiž psát

$$10^{12n+6} = (1000000)^{2n+1},$$
$$11^{4n+2} = (121)^{2n+1}.$$

Pokud $a \equiv b \pmod{m}$, pak pro libovolné $k$ přirozené platí $a^k \equiv b^k \pmod{m}$. S využitím tohoto pravidla dostaneme

$$1000000 \equiv -121 \pmod{1000121}$$
$$(1000000)^{2n+1} \equiv (-121)^{2n+1} = -(121)^{2n+1} \pmod{1000121},$$

což jsme chtěli ukázat. V poslední úpravě jsme využili faktu, že $2n+1$ je liché číslo. Kongruence ze zadání se tak zjednodušila na

$$11^{n+1} \equiv 1 \pmod{1000121}.$$

Přišel čas na Malou Fermatovu větu, která říká, že pro $p$ prvočíslo a $a$ přirozené číslo nesoudělné s $p$ platí $a^{p-1} \equiv 1 \pmod{p}$. Podle rady ze zadání je 1000121 prvočíslo. Můžeme tedy zvolit takové $n$, aby platilo

$$11^{n+1} = 11^{1000121-1} \equiv 1 \pmod{1000121}.$$

Řešením úlohy je například $n = 1000119$.

Poznámky:

Úlohu neposlalo mnoho lidí (na čtyřku), z došlých řešení pak byly zhruba tři čtvrtiny správně. Postupy se od sebe lišily především důkazem toho, že součet druhého a třetího členu je dělitelný daným prvočíslem – kromě výše uvedeného mnozí argumentovali tvrzením, že pro liché $m$ platí $a+b \mid a^m+b^m$.

Řešitelé, kteří si tohoto pěkného součtu nevšimli, se mě často snažili přesvědčit, že žádné vyhovující $n$ neexistuje. *(Bára Kociánová)*

## Úloha 5. (90; 88; 4,76; 5,0)

*Dokažte, že* $1^1+11^{11}+\cdots+1111111111^{1111111111}$ *(sčítanců je deset) je dělitelné 100.*

*(Kuba Krásenský)*

Řešení:

Jelikož

$$1\ldots111 \equiv 11 \pmod{100},$$

platí i

$$1\ldots11^{1\ldots11} \equiv 11^{1\ldots11} \pmod{100},$$

tudíž všechny členy zadaného součtu kromě $1^1$ jsou kongruentní s $11^{1\ldots11}$ modulo 100 a máme

$$\begin{aligned} &1^1+11^{11}+111^{111}+\cdots+1111111111^{1111111111} \equiv \\ &\equiv 1+11^{11}+11^{111}+\cdots+11^{1111111111} \pmod{100}. \end{aligned}$$

Všimneme si, že $11^{10} \equiv 1 \pmod{100}$, dle binomické věty totiž platí

$$11^{10}=(10+1)^{10}=1+\binom{10}{1}\cdot 10+\binom{10}{2}\cdot 10^2+\cdots \equiv 1+10\cdot 10 \equiv 1 \pmod{100},$$

neboť všechny členy tohoto součtu kromě 1 jsou dělitelné 100. Dál upravujeme součet ze zadání:

$$\begin{aligned} &1+11^{1\cdot 10+1}+11^{11\cdot 10+1}+\cdots+11^{111111111\cdot 10+1} = \\ &=1+(11^{10})^1\cdot 11+(11^{10})^{11}\cdot 11+\cdots+(11^{10})^{111111111}\cdot 11 \equiv \\ &\equiv 1+1^{11}\cdot 11+\cdots+1^{111111111}\cdot 11 = 1+9\cdot 11 = 100 \pmod{100}. \end{aligned}$$

Zadaný součet je tedy kongruentní s 0 modulo 100, neboli je stem dělitelný, což jsme měli dokázat.

Poznámky:

Naprostá většina řešitelů řešila tuto úlohu obdobně jako ve vzoráku, pouze tři z vás si nejprve rozložili 100 na $4\cdot 25$ a dokazovali zvlášť dělitelnost čtyřmi a dvaceti pěti, což ovšem řešení spíše prodloužilo. Těm, kteří platnost $11^{1\ldots11} \equiv 11 \pmod{100}$ pouze bez důkazu prohlásili, jsem nakonec strhával jeden bod. *(Tomáš Novotný)*

## Úloha 6. (64; 58; 4,22; 5,0)

*Sedmiciferné přirozené číslo nazveme spořádané, pokud je každá z číslic 1, 2, 3, 4, 5, 6, 7 v jeho desítkovém zápisu obsažena právě jednou. Existují dvě různá spořádaná čísla taková, že jedno dělí druhé?* *(Anh Dung „Tonda“ Le)*

Řešení:
Dokážeme, že neexistují dvě různá spořádaná čísla $a$, $b$ taková, že $a = bk$. Pro spor předpokládejme opak. Podíl 7654321/1234567 je menší než 7, a proto $2 \leq k \leq 6$. Dále platí, že každé přirozené číslo dává stejný zbytek po dělení devíti jako jeho ciferný součet, a proto:

$$a \equiv b \equiv 1 + 2 + \cdots + 7 = 28 \equiv 1 \pmod 9.$$

Z toho pak plyne:

$$1 \equiv a = bk \equiv k \pmod 9.$$

Požadovaný vztah nesplňuje žádné přirozené $k$ mezi 2 a 6, takže jsme došli ke sporu. Hledaná spořádaná čísla tedy neexistují.

