# Teorie čísel

1. seriálová série — Termín odeslání: 2. prosince 2013

*Úlohy nejsou řazeny podle obtížnosti, do výsledného hodnocení se počítají body za všechny tři úlohy.*

Úloha 1. (5 bodů)
Nechť $n$, $k$ jsou přirozená čísla a $k$ je bezčtvercové.[1] Předpokládejme, že

$$\frac{n^3 + 2n^2 + k}{n^2 + k}$$

je celé číslo. Dokažte, že pak už platí $n = k$.

Úloha 2. (5 bodů)
Mějme přirozené číslo $n \geq 2$. Dokažte, že každé z čísel $n! + 2, n! + 3, \ldots, n! + n$ má takového prvočíselného dělitele, který není dělitelem žádného z $n - 2$ zbylých čísel.

Úloha 3. (5 bodů)
Mějme celé číslo $n$ a prvočíslo $p$. Víme, že platí

$$2^{4n} + 9^{2n} \equiv 36^n \pmod{p}.$$

Dokažte, že $p$ je tvaru $4k + 1$ pro nějaké celé číslo $k$.

[1] Tedy neexistuje přirozené číslo $a > 1$ takové, že $a^2 \mid k$.

# Teorie čísel

1. seriálová série — Vzorové řešení

## Úloha 1. (49; 28; 2,86; 3,0)

*Nechť $n$, $k$ jsou přirozená čísla a $k$ je bezčtvercové.*[2] *Předpokládejme, že*

$$\frac{n^3+2n^2+k}{n^2+k}$$

*je celé číslo. Dokažte, že pak už platí $n=k$.* *(Štěpán Šimsa)*

Standardní řešení:
Aby byl zlomek $\frac{n^3+2n^2+k}{n^2+k}$ celé číslo, musí platit

$$n^2+k \mid n^3+2n^2+k,$$

tedy $n^2+k \mid n^3+2n^2+k-(n+2)\cdot(n^2+k) = -nk-k$, neboli $n^2+k \mid nk+k$. Označme si[3] $d=(n,k)$ a vezměme si taková čísla $N$, $K$, že $n=Nd$ a $k=Kd$. Z vlastností největšího společného dělitele víme $(N,K)=1$. Navíc pokud $(K,d)=a$, tak $a \mid d$, $a \mid K$, takže $a^2 \mid k$, z čehož plyne $a=1$ ($k$ je bezčtvercové). Odtud máme, že i čísla $K$ a $d$ jsou nesoudělná. Rozepišme si nyní $n^2+k \mid nk+k$ do $N$, $K$ a $d$ a upravme:

$$\begin{aligned} N^2d^2+Kd &\mid NdKd+Kd, \\ N^2d+K &\mid NKd+K = K(Nd+1), \end{aligned}$$

ale protože je $(N,K)=1$ a $(d,K)=1$, tak $(N^2d+K,K)=(N^2d,K)=1$, a proto platí i $N^2d+K \mid Nd+1$. Čísla $N^2d+K$ i $Nd+1$ jsou obě přirozená, platí tedy $N^2d+K \le Nd+1$, což spolu s tím, že $N^2d \ge Nd$ a $K \ge 1$, znamená, že musí nastat rovnosti, a tedy $K=1$, $N=1$. Proto $n=d=k$, což jsme chtěli dokázat.

Rychlé řešení (podle Miroslava Stankoviče):
Jako minule $n^2+k \mid nk+k$, takže pro nějaké přirozené číslo $a$ platí $a(n^2+k)=nk+k$, neboli $an^2=k(n+1-a)$. Proto $k \mid an^2$, ale jelikož je $k$ bezčtvercové, tak i $k \mid an$, tedy $k \le an$. Proto $n+1-a=an^2/k \ge n$, z čehož plyne $a \le 1$. Je tedy $a=1$ a $n^2=kn$, a tak skutečně platí $n=k$.

[2] Tedy neexistuje přirozené číslo $a>1$ takové, že $a^2 \mid k$.

[3] Připomeňme si, že $(a,b)$ značí největšího společného dělitele čísel $a$, $b$.

Trikové řešení (podle Markéty Calábkové):
Opět $a(n^2+k) = nk+k$ pro nějaké přirozené číslo $a$. Tuto rovnost upravíme na tvar

$$an^2 - kn + k(a-1) = 0, \qquad (\clubsuit)$$

což je kvadratická rovnice v $n$, jejíž jeden kořen musí být přirozené číslo. Proto její diskriminant $k^2 - 4ka(a-1) = k(k-4a(a-1))$ musí být druhá mocnina celého čísla. Proto musí $k$ dělit celou druhou závorku (díky bezčtvercovosti), tedy $k \mid k-4a(a-1)$, a tedy i $k \mid 4a(a-1)$. Aby však měla rovnice ($\clubsuit$) vůbec řešení, musí být $k \geq 4a(a-1)$, takže je $4a(a-1)$ buď rovno $k$, nebo je to 0, nebo záporné číslo. Poslední možnost nemůže nastat, protože $a$ je přirozené číslo. Dále $k \neq 4a(a-1)$, protože jinak by $k$ bylo dělitelné čtyřmi, tedy by nebylo bezčtvercové. Proto $4a(a-1) = 0$, z čehož plyne $a = 1$. Rovnice ($\clubsuit$) tedy přejde na tvar $n^2 - kn = 0$, což má jediné kladné řešení $n = k$.

