2. série

Téma: Prvočísla

Datum odeslání: 7. LISTOPADU 2005

1. ÚLOHA (3 BODY)
Dokažte, že každé prvočíslo větší než 5 jde psát ve tvaru $6k + 1$ nebo $6k - 1$, kde k je nějaké přirozené číslo.

2. ÚLOHA (3 BODY)
Mějme libovolné přirozené číslo n, které dává po dělení 3 zbytek 2. Dokažte, že potom existuje prvočíslo p, které dělí n a po dělení 3 dává také zbytek 2.

3. ÚLOHA (3 BODY)
Uvažujme číslo $M(n) = 2^{2^n} - 1$ pro libovolné nezáporné celé číslo n. Zapišme toto číslo jako součin prvočísel, tedy $M(n) = p_1 p_2 \cdots p_k$, kde p_1, p_2, ... , p_k jsou ne nutně různá prvočísla. Dokažte, že $k \geq n$.[1]

4. ÚLOHA (5 BODŮ)
Najděte všechna přirozená čísla n s následující vlastností: je-li p libovolné prvočíslo, $2 < p \leq n$, potom je i číslo $n - p$ prvočíslo.

5. ÚLOHA (5 BODŮ)
Najděte největší prvočíslo p takové, že p^{73} dělí číslo 2005! (symbolem $n!$ značíme faktoriál čísla n, tedy číslo $1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$).

6. ÚLOHA (5 BODŮ)
Buď n jakékoliv přirozené číslo. Dokažte, že číslo $6n - 1$ je prvočíslo právě tehdy, když n nejde psát ve tvaru $n = (6k + 1)l - k$ pro žádná přirozená čísla k a l.

7. ÚLOHA (5 BODŮ)
Mějme libovolné prvočíslo p větší než 5. Dokažte, že délka nejmenší periody čísla $\frac{1}{p}$ (zapsaného v desítkové soustavě) dělí číslo $p - 1$.

8. ÚLOHA (5 BODŮ)
Buď p libovolné prvočíslo a k přirozené číslo splňující $1 \leq k \leq p - 1$. Uvažujme součet

$$S = \sum_I \prod_{i \in I} i,$$

kde sčítáme přes všechny k-prvkové podmnožiny I množiny $\{1, 2, \ldots, p-1\}$.[2]

[1] Pro náročnější: najděte co nejlepší odhad na počet prvočísel k – například pro $6 \leq n \leq 23$ platí, že $k \geq 2n - 5$. (Maximální počet bodů ale získáte i pokud vyřešíte jen první část úlohy.)

[2] Řečeno lidskou řečí, S dostaneme tak, že vezmeme libovolnou podmnožinu I množiny $\{1, 2, \ldots, p-1\}$, vynásobíme všechny její prvky, a nakonec sečteme tyto součiny pro všechny možné podmnožiny I. Například pro $p = 5$ a $k = 2$ jde tedy o součet $S = 1 \cdot 2 + 1 \cdot 3 + 1 \cdot 4 + 2 \cdot 3 + 2 \cdot 4 + 3 \cdot 4$.

V závislosti na p a k určete, jaký zbytek dává S po dělení prvočíslem p.

Řešení 2. série

1. úloha **(100, 95, 2,85, 3,0)**

Dokažte, že každé prvočíslo větší než 5 jde psát ve tvaru $6k+1$ nebo $6k-1$, kde k je nějaké přirozené číslo.

Uvědomme si, že každé celé číslo jde vyjádřit v (právě) jednom z následujících tvarů: $6k$, $6k+1$, $6k+2$, $6k+3$, $6k+4$ nebo $6k+5$. Kdyby $p>5$ bylo prvočíslo tvaru $6k$, $6k+2$ nebo $6k+4$, bylo by dělitelné 2, což není možné. Kdyby bylo tvaru $6k+3$, bylo by dělitelné 3, což také nejde. Musí tedy být buďto $p=6k+1$ nebo $p=6k+5=6(k+1)-1$, což je to, co jsme chtěli dokázat.