Poznámky:
Šestá úloha byla tentokrát relativně lehká, a proto došlo hodně správných řešení. Velká část řešitelů bohužel nepřišla na použití kongruence a zabývala se rozebíráním případů. Někteří se zase báli modulo 9 a preferovali modulo 3, kvůli čemuž měli o kus práce víc.

*(Anh Dung „Tonda“ Le)*

## Úloha 7. (20; 12; 2,75; 2,0)

*Nalezněte všechny posloupnosti přirozených čísel $(a_n)_{n=1}^{\infty}$, které pro každé prvočíslo $p$ a každé přirozené číslo $n$ splňují vztah*

$$a_n^p \equiv n \pmod{a_p}.$$

*(David Hruška)*

Řešení:
Domluvme se, že $n$ značí vždy přirozené číslo a $p$, $q$ prvočísla. Nechť posloupnost $a_n$ splňuje zadanou rovnost. Dosazením $p$ za $n$ dostaneme

$$0 \equiv a_p^p \equiv p \pmod{a_p} \quad \text{neboli} \quad a_p \mid p,$$

tedy pro každé $p$ platí buď $a_p = 1$, nebo $a_p = p$. Dále předpokládejme, že pro nějaké $p$ platí $a_p = p$. Pak pro libovolné $q$, pro které $a_q = 1$, platí

$$1 \equiv a_q^p \equiv q \pmod p,$$

tedy $p$ dělí $q - 1$, speciálně $p < q$. To znamená, že v posloupnosti budou napřed prvočísla, pro která $a_p = p$ (pokud vůbec nějaká jsou) a pak už samá taková, pro která $a_p = 1$ (pokud vůbec nějaká jsou).

Nyní ukážeme, že $a_3 = 3$ již vynutí $a_p = p$ pro všechna prvočísla $p$. Kdyby ne, měli bychom jen konečně mnoho prvočísel $p$, pro která $a_p = p$. Uvažme jejich součin $S$. Pak všechna $q$, která dělí $S - 1$, splňují $a_q = 1$ a vzhledem k tomu, že $S - 1 \equiv 2 \pmod 3$, najdeme v $S - 1$ i prvočíselného dělitele $q \equiv 2 \pmod 3$, což je ale ve sporu s rovnicí ze zadání pro $p = 3$.

Rozeberme tedy tři možnosti:

(1) Pokud pro všechna $p$ platí $a_p = 1$, je pro každé $p$ a $n$ kongruence ze zadání splněna triviálně. Zadání tak vyhovuje každá posloupnost přirozených čísel $a_n$ splňující $a_p = 1$ pro všechna $p$.

(2) Pokud pro všechna $p$ platí $a_p = p$, vezměme libovolné $n$ a prvočíslo $q$ splňující zároveň $q > n$ a $q > a_n$. Podle zadání a Malé Fermatovy věty platí $a_n^q \equiv a_n \equiv n \pmod q$, což vzhledem k volbě $q$ implikuje $a_n = n$. Tedy v tomto případě připadá v úvahu pouze posloupnost $a_n = n$, která díky Malé Fermatově větě opravdu vyhovuje.

(3) Ve zbylých případech již víme, že nutně $a_2 = 2$ a $a_p = 1$ pro všechna $p > 2$. Netriviální podmínku dává zadání pouze pro hodnotu $p = 2$, a sice, že $a_n^2 \equiv n \pmod 2$. To je ekvivalentní tomu, že $a_n$ je liché pro lichá $n$ a sudé pro sudá $n$. Můžeme si všimnout, že této podmínce již stanovené hodnoty (ty s prvočíselnými indexy) vyhovují. V tomto případě tedy vyhovují právě ty posloupnosti $a_n$ splňující $a_2 = 2$, $a_p = 1$ pro každé liché prvočíslo a $a_n$ má stejnou paritu jako $n$ pro každé $n$.

