Povídání k 5. sérii

Mějme celá čísla a a b a přirozené číslo n. Pokud $n|(a-b)$, řekneme, že čísla a a b jsou kongruentní podle modulu n (případně kongruentní modulo n), a píšeme $a \equiv b \pmod{n}$.

S kongruencemi se dá pracovat skoro stejně jako s rovnicemi. K oběma stranám kongruence můžeme přičíst (nebo od nich odečíst) libovolné celé číslo a můžeme je vynásobit jakýmkoli nenulovým číslem. Dělit je ale možné jen čísly nesoudělnými s modulem (tak se říká číslu n z předchozí definice). Také můžeme sečíst, odečíst nebo vynásobit libovolné dvě kongruence podle stejného modulu.

Příklad. Řešte kongruenci $3x \equiv 4 \pmod{5}$ v oboru celých čísel.

Řešení. Protože $5|(0-5)$, platí kongruence $0 \equiv 5 \pmod{5}$. Přičteme-li tuto kongruenci k té zadané, dostaneme $3x + 0 \equiv 4 + 5 \pmod{5}$, tedy $3x \equiv 9 \pmod{5}$. Protože jsou čísla 3 a 5 nesoudělná, můžeme kongruenci vydělit číslem 3. Tím dostaneme $x \equiv 3 \pmod{5}$. Všechna řešení zadané kongruence tedy dávají po dělení 5 zbytek 3. Jak každý snadno ověří, každé číslo tohoto tvaru je řešením dané kongruence. Tu tedy řeší právě ta čísla, která dávají (mod 5) zbytek 3.

Příklad. Řešte kongruenci $x^2 \equiv 2 \pmod{5}$ v oboru celých čísel.

Řešení. Tato kongruence nemá žádné řešení. Pro $x \equiv 0 \pmod{5}$ je totiž $x^2 \equiv 0 \pmod{5}$; pro $x \equiv 1 \pmod{5}$ je $x^2 \equiv 1 \pmod{5}$; pro $x \equiv 2 \pmod{5}$ je $x^2 \equiv 4 \pmod{5}$; pro $x \equiv 3 \pmod{5}$ je $x^2 \equiv 4 \pmod{5}$ a konečně pro $x \equiv 4 \pmod{5}$ je $x^2 \equiv 1 \pmod{5}$. Pro žádné číslo x tedy není $x^2 \equiv 2 \pmod{5}$.

O kongruencích platí ještě několik zajímavých tvrzení, která by se ti někdy mohla hodit:

Věta (malá Fermatova). Mějme přirozené číslo a a prvočíslo p, které nedělí a. Potom platí $a^{p-1} \equiv 1 \pmod{p}$.

Ať je n přirozené číslo. Počet všech s n nesoudělných přirozených čísel, jež jsou menší nebo rovna n, značíme $\varphi(n)$. Této funkci říkáme Eulerova.

Věta. Ať je n přirozené číslo větší než 1 a ať je $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}$ jeho rozklad na součin prvočísel (p_1, p_2, …, p_k jsou po dvou různá prvočísla, α_1, α_2, …, α_k jsou přirozená čísla). Potom platí $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$.

Věta (Eulerova). Buďte a celé číslo a m přirozené číslo nesoudělné s a. Potom platí $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Věta (Wilsonova). Mějme přirozené číslo n různé od 1. Potom platí: n je prvočíslo právě tehdy, když $(n-1)! \equiv -1 \pmod{n}$.

5th series

Topic: Congruences

Date due: February 28, 2005

PROBLEM 1 (3 POINTS)

Find all integers a, b satisfying

$$4a + 2b \equiv -1 \pmod 6,$$

$$a + b \equiv 1 \pmod 3.$$

PROBLEM 2 (3 POINTS)

Find all integers a, b satisfying

$$(a + b)^2 + 2ab = 7.$$

PROBLEM 3 (3 POINTS)

A positive integer k has the following property: if $a \equiv 0 \pmod k$ then $\tilde{a} \equiv 0 \pmod k$, where $\tilde{a}$ denotes the number a written backwards. Show that $99 \equiv 0 \pmod k$.

PROBLEM 4 (5 POINTS)

Let $n \geq 2$ be an integer. Prove that

$$\sum \frac{1}{i_1 i_2 \cdots i_k} \equiv \sum i_1 i_2 \cdots i_k \pmod{n+1},$$

summation spreading over all nonempty subsets $\{i_1, i_2, \ldots, i_k\}$ of the set $\{1, 2, \ldots, n\}$.