Poznámky k došlým řešením: Většina řešitelů vše správně dokázala, a tak získala právem tři body. Za malé nedorazy (například nezdůvodnění, proč $6k$ není prvočíslo) jsme body neubírali. Stejně tak jsme byli hodní na ty, kteří ke správnému důkazu připsali neplatnou větu (nejčastěji obrácenou implikaci). Několik řešitelů uvedlo jen několik prvních prvočísel, pro která vztah platí, a napsali, že podobně to bude i pro prvočísla vyšší. Za nedostatečné zdůvodnění jsme nemohli udělit žádný bod.

2. úloha **(83, 59, 2,27, 3,0)**

Mějme libovolné přirozené číslo n, které dává po dělení 3 zbytek 2. Dokažte, že potom existuje prvočíslo p, které dělí n a po dělení 3 dává také zbytek 2.

Každé přirozené číslo $n>1$ jde jednoznačně rozložit na součin prvočísel (protože n dává po dělení 3 zbytek 2, je skutečně $n>1$). Kdyby n nebylo dělitelné žádným prvočíslem, které po dělení 3 dává také zbytek 2, dávala by všechna prvočísla v rozkladu n zbytek 1 po dělení 3 (dělitelná 3 být nemohou, pak by totiž bylo i n dělitelné 3). Mohli bychom tedy psát

$$n=(3k_1+1)(3k_2+1)\cdots(3k_l+1),$$

kde $3k_i+1$ jsou uvažovaná prvočísla. Jak ale snadno ověříš roznásobením, součin dvou čísel tvaru $3k+1$ je opět téhož tvaru, takže postupně roznásobováním (a formálně bychom to mohli dokázat třeba matematickou indukcí) dostaneme, že i číslo n je tvaru $3k+1$. To je ale spor s předpoklady úlohy.

3. úloha **(66, 51, 2,32, 3,0)**

Uvažujme číslo $M(n)=2^{2^n}-1$ pro libovolné nezáporné celé číslo n. Zapišme toto číslo jako součin prvočísel, tedy $M(n)=p_1p_2\cdots p_k$, kde p_1, p_2, …, p_k jsou ne nutně různá prvočísla. Dokažte, že $k\geq n$.[3]

[3]Pro náročnější: najděte co nejlepší odhad na počet prvočísel k – například pro $6\leq n\leq 23$ platí, že $k\geq 2n-5$. (Maximální počet bodů ale získáte i pokud vyřešíte jen první část úlohy.)

Dokazujme matematickou indukcí:

(1) Je-li $n = 1$, je $M(n) = 3 = p_1$, takže vskutku je počet prvočísel $1 = k \geq n = 1$.

(2) Předpokládejme, že $M(n-1) = p_1 p_2 \cdots p_k$, kde (podle indukčního předpokladu) platí $k \geq n-1$ Všimněme si, že

$$M(n) = 2^{2^n} - 1 = \left(2^{2^{n-1}}\right)^2 - 1 = \left(2^{2^{n-1}} - 1\right)\left(2^{2^{n-1}} + 1\right) = M(n-1)\left(2^{2^{n-1}} + 1\right).$$

Číslo $2^{2^{n-1}} + 1$ můžeme psát ve tvaru součinu prvočísel jako $2^{2^{n-1}} + 1 = p_{k+1} p_{k+2} \cdots p_{k+l}$, kde $l \geq 1$, takže $M(n) = M(n-1)\left(2^{2^{n-1}} + 1\right) = p_1 p_2 \cdots p_k \cdot p_{k+1} p_{k+2} \cdots p_{k+l}$; počet prvočísel v rozkladu je $k + l \geq (n-1) + 1 = n$, čímž jsme dokázali i indukční krok.

4. úloha **(79, 54, 2,67, 3,0)**

Najděte všechna přirozená čísla n s následující vlastností: je-li p libovolné prvočíslo, $2 < p \leq n$, potom je i číslo $n - p$ prvočíslo.

Volby $n = 1$, 2 snadno vyhoví zadání, jelikož neexistuje prvočíslo p takové, že $2 < p \leq n$. Naopak $n = 3$, 4, 9 zadání nesplňují kvůli volbě $p = 3$; $n = 5, 6$ nesplňují kvůli volbě $p = 5$ a $n = 7$, 8 kvůli volbě $p = 7$. Snadno se ověří, že $n = 10$ má požadovanou vlastnost. Dokážeme, že už žádná jiná n požadovanou vlastnost nemají. Čísla 3, 5, 7 dávají různé zbytky při dělení třemi, tudíž pro $n \geq 11$ je alespoň jedno z čísel $n-3$, $n-5$, $n-7$ složené (je dělitelné třemi a větší než tři).

