Povídání ke druhé sérii

Tato série se zabývá prvočísly a dělitelností přirozených čísel, tedy pojmy, které asi nejspíš již znáš. Pro úplnost je zde však v krátkosti připomeneme a uvedeme ještě pojem kongruence, který sice v zadání nevystupuje, avšak při řešení by se Ti mohl hodit.

Jsou-li a, b celá čísla, pak řekneme, že a *dělí* b (píšeme $a \mid b$), pokud existuje celé číslo d takové, že platí $b = ad$. Přirozené číslo p je prvočíslo, pokud má právě dva (různé) dělitele — sebe a 1.

Máme-li a, b celá, m přirozené, pak řekneme, že číslo a je *kongruentní* s číslem b při modulu m, pokud číslo a dává při dělení číslem m stejný zbytek jako číslo b, jinými slovy $m \mid a - b$. Tuto skutečnost zapisujeme ve tvaru $a \equiv b \pmod m$, tento zápis pak nazýváme kongruencí.

Snadno si zajisté sám dokážeš (vše plyne přímo z definice), že kongruence mají následující vlastnosti:

(a) Pokud $a \equiv b \pmod m$ a $c \equiv d \pmod m$, pak $a+c \equiv b+d \pmod m$ a $ac \equiv bd \pmod m$.
(b) Pokud $a \equiv b \pmod m$, $a = a'd$, $b = b'd$ a $(d, m) = 1$, pak $a' \equiv b' \pmod m$.

Tyto dvě vlastnosti nám neříkají nic jiného než, že kongruence lze mezi sebou sčítat, násobit a za jistých předpokladů je lze dělit číslem.

Nechť je nyní p prvočíslo, uvažujme $p-1$ čísel $1, 2, \ldots, p-1$. Je-li $a \in \mathbb{Z}$ a p nedělí a, je a kongruentní právě s jedním z čísel $1, 2, \ldots, p-1$. Všechna celá čísla nedělitelná p můžeme tedy rozdělit do $p-1$ disjunktních skupin podle toho, s kterým z čísel $1, 2, \ldots, p-1$ jsou kongruentní.[1] Vybereme-li nyní z každé skupiny po jednom číslu, dostáváme systém p čísel, který nazýváme *redukovaný systém zbytků při modulu p*.

Ještě se zmiňme o jednom ne zcela obvyklém zápisu, který se vyskytuje v šesté úloze. Zápisem $n!$ je pochopitelně míněno n faktoriál, tj. $n(n-1)(n-2)\ldots 2.1$. Zápisem 11!! je však míněno (11!)!, zápis 11!!! značí ((11!)!)! atd. (Obvykle se zápisem $n!!$ myslí součin všech přirozených čísel menších nebo rovných n, která mají stejnou paritu jako n, tj. např. $11! = 11.9.7.5.3.1$, zatímco $10! = 10.8.6.4.2.$)

2. série

Téma: Prvočísla a dělitelnost

Termín odeslání: 26. ŘÍJNA 1998

1. ÚLOHA (3 BODY)

Rozhodněte, zda je číslo $1234567891011121314\ldots197198199200$ dělitelné devíti. Dekadický zápis našeho čísla vznikne tak, že píšeme za sebe postupně čísla od jedné až do dvou set.

[1] Do první skupiny dáme čísla dávající při dělení p zbytek 1, do druhé ta se zbytkem 2, ..., do $(p-1)$-vé čísla, která při dělení p dají zbytek $p-1$.

2. úloha (3 body)
Ukažte, že pro libovolné přirozené číslo n je číslo $7^{7^n} + 2$ dělitelné devíti.

3. úloha (3 body)
Uvažujme čísla tvaru $\frac{1}{p}$, kde p je prvočíslo. Rozhodněte, zda z nich můžeme vybrat konečně mnoho různých čísel, jejichž součet je 1.