PROBLEM 5 (5 POINTS)

Prove that there are exactly three at most n-digit natural numbers a such that

$$a^2 \equiv a \pmod{10^n}.$$

PROBLEM 6 (5 POINTS)

Let p be a prime number. Find all integers satisfying

$$a^2 \equiv b^3 \pmod p.$$

PROBLEM 7 (5 POINTS)

a) Let p be a prime number. Show that for each $a \in \{1, 2, \ldots, p-1\}$ there is exactly one integer $x \in \{1, 2, \ldots, p-1\}$ such that $ax \equiv 1 \pmod p$. Denote such x as a^{-1} and call it the inversion of a.

b) Determine the value of

$$1 \cdot 2^{-1} + 2 \cdot 3^{-1} + \cdots + (p-2) \cdot (p-1)^{-1} \pmod p$$

for any odd prime p.

PROBLEM 8 (5 POINTS)
Let n be a positive integer and p be a prime number, $p|n^2+n+1$. Prove that $p \equiv 1 \pmod 6$ or $p = 3$.

La 5 série

Sujet: Les congruences

Date d'expedition: 28 FÉVRIER 2005

PROBLÈME 1 (3 POINTS)
Trouvez toutes les solutions du système des congruences

$$4a + 2b \equiv -1 \pmod 6,$$
$$a + b \equiv 1 \pmod 3$$

dans l'ensemble des nombres entiers.

PROBLÈME 2 (3 POINTS)
Résolvez l'equation

$$(a+b)^2 + 2ab = 7$$

dans l'ensemble des nombres entiers.

PROBLÈME 3 (3 POINTS)
Pour le nombre naturel k s'appliqué: si $a \equiv 0 \pmod k$, donc $\tilde{a} \equiv 0 \pmod k$, où $\tilde{a}$ désigné le nombre a inscrit dans le systčme decimal a l'envers. Démontrez que $99 \equiv 0 \pmod k$.

PROBLÈME 4 (5 POINTS)
Nous avons un nombre naturel $n \geq 2$. Démontrez que

$$\sum \frac{1}{i_1 i_2 \cdots i_k} \equiv \sum i_1 i_2 \cdots i_k \pmod{n+1},$$

où dans les deux sommes nous additionnons a travers de tous les sous-ensembles pas vides $\{i_1, i_2, \ldots, i_k\}$ le ensemble $\{1, 2, \ldots, n\}$.

PROBLÈME 5 (5 POINTS)
Démontrez qu'il existe justement trois nombres naturels a, au maximum n-chiffres, lesquels

$$a^2 \equiv a \pmod{10^n}.$$

PROBLÈME 6 (5 POINTS)
Soit p n'importe quel nombre premier. Resolvez la congruence

$$a^2 \equiv b^3 \pmod p$$

dans l'ensemble des nombres entiers.

PROBLÈME 7 (5 POINTS)
a) Soit p n'importe quel nombre premier. Démontrez que pour chaque $a \in \{1, 2, \ldots, p-1\}$ existe justement un nombre $x \in \{1, 2, \ldots, p-1\}$, lequel est $ax \equiv 1 \pmod{p}$. Ce x nous désignons a^{-1} et nous l'appelons le nombre inversé vers le nombre a.
b) Déterminez la valeur

$$1 \cdot 2^{-1} + 2 \cdot 3^{-1} + \cdots + (p-2) \cdot (p-1)^{-1} \pmod{p}$$

pour n'importe quel nombre premier impair p.

PROBLÈME 8 (5 POINTS)
Soit n nombre naturel et p nombre premier, lequel divise $n^2 + n + 1$. Démontrez que $p \equiv 1 \pmod{6}$ ou $p = 3$.

Serie N. 5

Thema: Die Kongruenz

Termin der Absendung: 28. FEBRUAR 2005

AUFGABE N. 1 (3 PUNKTE)
Finden Sie alle Lösungen des Kongruenzensystem

$$4a + 2b \equiv -1 \pmod{6},$$

$$a + b \equiv 1 \pmod{3}$$

im Bereich der ganzen Zahlen.

AUFGABE N. 2 (3 PUNKTE)
Lösen Sie die Gleichung

$$(a+b)^2 + 2ab = 7$$

im Bereich der ganzen Zahlen.

AUFGABE N. 3 (3 PUNKTE)
Gelte für eine natürliche Zahl k die Bedingung: Falls $a \equiv 0 \pmod{k}$, dann ist auch $\tilde{a} \equiv 0 \pmod{k}$, wobei $\tilde{a}$ die Zahl a im Dezimalsystem rückwärts geschrieben ist.
Beweisen Sie, dass dann $99 \equiv 0 \pmod{k}$.

AUFGABE N. 4 (5 PUNKTE)
Sei $n \geq 2$ eine natürliche Zahl. Beweisen Sie, dass

$$\sum \frac{1}{i_1 i_2 \cdots i_k} \equiv \sum i_1 i_2 \cdots i_k \pmod{n+1},$$

wobei in beiden Summen über alle nichtleere Untermengen $\{i_1, i_2, \ldots, i_k\}$ der Menge $\{1, 2, \ldots, n\}$ summiert wurde.