Poznámky:
Všechna řešení aspoň nějakou vyhovující posloupnost nalezla a většinou i ověřila, že splňuje zadání. Zhruba polovina řešitelů pak rozbor zdárně dokončila nějakou obměnou výše uvedeného postupu. *(David Hruška)*

## Úloha 8. (13; 7; 2,62; 3,0)

*Mějme libovolné prvočíslo $p \geq 7$. Dokažte, že pak existuje přirozené číslo $n$ a celá čísla $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_n$ nesoudělná s $p$ taková, že*

$$\begin{aligned} x_1^2 + y_1^2 &\equiv x_2^2 \pmod p, \\ x_2^2 + y_2^2 &\equiv x_3^2 \pmod p, \\ &\vdots \\ x_n^2 + y_n^2 &\equiv x_1^2 \pmod p. \end{aligned}$$

*(Filip Hlásek)*

Řešení:
Upravujme postupně následující rovnosti:

$$\begin{array}{rcrcll} 3^2 & + & 4^2 & = & 5^2 & \text{násobíme rovnost } (3^p)^2 \\ \left(3^{p+1}\right)^2 & + & \left(4 \cdot 3^p\right)^2 & = & \left(3^p \cdot 5\right)^2 & \text{násobíme rovnost } \left(\frac{5}{3}\right)^2 \\ \left(3^p \cdot 5\right)^2 & + & \left(4 \cdot 3^{p-1} \cdot 5\right)^2 & = & \left(3^{p-1} \cdot 5^2\right)^2 & \text{násobíme rovnost } \left(\frac{5}{3}\right)^2 \\ \left(3^{p-1} \cdot 5^2\right)^2 & + & \left(4 \cdot 3^{p-2} \cdot 5^2\right)^2 & = & \left(3^{p-2} \cdot 5^3\right)^2 & \text{násobíme rovnost } \left(\frac{5}{3}\right)^2 \\ \vdots & & \vdots & & & \\ \left(3^{p-i+1} \cdot 5^i\right)^2 & + & \left(4 \cdot 3^{p-i} \cdot 5^i\right)^2 & = & \left(3^{p-i} \cdot 5^{i+1}\right)^2 & \text{násobíme rovnost } \left(\frac{5}{3}\right)^2 \\ \vdots & & \vdots & & & \\ \left(3^2 \cdot 5^{p-1}\right)^2 & + & \left(4 \cdot 3^1 \cdot 5^{p-1}\right)^2 & = & \left(3^1 \cdot 5^p\right)^2 & \end{array}$$

Když pro $i \in \{0, 1, \ldots, p-1\}$ zvolíme $\overline{x_i} = 3^{p-i+1} \cdot 5^i$, $\overline{y_i} = 4 \cdot 3^{p-i} \cdot 5^i$, bude pro každé $i \in \{0, 1, \ldots, p-2\}$ platit

$$\overline{x_i}^2 + \overline{y_i}^2 \equiv \overline{x_{i+1}}^2 \pmod p$$

(nastane dokonce rovnost) a navíc jsou všechna $\overline{x_i}$ i $\overline{y_i}$ nesoudělná s prvočíslem $p \geq 7$. Z přihrádkového principu plyne, že existují $i, j \in \{0, 1, \ldots, p-1\}$ taková, že $i < j$ a zároveň $\overline{x_i}^2 \equiv \overline{x_j}^2 \pmod p$. Celá čísla $n = j - i$, $x_1 = \overline{x_i}$, $\ldots$, $x_n = \overline{x_{j-1}}$, $y_1 = \overline{y_i}$, $\ldots$, $y_n = \overline{y_{j-1}}$ splňují zadané kongruence a jsou nesoudělná s prvočíslem $p$.

Poznámky:

Zhruba stejným směrem jako autorské řešení se ubíral jedině *Radovan Švarc*, který si svým stručným a přehledným řešením vysloužil také imaginární bod.

Ostatní postupy téměř výhradně začínaly tím, že zvolily libovolné $x$ nesoudělné s $p$ a hledaly $y$ a $z$ takové, aby platilo $x^2 + y^2 \equiv z^2 \pmod{p}$. Takto postupně od libovolného $\overline{x_1}$ vygenerovaly nekonečnou posloupnost čísel $\overline{x_i}$ a $\overline{y_i}$ a poté nalezly vhodné $\overline{x_i}$ a $\overline{x_j}$ podobně jako ve vzorovém řešení. Netriviální částí je ovšem ukázat, že pro každé $x$ taková dvě celá čísla nesoudělná s $p$ existují. Některým řešitelům se to podařilo, ale cesta to byla obvykle poměrně strastiplná.

Další zajímavá úvaha postupovala obráceně. Začneme od libovolného $x_m$ nesoudělného s $p$ a pokusíme se ho rozložit na součet $x_{m-1}^2 + y_{m-1}^2 \equiv x_m^2 \pmod{p}$. Dokonce i takový postup funguje a pro každé takové $x_m$ rozklad existuje. Řešení se poté dokončí obdobně jako v předchozích případech.

Platí také silnější tvrzení než je zadaná úloha. Vždy stačí volit $n \leq 3$, $y_1 = 1$ a $1 \leq x_1 \leq 3$. Dále si všimněte, že jsme v řešení nevyužili, že $p$ je prvočíslo, ale pouze to, že je nesoudělné s čísly 3, 4 a 5. Tvrzení platí pro všechna taková čísla a dokonce bychom si mohli na začátku zvolit jinou Pythagorejskou trojici, ale tím bychom si nepomohli, neboť v každé takové trojici se vyskytuje číslo dělitelné dvěma, číslo dělitelné třemi a číslo dělitelné pěti. *(Filip Hlásek)*