4. úloha (5 bodů)
Označme a_n n-tou číslici v desetinném rozvoji Ludolfova čísla π (o tomto čísle můžete bez důkazu předpokládat, že je iracionální), přičemž všechny nuly nahradíme desítkami. Dále označme $b_n = a_1 \cdot a_2 \cdot \ldots \cdot a_n \bmod 11$. Dokažte, že b_n není periodická posloupnost (ani s případnou předperiodou).

5. úloha (5 bodů)
Ukažte, že existuje nekonečně mnoho přirozených čísel n takových, že číslo $n^{n+1} + 1$ je dělitelné číslem 17.

6. úloha (5 bodů)
Ukažte, že posloupnost $11! + 1$, $11!! + 1$, $11!!! + 1$, $11!!!! + 1$, ... , obsahuje nekonečně mnoho čísel složených.

7. úloha (5 bodů)
Zvolme si nějaká dvě přirozená čísla a_0, k a vytvořme posloupnost $\{a_n\}_{n=0}^{\infty}$ tak, že a_{n+1} je největší prvočíslo, které dělí číslo $a_n + k$. Dokažte, že tato posloupnost je periodická (s případnou předperiodou).

8. úloha (5 bodů)
Nalezněte všechna lichá přirozená čísla n taková, že n dělí číslo $17^n - 1$.

Řešení 2. série

1. úloha
Rozhodněte, zda je číslo $1234567891011121314 \ldots 197198199200$ dělitelné devíti. Dekadický zápis našeho čísla vznikne tak, že píšeme za sebe postupně čísla od jedné až do dvou set.

Tuto úlohu by šlo řešit pomocí známého pravidla pro dělitelnost devíti, které tvrdí, že číslo je dělitelné devíti právě tehdy, když jeho ciferný součet je dělitelný devíti, v autorském řešení se pokusím ukázat mnohem méně pracný postup.

Označme nejprve $A = 1234567891011121314\ldots197198199200$. Uvědomíme-li si, co dekadický zápis přirozeného čísla vlastně znamená, můžeme si zkoumané číslo přepsat do tvaru $A = 200+199\cdot10^3+198\cdot10^6+197\cdot10^9+\cdots$. Dále víme, že pro libovolné přirozené číslo k platí $10^k-1 = (10-1)\cdot(10^{k-1}+10^{k-2}+\cdots+10^2+10+1) = 9\cdot(10^{k-1}+10^{k-2}+\cdots+10^2+10+1) = 9\cdot m$, kde m je přirozené číslo, tudíž číslo 10^k-1 je pro libovolné přirozené k dělitelné devíti. Tento poznatek využijeme pro naše zkoumané číslo a máme

$$\begin{aligned}
A &= 200 + 199\cdot10^3 + 198\cdot10^6 + 197\cdot10^9 + \cdots \\
&= 200 + 199\cdot(10^3 - 1 + 1) + 198\cdot(10^6 - 1 + 1) + 197\cdot(10^9 - 1 + 1) + \cdots \\
&= 200 + 199 + 198 + 197 + \cdots + 199\cdot(10^3 - 1) + 198\cdot(10^6 - 1) + 197\cdot(10^9 - 1) + \cdots \\
&= 200 + 199 + 198 + 197 + \cdots + 1 + 9\cdot j,
\end{aligned}$$

kde j je nějaké přirozené číslo. Tedy otázka, zda je původní číslo dělitelné číslem 9 se nám převedla na otázku, zda je číslo $200+199+198+197+\cdots+3+2+1$ dělitelné číslem devět. Ono je však součtem čísel od jedné do dvou set, což dle známého vzorečku je $\frac{200\cdot201}{2}$. Toto číslo devíti dělitelné není, a proto ani naše zkoumané číslo A není dělitelné devíti.