AUFGABE N. 5 (5 PUNKTE)
Beweisen Sie, dass drei höchstens n-stellige natürliche Zahlen a existieren, so dass

$$a^2 \equiv a \pmod{10^n}.$$

AUFGABE N. 6 (5 PUNKTE)
Sie p eine beliebige Primzahl. Lösen Sie die Kongruenzrelation

$$a^2 \equiv b^3 \pmod{p}$$

im Bereich der ganzen Zahlen.

AUFGABE N. 7 (5 PUNKTE)
a) Sei p eine beliebige Primzahl. Beweisen Sie, dass für jedes $a \in \{1, 2, \ldots, p-1\}$ genau eine Zahl $x \in \{1, 2, \ldots, p-1\}$ existiert, so dass $ax \equiv 1 \pmod{p}$. Diese Zahl wurde a^{-1} bezeichnet und Inverszahl zur Zahl a genannt.
b) Berechnen Sie

$$1 \cdot 2^{-1} + 2 \cdot 3^{-1} + \cdots + (p-2) \cdot (p-1)^{-1} \pmod{p}$$

für beliebige ungerade Primzahl p.

AUFGABE N. 8 (5 PUNKTE)
Sei n eine natürliche Zahl und p sei eine Primzahl, die $n^2 + n + 1$ teilt. Beweisen Sie, dass $p \equiv 1 \pmod{6}$ oder $p = 3$ ist.

5. série

Téma: Nerovnosti

Termín odeslání: 28. UNORA 2005

1. ÚLOHA (3 BODY)
Určete všechna celá čísla a, b splňující

$$4a + 2b \equiv -1 \pmod 6,$$
$$a + b \equiv 1 \pmod 3.$$

2. ÚLOHA (3 BODY)
Určete všechna celá čísla a, b splňující

$$(a + b)^2 + 2ab = 7.$$

3. ÚLOHA (3 BODY)
Přirozené číslo k má následující vlastnost: je-li $a \equiv 0 \pmod k$, potom $\tilde{a} \equiv 0 \pmod k$, kde $\tilde{a}$ značí číslo a napsané pozpátku. Ukažte, že $99 \equiv 0 \pmod k$.

4. ÚLOHA (5 BODŮ)
Buď $n \geq 2$ přirozené. Dokažte, že

$$\sum \frac{1}{i_1 i_2 \cdots i_k} \equiv \sum i_1 i_2 \cdots i_k \pmod{n+1},$$

přičemž sčítáme přes všechny neprázdné podmnožiny $\{i_1, i_2, \ldots, i_k\}$ množiny $\{1, 2, \ldots, n\}$.

5. ÚLOHA (5 BODŮ)
Dokažte, že existují právě tři nejvýše n-ciferná přirozená čísla a taková, že

$$a^2 \equiv a \pmod{10^n}.$$

6. ÚLOHA (5 BODŮ)
Buď p prvočíslo. Najděte všechna celá čísla a, b splňující

$$a^2 \equiv b^3 \pmod p.$$

7. ÚLOHA (5 BODŮ)
a) Buď p prvočíslo. Ukažte, že pro každé $a \in \{1, 2, \ldots, p-1\}$ existuje právě jedno celé číslo $x \in \{1, 2, \ldots, p-1\}$ takové, že $ax \equiv 1 \pmod p$. Označme toto x jako a^{-1} a nazývejme ho inverzí k a.
b) Určete hodnotu výrazu

$$1 \cdot 2^{-1} + 2 \cdot 3^{-1} + \cdots + (p-2) \cdot (p-1)^{-1} \pmod p$$

pro libovolné liché prvočíslo p.

8. ÚLOHA (5 BODŮ)
Nechť je n přirozené číslo a p prvočíslo, $p | n^2 + n + 1$. Dokažte, že $p \equiv 1 \pmod 6$ nebo $p = 3$.

Řešení 5. série

1. úloha **(67, 58, 2,54, 3,0)**

Určete všechna celá čísla a, b splňující

$$4a + 2b \equiv -1 \pmod 6,$$

$$a + b \equiv 1 \pmod 3.$$

Z první rovnice podle definice kongruence dostáváme, že

$$4a + 2b - 1 = 6k$$

pro nějaké celé číslo k. Jenže na levé straně je liché číslo a na pravé straně je sudé číslo, tudíž tato kongruence nemůže mít řešení. Omlouváme se řešitelům, že úloha byla až tak jednoduchá. Původní plán byl, aby soustava měla řešení, nicméně se nám do zadání vloudila chybička.