Zadání tedy splňují volby $n = 1$, 2, 10.

Poznámky k došlým řešením: Nejčastější chybou bylo i u zkušených řešitelů to, že zapomínali na čísla 1 a 2. Zadání úlohy je nevylučuje! Je tam pouze řečeno, že $(n - p)$ má být prvočíslo pro všechna prvočísla $p > 2$ a zároveň $p \leq n$. Většina úspěšných řešitelů využila počítání modulo 3, což bylo nejjednodušší, někteří modulo 5 či modulo jiné prvočíslo, i to bylo naprosto korektní. Bohužel někteří stále považují za prvočíslo 1 nebo dokonce i 0! Z toho vznikala chybná uvádění čísel 4, 6, 8 nebo 5 mezi vyhovujícími přirozenými čísly.

5. úloha **(89, 80, 4,00, 5,0)**

Najděte největší prvočíslo p takové, že p^{73} dělí číslo 2005! (symbolem $n!$ značíme faktoriál čísla n, tedy číslo $1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$).

Nejprve si připomeňme tento známý fakt: Největší číslo k takové, že číslo p^k dělí $n!$, je

$$k = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Proč tomu tak je? Mezi čísly $1, 2, \ldots, n$ je právě $\left\lfloor \frac{n}{p} \right\rfloor$ čísel dělitelných p (jsou to čísla $p, 2p, \ldots, \left\lfloor \frac{n}{p} \right\rfloor p$). Každé z nich přispěje k exponentu k jedničkou. Některá z nich jsou ale dokonce dělitelná p^2. Těch je $\left\lfloor \frac{n}{p^2} \right\rfloor$ a ke k přispějí aspoň 2. Jednou už byla započítána v číslech dělitelných p, stačí je tedy připočíst jen jednou. Obdobně když budeme uvažovat čísla dělitelná vyššími mocninami p, dostaneme i další členy uvedeného součtu.

Ještě si uvědomme, že ač je tento součet psaný jako nekonečný, stačí uvažovat jen konečně mnoho jeho členů. Je-li totiž $p^i > n$, je $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$, takže takovéto členy v součtu nehrají žádnou roli.

A nyní hurá na řešení úlohy! Snadno spočteme, že pro $p = 23$ je odpovídající $k = \left\lfloor \frac{2005}{23} \right\rfloor + \left\lfloor \frac{2005}{23^2} \right\rfloor + \left\lfloor \frac{2005}{23^3} \right\rfloor + \cdots = 87 + 3 + 0 + 0 + \cdots = 90 > 73$. My ale máme najít největší takové p, takže co kdyby pro nějaké větší p bylo 2005! dělitelné také číslem p^{73}? Pak musí být $p \geq 29$, a tedy

$$k = \sum_{i=1}^{\infty} \left\lfloor \frac{2005}{p^i} \right\rfloor \leq \sum_{i=1}^{\infty} \left\lfloor \frac{2005}{29^i} \right\rfloor = \left\lfloor \frac{2005}{29} \right\rfloor + \left\lfloor \frac{2005}{29^2} \right\rfloor + \left\lfloor \frac{2005}{29^3} \right\rfloor + \cdots = 69+2+0+0+\cdots = 71 < 73.$$

Žádné $p > 23$ tedy podmínkám úlohy nevyhovuje, takže $p = 23$ je hledané největší číslo.

6. úloha **(48, 43, 3, 31, 3, 5)**

Buď n jakékoliv přirozené číslo. Dokažte, že číslo $6n - 1$ je prvočíslo právě tehdy, když n nejde psát ve tvaru $n = (6k + 1)l - k$ pro žádná přirozená čísla k a l.

Máme dokázat ekvivalenci, dokažme tedy postupně dvě implikace:

„⇒“ Předpokládejme, že $6n - 1$ je prvočíslo a přitom existují přirozená čísla k a l taková, že $n = (6k + 1)l - k$. Potom $6n - 1 = 6((6k + 1)l - k) - 1 = 36kl + 6l - 6k - 1 = (6k + 1)(6l - 1)$, což je spor s tím, že $6n - 1$ je prvočíslo.