Poznámky opravovatele: Většina řešitelů měla správné řešení. Ti, co si chtěli úlohu hodně zjednodušit, měli obvykle nedostatečné zdůvodnění a já jsem jim musel strhnout body, i když vlastně přišli na něco navíc, takže mě to mrzelo. Mnozí řešitelé vyslovili kriterium dělitelnosti devíti ve formě implikace, a pak použili opačnou implikaci — to se mi nelíbilo, ale body jsem za to nestrhával.

2. úloha
Ukažte, že pro libovolné přirozené číslo n je číslo $7^{7^n}+2$ dělitelné devíti.

Tvrzení dokážeme matematickou indukcí. Pro $n=0$ je naše číslo rovno $7^{7^0}+2 = 7^1+2 = 9$, tedy je dělitelné číslem devět. Nyní předpokládejme, že pro $n=k$ (kde $k\geq0$) platí, že naše číslo je dělitelné devíti a ukažme, že tomu tak je i pro $n=k+1$. Dle předpokladu víme, že $7^{7^k}+2 = 9\cdot r$, kde r je přirozené číslo. Nyní si trochu poupravíme naše číslo pro $n=k+1$:

$$7^{7^{k+1}} + 2 = 7^{7\cdot7^k} + 2 = \left(7^{7^k}\right)^7 + 2 = (9\cdot r - 2)^7 + 2,$$

kde v poslední úpravě jsme využili indukční předpoklad. Abychom nyní ukázali, že zkoumané číslo je pro $n=k+1$ dělitelné číslem devět, stačí nahlédnout, že číslo uvedené v poslední sadě rovností vpravo, tj. číslo $(9\cdot r-2)^7+2$, je dělitelné devíti. To je však vidět, když si závorku roznásobíme pomocí binomické věty: $(9\cdot r-2)^7+2 = (9\cdot r)^7 - 7\cdot(9\cdot r)^6\cdot2+\cdots+(-128+2)$. Napravo máme součet čísel, z nichž každé je dělitelné devíti, tj. i jejich součet je dělitelný devíti, tedy i naše zkoumané číslo pro $n=k+1$ je dělitelné devíti. Tím je hotov druhý indukční krok a důkaz je ukončen.

Poznámky opravovatele: Tuto poměrně jednoduchou úlohu řešila většina z těch, kdo ji poslali, standardně a taky bezchybně. Jelikož se žádná originální správná řešení neobjevila, imaginárními body jsem šetřil.

3. úloha
Uvažujme čísla tvaru $\frac{1}{p}$, kde p je prvočíslo. Rozhodněte, zda z nich můžeme vybrat konečně mnoho různých čísel, jejichž součet je 1.

Odpověď zní ne. Tuto odpověď zdůvodníme tzv. důkazem sporem, tj. budeme předpokládat, že z našich čísel lze vybrat taková, že jejich součet je jedna a odvodíme nesmyslné tvrzení — spor.

Mějme tedy n prvočísel $p_i, i = 1, \dots n$, takových, že platí

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots + \frac{1}{p_n} = 1.$$

Když tuto rovnost vynásobíme součinem $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$, dostaneme na levé straně součet přirozených čísel, z nichž první číslo není dělitelné p_1 a zbývající jsou dělitelná číslem p_1, tj. dohromady není levá strana dělitelná prvočíslem p_1, naproti tomu na pravé straně rovnosti budeme mít součin čísel $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$, který je dělitelný prvočíslem p_1. Dostali jsme tedy rovnost, kde jedna strana je dělitelná p_1 a druhá není, to však nastat nikdy nemůže a tím jsme nalezli hledaný spor.

Poznámky opravovatele: S radostí jsem po delší době uděloval téměř jenom plné počty bodů, v řešeních se v drtivé většině případů nevyskytovaly žádné vážnější chyby. Jen bych snad chtěl poprosit některé zkušenější řešitele: Pokud řešíte tyto jednodušší úložky, snažte se precizně formulovat svá řešení, uvidíte, že pak pro vás může být i lehká úloha dosti přínosná.