2. úloha **(53, 35, 2,17, 3,0)**

Určete všechna celá čísla a, b splňující

$$(a + b)^2 + 2ab = 7.$$

Předpokládejme, že a a b jsou libovolná čísla vyhovující zadání. Uvažujme zadanou rovnici modulo 4: po roznásobení druhé mocniny dostaneme, že $a^2 + b^2 \equiv 3 \pmod 4$. Jak snadno zjistíš vyzkoušením všech možných zbytků modulo 4 (podobně jako v úvodu k této sérii), platí pro libovolné celé číslo x buďto $x^2 \equiv 0 \pmod 4$, nebo $x^2 \equiv 1 \pmod 4$. To ale znamená, že součet dvou druhých mocnin může po dělení čtyřmi dávat pouze zbytky 0, 1 nebo 2. Pro žádná celá čísla tedy neplatí $a^2 + b^2 \equiv 3 \pmod 4$, úloha tudíž nemá řešení.

3. úloha **(33, 2, 0,61, 1,0)**

Přirozené číslo k má následující vlastnost: je-li $a \equiv 0 \pmod k$, potom $\tilde{a} \equiv 0 \pmod k$, kde $\tilde{a}$ značí číslo a napsané pozpátku. Ukažte, že $99 \equiv 0 \pmod k$.

Milí řešitelé,

úvodem řešení této úlohy bych se Vám chtěl omluvit za její obtížnost. Když jsme ji zadávali, považovali jsme ji za poměrně jednoduchou. Jak se ale blížil ten nepříjemný okamžik, kdy bylo třeba napsat vzorové řešení, se stále zvětšujícím se úlekem jsem si začínal uvědomovat, že úloha není tak jednoduchá, jak se napřed zdála, a že ji snad ani nedokážu vyřešit. Tak špatně to naštěstí nakonec nedopadlo, takže se můžete pokochat řešením, které jeden z Vás našel v nějaké knize.

Ať je k libovolné přirozené číslo, které splňuje podmínky ze zadání. Není těžké si uvědomit, že k má nějaký násobek, který začíná $500\ldots$ Pišme tento násobek n v desítkové soustavě jako $n = 500abc\ldots z$, počet cifer tohoto čísla značme m. Protože k dělí číslo n, dělí i číslo $\tilde{n} = z\ldots cba005$. Vynásobíme-li toto číslo číslem 10^{m-1}, dostaneme číslo $z\ldots cba0050\ldots0$, jež je také násobek čísla k. Přičteme-li k němu číslo n, zjistíme, že k dělí i číslo $l = z\ldots cba01000abc\ldots z$. Pak nutně k dělí i $\tilde{l} = z\ldots cba00010abc\ldots z$, a tedy i $l - \tilde{l} = 990\ldots0 = 99 \cdot 10\ldots0$.

A nyní už nám ke spokojenosti chybí jen maličkost, a sice uvědomit si, že k je nesoudělné s 10. Pro spor předpokládejme, že tomu tak není.

a) $10|k$. Pak by muselo být $k|\tilde{k}$, ale číslo $\tilde{k}$ má méně cifer než k, a je tedy menší než k, což není možné.

b) $2|k$, ale 5 nedělí k. V tomto případě dostaneme spor při uvažování čísla $\widetilde{5k}$.

c) $5|k$, ale 2 nedělí k. Tentokrát bude spor třeba kvůli číslu $\widetilde{2k}$.

A to je vše, zbývá už jen popřát dobrou noc a sladké sny ...

Poznámky k došlým řešením: Opravovat tuto úlohu pro mne jako pro studentku logiky znamenalo vrcholný zážitek – logických chyb se vyvarovalo jen několik řešitelů, skutečně správné řešení se objevilo jen jedno jediné.

poučení první

V anglickém zadání byla chyba. Omlouváme se všem, kteří se o ní nedověděli včas. Zejména u cizojazyčných sérií se chyby v zadání občas vyskytnou, většinou ale bývá jednoduché je odhalit srovnáním zadání v různých jazycích. Pokud se vám zdá, že po vás chceme důkaz tvrzení, které neplatí, doporučuji následující postup:

1. Přečtěte si zadání ještě jednou.

2. Podívejte se na naše webové stránky; jakmile se o chybě v zadání dovíme, informujeme vás o tom přímo na hlavní stránce.

3. Pošlete nám mail.

Snažila jsem se, aby řešitelé, kteří vycházeli z chybného zadání, nebyli znevýhodněni oproti těm, kteří měli k dispozici zadání správné. Tedy to, že jsme udělali chybu, by vám nemělo uškodit. Přesto bývá v těchto případech těžké být docela fair...

poučení druhé

Tentokrát už k těm logickým chybám.

Podle zadání jste měli dokázat následující tvrzení:

$$(\forall a\,(k|a \Rightarrow k|\tilde{a})) \Rightarrow k|99.$$

V řeči lidské: ze zadání vyplývalo, že o k platí: **kdykoli** $k|a$, pak také $k|\tilde{a}$. Ještě jinak: číslo k má zmiňovanou vlastnost pro **všechna** čísla a! V matematice se často výslovné vyjádření toho, že danou vlastnost mají všechny uvažované objekty, vynechává – uvažte například následující věty:

„Součet úhlů v trojúhelníku je 180°."