„⇐“ Předpokládejme, že n nejde psát ve tvaru $n = (6k + 1)l - k$ pro žádná přirozená čísla k a l a přitom $p = 6n - 1$ není prvočíslo. Pak ale má p vlastního dělitele tvaru $6l - 1$ (stačí použít obdobnou úvahu jako v řešení 2. úlohy), a můžeme je tedy psát jako $p = (6l - 1)m$. Číslo p je nesoudělné s 6, takže i m je nesoudělné s 6, a tedy je m tvaru $6k - 1$, nebo $6k + 1$.

Kdyby bylo $m = 6k - 1$, tak $p = (6l - 1)(6k - 1) = 36kl - 6l - 6k + 1 = 6(6kl - k - l) + 1 \neq \neq 6n - 1 = p$ (p má dávat po dělení 6 zbytek 5, ne 1).

Nastane tedy druhý případ a $m = 6k + 1$. Pak $p = (6l - 1)(6k + 1) = 36kl + 6l - 6k - 1 = = 6(6kl - k + l) - 1 = 6n - 1$, takže $n = 6kl - k + l = (6k + 1)l - k$. Ale to je spor s předpokladem, že se takto n psát nedá!

7. úloha **(31, 23, 3, 23, 5, 0)**

Mějme libovolné prvočíslo p větší než 5. Dokažte, že délka nejmenší periody čísla $\frac{1}{p}$ (zapsaného v desítkové soustavě) dělí číslo $p - 1$.

Předpokládejme, že nejkratší perioda desetinného zápisu vypadá jako $x = \overline{\alpha_1\alpha_2\ldots\alpha_m}$ (ta čára nahoře značí desítkový zápis – nejde o násobení čísel α_i).

Potom pro vhodná k, z (obojí přirozená, k je větší nebo rovno počtu číslic čísla z) platí:

$$\frac{1}{p} = 10^{-k} \cdot z + 10^{-k-m} \cdot x + 10^{-k-2m} \cdot x + \ldots$$

Můžeme použít vzorec pro součet geometrické řady a dostaneme:

$$\frac{1}{p} = 10^{-k} \cdot z + 10^{-k-m} \cdot x \frac{1}{1 - 10^{-m}} = 10^{-k} \cdot z + 10^{-k} \frac{x}{10^m - 1}$$

$$\frac{10^k}{p} = z + \frac{x}{10^m - 1}$$

Kdyby bylo x dělitelné $10^m - 1$, tak $x = (10^m - 1) \cdot c$ (kde $c \in \mathbb{N}_0$) a máme $\frac{10^k}{p} = z + c \in \mathbb{N}_0$, tedy $p|10^k$. Protože ale $p > 5$, je p zjevně nesoudělné s desítkou, a proto nemůže dělit žádnou její mocninu. Tedy $10^m - 1$ nedělí x.

Jednoduchou úpravou dostáváme:

$$10^k - z \cdot p = \frac{xp}{10^m - 1}.$$

Výraz na levé straně je celé číslo, takže musí být $10^m - 1|xp$. Přitom $10^m - 1 \nmid x$, takže čísla p a $10^m - 1$ musí být soudělná. Protože p je prvočíslo a $10^m - 1 > 1$, může to nastat jenom tak, že $p|10^m - 1$.

Naopak, pokud pro nějaké $m \in \mathbb{N}$ platí, že $p|10^m - 1$, položíme $x = \frac{10^m - 1}{p} < 10^m$ a máme:

$$\begin{aligned} 1 &= \frac{xp}{10^m - 1} \\ \frac{1}{p} &= \frac{x}{10^m - 1} = \frac{x10^{-m}}{1 - 10^{-m}} \\ \frac{1}{p} &= 10^{-m} x \frac{1}{1 - 10^{-m}} = 10^{-m} x + 10^{-2m} x + \ldots, \end{aligned}$$

takže $\frac{1}{p} = \overline{\alpha_1 \alpha_2 \ldots \alpha_m \alpha_1 \alpha_2 \ldots}$ a jsme hotovi.

Tedy nejkratší délka periody $\frac{1}{p}$ je právě nejmenší přirozené číslo m takové, že $p|10^m - 1$. Teď nám stačí použít známé tvrzení:

Věta. (Malá Fermatova) Pokud p je prvočíslo, a je nesoudělné s p, tak platí $p|a^{p-1} - 1$.