4. úloha
Označme a_n n-tou číslici v desetinném rozvoji Ludolfova čísla π (o tomto čísle můžete bez důkazu předpokládat, že je iracionální), přičemž všechny nuly nahradíme desítkami. Dále označme $b_n = a_1 \cdot a_2 \cdot \ldots \cdot a_n \bmod 11$. Dokažte, že b_n není periodická posloupnost (ani s případnou předperiodou).

Nejdříve si uvědomíme, že 11 je prvočíslo, a tedy pro každé a nedělitelné 11 existuje b takové, že $ab \equiv 1 \mod 11$ (to si můžeš dokázat sám pomocí Eukleidova algoritmu na hledání největšího společného dělitele, nebo nahlédni do důkazu *lemmatu 1*). Takové b se jmenuje prvek inverzní k a. To nám umožňuje „dělit“ modulo 11 („nenulovým číslem“, tj. číslem nedělitelným 11) — dělení je totiž totéž, co násobení inverzním prvkem.

Důkaz vedeme sporem. Nechť pro nějaká n_0, k platí: je-li $n > n_0$, pak $b_n = b_{n+k}$. Jelikož b_n je určitě nedělitelné jedenácti, dostaneme dělením této rovnosti číslem $b_n = b_{n+k}$ kongruenci $a_{n+1} \cdot \ldots \cdot a_{n+k} \equiv 1 \mod 11$. Je-li n dost velké, platí také (stejné argumenty) $a_n \cdot \ldots \cdot a_{n+k-1} \equiv 1 \mod 11$. Tedy

$$a_{n+1} \cdot \ldots \cdot a_{n+k} \equiv a_n \cdot \ldots \cdot a_{n+k-1} \mod 11\,,$$

po dalším dělení $a_n \equiv a_{n+k} \mod 11$. Čísla a_n jsou ale cifry nebo desítka, tedy $a_n = a_{n+k}$ pro $n > n_0 + 1$. To dává, že desetinný rozvoj čísla π je periodický, pak by ale π muselo být racionální, čímž dostáváme spor.

Poznámky opravovatele: Jediná závažná chyba, která se ve vašich řešeních vyskytovala, byly důkazy typu: „Posloupnost cifer čísla π je nepravidelná, a tedy i posloupnost z ní odvozená je nepravidelná.“ To jste právě měli dokázat (nahradíme-li slovo nepravidelná slovem neperiodická). Neumím si vůbec představit, jak dokazujete, že posloupnost cifer π braná „ob jednu“ není periodická.

Také jsem strhával bod, pokud jste „dělili modulo 11“, aniž byste zmínili korektnost takové úpravy.

5. úloha

Ukažte, že existuje nekonečně mnoho přirozených čísel n takových, že číslo $n^{n+1}+1$ je dělitelné číslem 17.

Uvažujme čísla tvaru $n = 16\cdot(17\cdot k+1)$, kde k je přirozené číslo. Těchto čísel je nekonečně mnoho, protože pro různá k dostaneme různá n. Nyní již stačí ukázat, že tato čísla mají vlastnost požadovanou zadáním a úloha bude vyřešena.

Pro liché přirozené číslo m platí vzoreček $a^m + b^m = (a+b)\cdot(a^{m-1} - a^{m-2}b + \cdots - ab^{m-2} + b^{m-1})$. (Platnost tohoto vzorečku si snadno ověříš roznásobením závorek vpravo.) V našem případě je $n = 16\cdot(17\cdot k+1)$, tedy číslo $n+1$ je liché a dle posledně uvedeného vztahu (do vzorečku dosazujeme $a = n$, $b = 1$, $m = n+1$) máme

$$n^{n+1}+1 = (n+1)\cdot(n^n - n^{n-1} + \cdots - n + 1) = (16\cdot(17\cdot k+1)+1)\cdot r,$$

kde r je přirozené číslo. Po drobné úpravě můžeme poslední číslo zapsat ve tvaru $17\cdot(16\cdot k+1)\cdot r$, tj. vidíme, že je dělitelné sedmnácti, a to jsme chtěli ukázat.