„Číslo 3 má následující vlastnost: jestliže $3|a$, pak $3|S(a)$, kde $S(a)$ je ciferný součet čísla a."

Nestačilo tedy ukázat takové hodnoty k, a, že $k|a$, $k|\tilde{a}$, $k \nmid 99$, a prohlásit, že zadané tvrzení neplatí! Za tento typ „řešení" jsem neudělovala žádné body.

poučení třetí

K mému zděšení více než dvě třetiny řešitelů dokazovalo implikaci

$$k|99 \Rightarrow (\forall a\,(k|a \Rightarrow k|\tilde{a}))\,.$$

Doufám, že není třeba na tomto místě dlouze vysvětlovat, jaký je rozdíl mezi implikací „Jestliže A, pak B." a implikací „Jestliže B, pak A." Těm, kterým není jasný (ale i všem ostatním), vřele doporučuji knihu Raymonda Smullyana *Jak se jmenuje tahle knížka?* Po jejím přečtení vás snad nenapadne začít řešení slovy „Začnu od konce. Protože $k|99$, vím, že ... "

Obvykle bych za řešení tohoto typu žádné body neudělovala, ale velký počet nešťastníků, kteří se zmiňované chyby dopustili, mne obměkčil a za jinak správný důkaz zmiňované implikace jsem dávala bod.

4. úloha **(31, 30, 4,74, 5,0)**

Buď $n \geq 2$ přirozené. Dokažte, že

$$\sum \frac{1}{i_1 i_2 \cdots i_k} \equiv \sum i_1 i_2 \cdots i_k \pmod{n+1},$$

přičemž sčítáme přes všechny neprázdné podmnožiny $\{i_1, i_2, \ldots, i_k\}$ množiny $\{1, 2, \ldots, n\}$.

Mějme libovolné přirozené číslo $n \geq 2$.

Uvažujme nejprve součin $(1+1)(1+\frac{1}{2})(1+\frac{1}{3})\cdots(1+\frac{1}{n})$. Roznásobením zřejmě dostaneme $1 + \sum \frac{1}{i_1 i_2 \cdots i_k}$, kde stejně jako v zadání sčítáme přes všechny neprázdné podmnožiny množiny $\{1, 2, \ldots, n\}$. Tento součin je ale také roven $\frac{2}{1}\frac{3}{2}\frac{4}{3}\cdots\frac{n+1}{n} = n+1$. Porovnáním těchto vyjádření dostaneme, že $\sum \frac{1}{i_1 i_2 \cdots i_k} = n$.

Nyní uvažujme pro změnu součin $(1+1)(1+2)(1+3)\cdots(1+n) = (n+1)!$. Roznásobením tentokrát dostaneme $1 + \sum i_1 i_2 \cdots i_k$. Je tedy $\sum i_1 i_2 \cdots i_k = (n+1)! - 1$.

A protože zjevně $(n+1)! - 1 \equiv -1 \equiv n \pmod{n+1}$, dokazovaná kongruence platí.

Poznámky k došlým řešením: U mnoha řešitelů se vyskytl nešvar známý z řešení rovnic. Máteli dokázat $A = B$ (případně $A \equiv B$) a úpravami dojdete k $C = C$, není to ještě kompletní řešení. Musíte ještě dodat, že je možno postup sledovat i opačným směrem, že uvedené úpravy jsou ekvivalentní. Jinak se vaše řešení podobají tomuto: Chci dokázat $1 = 2$. Tak tuto rovnost vynásobím nulou a přičtu jedničku, dostanu $1 = 1$ a to platí. Problém je samozřejmě v násobení nulou, tento krok nemůžeme provést zpět, což je zde vidět, ovšem v kongruencích je situace více maskovaná, pokud uvažujeme kongruenci modulo n, potom takovéto „násobení nulou“ je i např. vynásobení obou stran číslem $(n+1)!$, což už je snadné přehlédnout. Za opomenutí úvahy o ekvivalentnosti úprav jsem body nestrhával, ovšem třeba opravovatelé matematické olympiády by tak rozhodně učinili.