Poznámky:
Ti, co se vydali standardní cestou, obvykle úlohu úspěšně dokončili a získali tak plný počet bodů. Poté se objevilo poměrně hodně rychlejších a trikovějších řešení, podobných jako ta citovaná, která byla ohodnocena imaginárním bodem. Bohužel se ale objevilo i hodně řešení se závažnou chybou, kterou bylo například tvrzení, že pokud $n^2+k \mid n^2(n+1)$, tak $n^2+k \mid n^2$ nebo $n^2+k \mid n+1$ (které neplatí, jak si můžete rozmyslet). Konečně někteří bohužel dokazovali jinou úlohu, když dosadili $n = k$ a zjistili, že se jedná o celé číslo. Bylo třeba dokázat přesně opačnou implikaci. *(Štěpán Šimsa)*

## Úloha 2. (29; 26; 3,52; 4,0)

*Mějme přirozené číslo $n \geq 2$. Dokažte, že každé z čísel $n!+2, n!+3, \ldots, n!+n$ má takového prvočíselného dělitele, který není dělitelem žádného z $n-2$ zbylých čísel.* *(Josef Svoboda)*

Řešení:
Uvažujme pevné $n$ a číslo $n!+k$. Rozebereme dva případy.

Pokud všechna prvočísla v prvočíselném rozkladu čísla $k$ dělí i některé (ne nutně stále stejné) z ostatních čísel $2, \ldots, k-1, k+1, \ldots, n$, rozložíme zkoumané číslo do tvaru $k(n!/k+1)$. Číslo $(n!/k+1)$ je větší než jedna, uvažujme některého jeho prvočíselného dělitele $p$. Platí $n!/k \equiv -1 \pmod{p}$. Prvočíslo $p$ tak nedělí žádné z čísel $2, \ldots, k-1, k+1, \ldots, n$, nedělí tedy ani $k$, a je proto větší než $n$. Máme tak $p$, které dělí $n!+k$, ale žádné ze zbylých $n-2$ čísel ze zadání, protože nejbližší další čísla dělitelná $p$ jsou $n+k-p$ a $n+k+p$. Je tedy hledaným prvočíslem.

Nyní naopak předpokládejme, že existuje prvočíslo v rozkladu čísla $k$ (označme jej $p$), které žádné z čísel $2, \ldots, k-1, k+1, \ldots, n$ nedělí. To ale znamená, že musí být $p = k$, protože jinak by $p$ bylo v tomto seznamu. Navíc musí platit $2p > n$, protože jinak by v seznamu bylo číslo $2p$. Takže $p$ dělí $(n!+k) = p(n!/p+1)$, ale nedělí žádné ze zbývajících $n-2$ čísel ze zadání, protože nejbližší další dělitelé čísla $p$ jsou $n!$ a $n!+2p$. Je tedy opět hledaným prvočíslem.

Poznámky:
Nejčastější chybou bylo opomenutí druhého případu, opravdu není pravda, že se vždy dá najít prvočíslo větší než $n$, které dělí $n!+k$ – stačí se podívat například na výrazy

$$2!+2, \quad 3!+2, \quad 3!+3, \quad 4!+3, \quad 5!+5.$$

Jeden řešitel ale vznesl hypotézu, že se vždy dá najít prvočíslo větší než $n-2$, to pro účely úlohy stačí. Pokud se vám povede rozhodnout platnost této hypotézy, nebojte se podělit na matematickém chatu na našich stránkách ;-) *(Mirek Olšák)*

## Úloha 3. (24; 21; 3,96; 5,0)

*Mějme celé číslo $n$ a prvočíslo $p$. Víme, že platí*

$$2^{4n} + 9^{2n} \equiv 36^n \pmod{p}.$$

*Dokažte, že $p$ je tvaru $4k + 1$ pro nějaké celé číslo $k$.* *(Josef Svoboda)*

Řešení:
Nejprve snadno vyloučíme možnost, že $p = 2$ nebo $p = 3$. Pro $p = 2$ bychom dostali

$$1 \equiv 2^{4n} + 9^{2n} \equiv 36^n \equiv 0 \pmod{2},$$

což neplatí, obdobně pro $p = 3$ bychom dostali, že 3 dělí $2^{4n}$, což také neplatí.

Pro přehlednost si zavedeme substituci $a = 2^n$, $b = 3^n$, zadání nyní vypadá takto:

$$a^4 + b^4 \equiv (ab)^2 \pmod{p},$$

což můžeme ekvivalentně upravit na

$$(a^2 - b^2)^2 \equiv -(ab)^2 \pmod{p}.$$

Protože jsme vyloučili možnosti $p = 2$ a $p = 3$, číslo $(ab)^2 = 2^{2n} \cdot 3^{2n}$ je nesoudělné s $p$ a můžeme jím tedy kongruenci ekvivalentně vydělit. Dostáváme tedy kongruenci

$$\left(\frac{a^2 - b^2}{ab}\right)^2 \equiv -1 \pmod{p},$$

ze které plyne, že $-1$ je kvadratický zbytek modulo $p$. Jak jsme si v seriálu ukázali (pomocí Eulerova kritéria), z toho už plyne, že $p$ je tvaru $4k + 1$, což jsme chtěli dokázat.

Poznámky:
Velká část řešení postupovala stejně jako vzorové, případně s pěknou obměnou při získávání dvou čtverců – výraz $a^4 - (ab)^2 + b^4$ můžeme vynásobit číslem $a^2 + b^2$ a dostaneme $(a^3)^2 + (b^3)^2$. Nejčastější chybou bylo svévolné přecházení od kongruence modulo $p$ ke kongruenci modulo 4. Bohužel však $a \equiv 0 \pmod{p}$ neimplikuje $a \equiv p \pmod{4}$, jak si snadno ověříte třeba na případu $a = 21$, $p = 3$. *(Pepa Svoboda)*