Poznámky opravovatele: Základem všech správných řešení byly myšlenky podobné autorskému řešení. Někteří řešitelé používali aparátu kongruencí. Na tomto místě bych rád jen uvedl na pravou míru jeden častěji se vyskytující omyl, který spočíval ve skutečnosti, že řešitel při formální manipulaci s kongruencemi používal odmocniny. Odmocňovat kongruence příliš nejde, jak si můžeš uvědomit třeba z následujícího příkladu: platí $9 \equiv 1 \pmod 8$, ale není už pravda, že $\sqrt{9} \equiv \sqrt{1} \pmod 8$.

6. úloha

Ukažte, že posloupnost $11!+1$, $11!!+1$, $11!!!+1$, $11!!!!+1$, ... , obsahuje nekonečně mnoho čísel složených.

Řešení naší úlohy bude založeno na následujícím *lemmatu 1*, které můžeš v literatuře najít pod názvem *Wilsonova věta*. Její důkaz nalezneš v samostatném odstavečku nazvaném *Důkazy použitých vět*.

Lemma 1. *Číslo p je prvočíslo právě tehdy když $(p-1)!+1$ je dělitelné číslem p.*

Uvažujme nyní dvě po sobě jdoucí čísla z naší posloupnosti. Pokud první z nich označíme n, pak následující číslo se dá psát ve tvaru $(n-1)!+1$. Pokud by nyní n bylo prvočíslo, vidíme přímo z Wilsonovy věty (v níž bereme $p=n$), že následující číslo v naší posloupnosti je dělitelné n, větší než n, a tudíž je složené. Tím jsme ukázali, že buď číslo n, nebo číslo, které za ním v naší posloupnosti následuje, je složené, a proto mezi každými dvěma po sobě jdoucími čísly v naší posloupnosti je aspoň jedno složené. Tedy naše posloupnost obsahuje nekonečně mnoho čísel složených, což jsme chtěli ukázat.

7. úloha

Zvolme si nějaká dvě přirozená čísla a_0, k a vytvořme posloupnost $\{a_n\}_{n=0}^{\infty}$ tak, že a_{n+1} je největší prvočíslo, které dělí číslo a_n+k. Dokažte, že tato posloupnost je periodická (s případnou předperiodou).

Zvolme p libovolné prvočíslo, které nedělí k. Mezi čísly $k, 2k, \ldots, pk$ nalezneme reprezentanty všech zbytkových tříd modulo p (srovnej s úvodem k řešení čtvrté úlohy). Tedy mezi čísly $a_n+k, a_n+2k, \ldots, a_n+pk$ je určitě jedno dělitelné prvočíslem p. Nemohou to tedy být jen prvočísla. Nechť je a_n+ik nejmenší z nich, které je složené. Platí $a_{n+j}=a_n+jk$ pro $j<i$ a a_{n+i} je největší prvočíslo, které dělí a_n+ik, tedy $a_{n+i}\le(a_n+ik)/2$.

Nyní indukcí dokážeme, že žádné a_n nedosáhne hodnoty a_0+2pk a že pokud $a_{n-1}>a_n$, tak je $a_n<a_0+pk$. Druhé tvrzení pro n snadno plyne s prvního pro $n-1$, první pro n dokážeme následovně: volme $m<k$ co největší tak, aby $a_{m-1}>a_m$. Pokud se nám to podaří, je dle indukčního předpokladu $a_m<a_0+pk$ a dle úvah v předchozím odstavci je i $a_n<a_0+pk+pk$. Pokud takové m neexistuje, tj. $a_0<a_1<\cdots<a_n$, je (opět dle předchozího odstavce) $a_n<a_0+pk<a_0+2pk$

Posloupnost $\{a_n\}$ je tedy omezená, a protože se jedná o celočíselnou posloupnost, nalezneme v ní dvě stejné hodnoty. Číslo a_{n+1} je závislé jen na hodnotě a_n, tím dostáváme dokazovanou periodicitu.