5. úloha **(41, 28, 3,37, 5,0)**

Dokažte, že existují právě tři nejvýše n-ciferná přirozená čísla a taková, že

$$a^2 \equiv a \pmod{10^n}.$$

Tvrzení dokažme indukcí podle přirozeného čísla n.

a) Je-li $n = 1$, hledáme všechna jednociferná přirozená čísla a splňující $a^2 \equiv a \pmod{10}$. Vyzkoušením všech devíti jednociferných čísel zjistíme, že kongruenci vyhovují pouze čísla 1, 5 a 6.

b) Mějme libovolné $n > 1$ a předpokládejme, že kongruence $a^2 \equiv a \pmod{10^{n-1}}$ má právě tři nejvýše $(n-1)$-ciferná řešení. Ať je $x = a + 10^{n-1}b$ libovolné nejvýše n-ciferné řešení kongruence $x^2 \equiv x \pmod{10^n}$, a je tedy nejvýše $(n-1)$-ciferné číslo a $b \in \{0, 1, \ldots, 9\}$. Potom $(a+10^{n-1}b)^2 \equiv a+10^{n-1}b \pmod{10^n}$, tedy $a^2+2ab10^{n-1}+10^{2n-2}b^2 \equiv a+10^{n-1}b \pmod{10^n}$, odkud dostáváme, že $a^2 \equiv a \pmod{10^{n-1}}$. Podle indukčního předpokladu tedy může a nabývat právě tří různých hodnot.

Nechť a dále nabývá libovolné z těchto možných hodnot a ukažme, že tomuto a odpovídá jediné b. Zřejmě platí $10^{2n-2} \equiv 0 \pmod{10^n}$, výše uvedenou kongruenci tedy můžeme psát jako $a^2+2ab10^{n-1} \equiv a+10^{n-1}b \pmod{10^n}$, což snadno upravíme do tvaru $10^{n-1}b(2a-1) \equiv (a-a^2) \pmod{10^n}$. Číslo $a-a^2$ je dělitelné číslem 10^{n-1}, označme $c = \frac{a-a^2}{10^{n-1}}$, což je celé číslo. Potom $10^{n-1}b(2a-1) \equiv 10^{n-1}c \pmod{10^n}$, a tudíž zřejmě platí $b(2a-1) \equiv c \pmod{10}$.

Jakých hodnot (mod 10) může číslo $2a-1$ nabývat? Protože $a \equiv a^2 \pmod{10^{n-1}}$, jistě také $a \equiv a^2 \pmod{10}$ a tedy a může dávat při dělení 10 pouze zbytky 1, 5, nebo 6. Pro $a \equiv 1 \pmod{10}$ je $2a-1 \equiv 1 \pmod{10}$, pro $a \equiv 5 \pmod{10}$ je $2a-1 \equiv 9 \pmod{10}$ a pro $a \equiv 6 \pmod{10}$ je $2a-1 \equiv 1 \pmod{10}$. Je-li $2a-1 \equiv 1 \pmod{10}$, označme $d = 1$, pro $2a-1 \equiv 9 \pmod{10}$ buď $d = -1$. V obou případech je $(2a-1)d \equiv 1 \pmod{10}$, takže vynásobíme-li výše uvedenou kongruenci číslem d, dostaneme $b \equiv b(2a-1)d \equiv cd \pmod{10}$. Protože $b \in \{0, 1, \ldots, 9\}$, je touto kongruencí číslo b určeno jednoznačně. Každé ze tří možných hodnot a tudíž odpovídá právě jedno b, kongruence tedy má právě tři řešení i pro n (úpravy vedoucí k určení b byly ekvivalentní, takže je jasné, že nalezené číslo $x = a + 10^{n-1}b$ kongruenci vskutku řeší).

6. úloha **(22, 5, 1,36, 0,5)**

Buď p prvočíslo. Najděte všechna celá čísla a, b splňující

$$a^2 \equiv b^3 \pmod{p}.$$

Úlohu budeme řešit pro $a, b \in \{0, 1, \ldots, p-1\}$. Rozmysli si, že všechna řešení pak dostaneme tak, že k takto získaným řešením přičteme celočíselný násobek p.

Všechny kongruence budou modulo p.

V případě, že $b = 0$, řešíme kongruenci

$$a^2 \equiv 0.$$

Podle definice kongruence je tedy a^2 násobek čísla p. Potom ale i číslo a musí být násobek p, jelikož p je prvočíslo. Totiž pro $a = 0$ není co řešit a je-li $a \neq 0$, potom pokud a neobsahuje p ve svém prvočíselném rozkladu, nebude p obsaženo ani v prvočíselném rozkladu a^2. V tomto případě tedy vyhovuje pouze $a = 0$.

V případě $b \neq 0$ využijeme řešení úlohy 7, části a. Pronásobíme rovnici výrazem b^{-2}, dostaneme tak

$$\left(ab^{-1}\right)^2 \equiv b.$$

Označme c takové číslo z $\{0, 1, \ldots, p-1\}$, že $c \equiv ab^{-1}$. Dostaneme tak, že $b \equiv c^2$. Dosadíme do rovnice:

$$a^2 \equiv c^6,$$

$$(a - c^3)(a + c^3) \equiv 0.$$

Odtud plyne, že $a \equiv c^3$ nebo $a \equiv -c^3$.

Dohromady dostáváme, že všechna řešení jsou tvaru $a \equiv \pm c^3$ a $b \equiv c^2$ pro nějaké vhodné $c \in \{0, 1, \ldots, p-1\}$. Na druhou stranu si dosazením snadno rozmyslíš, že takováto řešení vyhovují (navíc přechodem od c k $p - c$ stačí předpokládat, že $a \equiv c^3$).

7. úloha **(27, 25, 4,19, 5,0)**

a) Buď p prvočíslo. Ukažte, že pro každé $a \in \{1, 2, \ldots, p-1\}$ existuje právě jedno celé číslo $x \in \{1, 2, \ldots, p-1\}$ takové, že $ax \equiv 1 \pmod{p}$. Označme toto x jako a^{-1} a nazývejme ho inverzí k a.

b) Určete hodnotu výrazu

$$1 \cdot 2^{-1} + 2 \cdot 3^{-1} + \cdots + (p-2) \cdot (p-1)^{-1} \pmod{p}$$

pro libovolné liché prvočíslo p.

Části a) i b) vyřešíme velmi podobně.

V části a) chceme dokázat, že pro a ze zadání mezi čísly $a \cdot 1$, $a \cdot 2$, ... , $a \cdot (p-1)$ existuje právě jedno, které je kongruentní s 1 modulo p.

Nejprve si uvědomíme, že tato čísla dávají různé zbytky při dělení p. Pro spor předpokládejme, že $a \cdot y \equiv a \cdot z \pmod{p}$ pro $y \neq z$, $y, z \in \{1, 2, \ldots, p-1\}$. Protože a je nesoudělné s p, lze jím vydělit a dostaneme, že $y \equiv z \pmod{p}$. Tím, že $y, z \in \{1, 2, \ldots, p-1\}$, dostaneme, že $y = z$, což je spor s původním předpokladem, že $y \neq z$.

Tedy čísla $a \cdot 1$, $a \cdot 2$, ... , $a \cdot (p-1)$ dávají různé zbytky při dělení p, nikdy nedávají zbytek 0 (rozmysli si) a těchto čísel je $(p-1)$. Tedy zmiňovaná čísla musí dávat všechny z $p-1$ možných zbytků při dělení p různých od nuly. Speciálně tedy existuje právě jedno x takové, že $a \cdot x \equiv 1 \pmod{p}$.

V části b) máme sečíst $p-2$ čísel $1 \cdot 2^{-1}$, $2 \cdot 3^{-1}$, ... , $(p-2) \cdot (p-1)^{-1}$.

Budeme předpokládat $p \geq 3$. Pro $p = 2$ dostaneme prázdnou sumu, která se obvykle definuje jako 0.

Nejprve si uvědomíme, že tato čísla nikdy nedávají zbytek 0 nebo 1 (rozmysli si).

Dále si uvědomíme, že jsou navzájem různá.

Kdyby

$$y \cdot (y+1)^{-1} \equiv z \cdot (z+1)^{-1} \pmod{p},$$

pro $y \not\equiv z$, potom

$$y \cdot (z+1) \equiv z \cdot (y+1) \pmod{p},$$

$$y \equiv z \pmod{p},$$

což je opět spor s předpokladem $y \not\equiv z$.

Tedy, podobně jako v části a), čísla, která chceme sčítat, jsou v nějakém pořadí kongruentní s čísly 2, 3, 4, ... , $p-1$.

Závěrem

$$1 \cdot 2^{-1} + 2 \cdot 3^{-1} + \cdots + (p-2) \cdot (p-1)^{-1} \equiv 2 + 3 + \cdots + (p-1) \equiv$$

$$\equiv (2 + (p-1)) + (3 + (p-2)) + \cdots + \left(\frac{p-1}{2} + \frac{p+3}{2}\right) + \frac{p+1}{2} \equiv \frac{p-3}{2} \cdot (p+1) + \frac{p+1}{2} \equiv$$

$$\equiv \frac{(p-2)(p+1)}{2} \equiv -1 \equiv p-1 \pmod{p}.$$

8. úloha **(14, 3, 1,07, 0,0)**

Nechť je n přirozené číslo a p prvočíslo, $p|n^2+n+1$. Dokažte, že $p \equiv 1 \pmod 6$ nebo $p = 3$.

Řešení podle Franty Konopeckého.

Rozebírejme možné zbytky p při dělení 6. $n^2+n+1 = n(n+1)+1$ je liché číslo, tedy každé prvočíslo, které dělí n^2+n+1, musí být liché. Tím zbývají zbytky 1, 3, 5. Zbytek 1 povoluje zadání úlohy. Jediné prvočíslo, které dává zbytek 3 je trojka, která je povolena. Zbývá dokázat, že $p \not\equiv 5 \pmod 6$.