Poznámky opravovatele: Všechna řešení vycházela z toho, že naše posloupnost je omezená, a tedy (díky tomu, že splňuje rekurentní vztah) „někdy začne být periodická“. Většina řešitelů využila toho, že když najdou dostatečně mnoho (alespoň k) po sobě jdoucích složených čísel větších než a_0, tak přes ně posloupnost a_n nikdy „nepřeleze“, neboť se skládá z prvočísel a v každém kroku vzroste nejvýše o k. Ona složená čísla se najdou ve tvaru $t!+2$, $t!+3$, $\ldots$, $t!+t$, kde t je dostatečně velké (např. větší než k a a_0).

Toto řešení je jednodušší než autorské, zato v něm používáme „zbytečně velká čísla“, což by nám mohlo vadit, kdybychom chtěli najít nějaký odhad indexu, od nějž bude posloupnost periodická.

8. úloha

Nalezněte všechna lichá přirozená čísla n taková, že n dělí číslo 17^n-1.

Řešení naší úlohy bude založeno na následujícím *lemmatu 2*, které můžeš v literatuře najít pod názvem *Fermatova věta*. Její důkaz nalezneš v samostatném odstavečku nazvaném *Důkazy použitých vět*.

Lemma 2. *Nechť p je prvočíslo, a je přirozené číslo, a není dělitelné p. Pak je číslo $a^{p-1}-1$ dělitelné číslem p.*

Jediné liché přirozené číslo n takové, že n dělí 17^n-1, je $n=1$. Jednička jistě dělí 17^1-1. To, že další n už neexistují, zdůvodníme sporem.

Nechť tedy $n>1$ je takové přirozené číslo, pro které $n \mid 17^n-1$ a nechť p je nejmenší prvočíselný dělitel čísla n.

Nejprve využijeme *lemma 2*. Jelikož číslo p je prvočíslo, $p \neq 17$ (protože $p \mid n \mid 17^n-1$ a $n>0$), platí $p \mid 17^{p-1}-1$. Nechť nyní je číslo k nejmenší (nenulové) přirozené číslo takové, že $p \mid 17^k-1$. Takové k skutečně existuje a dle předcházející úvahy máme pro něj odhad $k \leq p-1$. Jelikož p je liché, platí též $k>1$. Dohromady máme pro číslo k odhady $1<k\leq p-1<p$.

Pokud by $k \mid n$, bylo by číslo k dělitelem čísla n, které je dle předcházejících odhadů menší než prvočíslo p. To by však byl spor s tím, že p je nejmenší prvočíselný dělitel čísla n. Odtud vidíme, že číslo k nedělí číslo n.

Nechť při celočíselném dělení čísla n číslem k dostaneme zbytek r, to znamená, že $n=k\cdot q+r$, kde q je nějaké přirozené číslo a r přirozené číslo splňující $1\leq r<k$. Pak dle předpokladu, že $n \mid 17^n-1$ vidíme, že platí též vztahy

$$p \mid \quad 17^n-1 = 17^{k\cdot q+r}-1 = 17^r(17^{k\cdot q}-1)+17^r-1 = 17^r((17^k)^q-1)+17^r-1 =$$

$$= 17^r(17^k-1)\cdot(17^{k\cdot(q-1)}+17^{k\cdot(q-2)}+17^{k\cdot(q-3)}+\cdots+17^{k\cdot 2}+17^k+1)+17^r-1,$$

ze kterých vidíme (jelikož $p \mid 17^k-1$), že též $p \mid 17^r-1$. To je však spor s definicí čísla k. Číslo r je totiž nenulové přirozené číslo menší než k, které má vlastnost požadovanou pro k; k však bylo zvoleno jako nejmenší číslo s touto vlastností. Tím je důkaz hotov.