Pro spor nechť $p \equiv 5 \pmod 6$. Jelikož $p|n^2+n+1$, platí i $p|(n-1)(n^2+n+1)$, tj. $n^3 \equiv 1 \pmod p$. Číslo $\frac{p-2}{3}$ je celé ($p \equiv 5 \pmod 6$), tudíž platí i

$$1 \equiv 1^{\frac{p-2}{3}} \equiv \left(n^3\right)^{\frac{p-2}{3}} \equiv n^{p-2} \pmod p.$$

Podle malé Fermatovy věty je $n^{p-1} \equiv 1 \pmod p$ (n a p jsou nesoudělná. Potom $n^{p-1} \equiv n^{p-2}$ a vydělením n^{p-2} (n^{p-2} a p jsou nesoudělná, jelikož n a p jsou nesoudělná) dostáváme, že $n \equiv 1 \pmod p$.

Nyní už jen $0 \equiv n^2+n+1 \equiv 1^2+1+1 \equiv 3 \pmod p$. Ale prvočíslo dělitelné 3 je jediné, totiž 3, a to není kongruentní s 5 modulo 6.

Jiné řešení.

Podobně jako v předchozím řešení zjistíme, že jediná problematická situace je, když $p \equiv 5 \pmod 6$.

Myšlenka řešení je, že si najdeme v jistém smyslu minimální dvojici (n, p), která nesplňuje podmínky. K této minimální dvojici pak najdeme ještě menší, což bude spor s minimalitou původní dvojice, tedy žádná dvojice nesplňující zadání nemůže existovat.

Pro spor nechť p je nejmenší prvočíslo p takové, že $p|n^2+n+1$ pro nějaké n a $p \equiv 5 \pmod 6$. K tomuto pevnému p nadále vybereme n nejmenší přirozené takové, že $p|n^2+n+1$. Jelikož $(n+kp)^2+(n+kp)+1 \equiv n^2+n+1 \pmod p$, je nutně $n \in \{1, 2, \ldots, p\}$. Snadno si dosazením ověříš, že p ani $p-1$ nevyhovují, tedy $n \in \{1, 2, \ldots, p-2\}$. Dále platí, že $(p-n-1)^2+(p-n-1)+1 \equiv (m+1)^2 - m - 1 + 1 \equiv m^2+m+1 \pmod p$. Jinými slovy, je-li kongruence splněna pro n, je splněna i pro $p-n-1$. Tedy nutně $n \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, jelikož jsme n volili, aby bylo nejmenší možné. Odtud si budeme pamatovat nerovnost $n \leq \frac{p-1}{2}$.

Víme, že $p|n^2+n+1$, tedy $n^2+n+1 = pq_1q_2\cdots q_k$, kde q_1, q_2, … q_k jsou nějaká (ne nutně různá) prvočísla. Přitom

$$q_1q_2\cdots q_k = \frac{n^2+n+1}{p} \leq \frac{\left(\frac{p-1}{2}\right)^2 + \frac{p-1}{2} + 1}{p} < \frac{\frac{p^2}{4} + \frac{p}{2} + 1}{p} = \frac{p}{4} + \frac{1}{2} + \frac{1}{p} < p,$$

v první nerovnosti jsme použili nerovnost odvozenou v předchozím odstavci, v poslední nerovnosti jsme využili skutečnosti, že $p \equiv 5 \pmod 6$, tedy $p \geq 5$.

Tedy všechna prvočísla q_1, q_2, … q_k jsou menší než p. Pokud mezi těmito prvočísly najdeme takové q_i, že $q_i \equiv 5 \pmod 6$, potom $q_i|n^2+n+1$, což je spor s minimální volbou p.

Nadále tedy můžeme předpokládat, že $q_i = 3$, nebo $q_i \equiv 1 \pmod 6$.

Rozlišme zbytky n po dělení 3.

Je-li $n \equiv 0 \pmod 3$, nebo $n \equiv 2 \pmod 3$, potom $n^2+n+1 \equiv 1 \pmod 6$. Jelikož $n^2+n+1 = pq_1\cdots q_k$, žádné q_i není 3, tedy všechna q_i jsou kongruentní s 1 modulo 6, potom ale n je kongruentní s p, což je kongruentní s 5 modulo 6, což je spor.

Je-li $n \equiv 1 \pmod 3$, tj. $n = 3h + 1$ pro nějaké h (nezáporné) celé. Potom

$$pq_1q_2 \cdots q_k = (3h+1)^2 + (3h+1) + 1 = 9h^2 + 9h + 3,$$

tedy právě jedno q_i je rovno 3, například q_1. Potom $pq_2 \cdots q_k = 3h^2 + 3h + 1 = 3h(h+1) + 1 \equiv 1 \pmod 6$. V předchozí kongruenci jsme využili toho, že číslo $3h(h+1)$ je sudé i dělitelné 3. Nyní si už snadno rozmyslíš, že se ke sporu dostaneme stejným způsobem jako v předchozím případě (kdy $n^2 + n + 1$ bylo kongruentní s 1 modulo 6).