Poznámky opravovatele: Většina řešitelů se domnívala, že úlohu vyřešila správně, ale obvykle se vloudila do řešení nějaká chybná úvaha. Zejména, není pravda, že lze odmocňovat kongruence stejně jako rovnice (např. $7^9 \equiv 1 \pmod 9$, ale $7 \not\equiv 1 \pmod 9$). Sedm řešení bylo správných, mezi nimi se našlo pět různých postupů (užívajících Eulerovu či Fermatovu větu nebo Eukleidův algoritmus). *Jan Kynčl* dokázal tvrzení bez použití těchto vět, což je chvályhodné, a tak dostal $+2i$.

Důkazy použitých vět

V této kapitole můžeš nalézt důkazy vět, které byly bez důkazu využity v autorském řešení 2. série. Lemmata jsou zformulována trochu jinak než v řešení úloh. U prvního lemmatu je zde ukázána jen jedna implikace, druhá je totiž triviální.

Lemma 1 (Wilsonova věta). *Je-li číslo p prvočíslo, pak* $(p-1)! \equiv -1 \pmod{p}$.

Důkaz: Uvažujme množinu čísel $M = \{1, 2, \ldots, p-1\}$. Množina M tvoří redukovaný systém zbytků při modulu p. Nechť $x \in M$, pak systém čísel tvaru $x, x \cdot 2, \ldots, x \cdot (p-1)$ je také redukovaný systém zbytků při modulu p. Zdůvodnění je stejné jako v důkazu *lemmatu 2*.

Tedy pro každé $x \in M$ existuje $y \in M$, takové, že $xy \equiv 1 \pmod{p}$. Snadno nahlédneme, že pro čísla x různá od 1 a $p-1$ je číslo y nutně různé od x. Z tohoto důvodu se nám čísla $2, 3, \ldots, p-2$ rozpadají na $\frac{p-3}{2}$ dvojic čísel x, y pro které platí $xy \equiv 1 \pmod{p}$. Vynásobením těchto kongruencí máme $(p-2)! \equiv 1 \pmod{p}$. Když tuto kongruenci vynásobíme ještě kongruencí $p-1 \equiv -1 \pmod{p}$, dostaneme dokazovaný vztah. Poznamenejme ještě, že jiný (trikový) důkaz Wilsonovy věty můžeš nalézt v loňském seriálu o teorii čísel.

Lemma 2 (Fermatova věta). *Nechť p je prvočíslo, a přirozené číslo, p neděli a, pak* $a^{p-1} \equiv 1 \pmod{p}$.

Důkaz: Nechť $c_1, c_2, \ldots c_{p-1}$ je redukovaný systém zbytků při modulu p, pak také ac_1, ac_2, $\ldots, ac_{p-1}$ je redukovaný systém zbytků při modulu p (neboť $(ac_i, p) = 1$, protože $(c_i, p) = 1$; a kdyby pro nějaké $i \neq j$ bylo $ac_i \equiv ac_j \pmod{p}$, pak by muselo dle vlastnosti (b) být též $c_i \equiv c_j \pmod{p}$, což nelze).

Proto pro každé c_i existuje právě jedno ac_j s ním kongruentní. Máme tedy $p-1$ kongruencí $c_i \equiv ac_j \pmod{p}$, kde i, j nabývají hodnot $1, 2, \ldots, p-1$, každou právě jednou. Vynásobením těchto kongruencí dle vlastnosti (a) dostaneme $c_1 \cdot c_2 \cdot \ldots \cdot c_{p-1} \equiv ac_1 \cdot ac_2 \cdot \ldots \cdot ac_{p-1} \pmod{p}$, což po zkrácení čísla $c_1 c_2 \ldots c_{p-1}$ dává dokazovaný vztah.