Důkaz[4] této věty je možno provádět například elementárně z binomické věty indukcí podle a.

Zjevně desítka není soudělná s p, takže $p|10^{p-1} - 1$. Nechť nyní pro spor délka nejmenší periody[5] m nedělí $p - 1$. Potom jistě $m < p - 1$ (víme, že $p - 1$ je perioda). Vydělením čísla $p - 1$ číslem m se zbytkem dostaneme: $p - 1 = m \cdot l + q$, kde $0 < q < m$ je přirozené. Ukážeme, že $p|10^q - 1$, což bude spor s minimalitou m. Víme, že:

$$10^{p-1} - 1 = 10^{m \cdot l + q} - 1 = 10^q \left(10^{m \cdot l} - 1 + 1\right) - 1 = 10^q - 1 + (10^{m \cdot l} - 1) \cdot 10^q.$$

Přitom $p|10^m - 1$ a snadno (třeba indukcí) nahlédneme, že potom také $p|10^{ml} - 1$ pro každé $l \in \mathbb{N}_0$, takže $p|(10^{m \cdot l} - 1) \cdot 10^q$. Proto můžeme psát:

$$p|10^{p-1} \Rightarrow p|10^q - 1 + (10^{m \cdot l} - 1) \cdot 10^q \Rightarrow p|10^q - 1,$$

což je kýžený spor s tím, že m je nejmenší perioda. Tím jsme tvrzení dokázali.

Poznámky k došlým řešením: Skoro všichni řešitelé, kteří v úloze použili Malou Fermatovu větu, tuto úlohu nakonec i úspěšně dořešili. Naopak, skoro všichni řešitelé, kteří si její použití odpustili,

[4] Hezčí důkaz najdeš spolu s dalšími poznatky třeba v seriálu o teorii čísel ze 17. ročníku Prasete v našem archivu na `http://mks.mff.cuni.cz/archive/archive.php`.

[5] Uvědom si, že takto můžeme postupovat jenom proto, že víme, že nějaká nejmenší délka periody vůbec existuje (třeba mezi čísly z intervalu $(0; 1)$ neexistuje nejmenší číslo).

nakonec tuto úlohu stejně nezvládli. Na tomto místě bych vyzvedl Víta Jakimiva a Rastislava Oľhavu, kteří byli světlými výjimkami bezfermatovců a vysloužili si almužničku v podobě i.

Jinak stojí za zmínku, že spousta řešitelů jakoby vycházela z toho, co se má dokázat. Tak to, milí řešitelé, opravdu nefunguje! I když nám to při řešení může pomoct, je potřeba úlohu řešit způsobem, že všechna čísla dělitelná čtyřmi jsou sudá, a ne, že sudá čísla jsou dělitelná čtyřmi.

8. úloha **(12, 5, 1,75, 0,0)**

Buď p libovolné prvočíslo a k přirozené číslo splňující $1 \leq k \leq p-1$. Uvažujme součet

$$S = \sum_{I} \prod_{i \in I} i,$$

kde sčítáme přes všechny k-prvkové podmnožiny I množiny $\{1, 2, \ldots, p-1\}$.[6]

V závislosti na p a k určete, jaký zbytek dává S po dělení prvočíslem p.

Označme $\mathbb{Z}_p$ množinu $\{0, 1, \ldots, p-1\}$ společně se sčítáním a násobením modulo p (tj. po provedení příslušné operace vezmeme zbytek výsledku po vydělení p). $\mathbb{Z}_p$ je takzvané těleso, nejdůležitější vlastností je, že pro každé $a \in \mathbb{Z}_p$, $a \neq 0$ existuje a' takové, že $a \cdot a' \equiv 1 \pmod{p}$. Takové a' se obvykle značí a^{-1}. Mějme polynom

$$P(x) = x^{p-1} - 1$$

s koeficienty v $\mathbb{Z}_p$. Podle malé Fermatovy věty je $a^{p-1} \equiv 1 \pmod{p}$ pro $a \in \mathbb{Z}_p$, $a \neq 0$, tudíž takové a je kořenem polynomu P. V tělesech je jednoznačná faktorizace polynomů, odkud plyne, že:

$$P(x) = (x-1)(x-2)\cdots(x-(p-1)))$$

v $\mathbb{Z}_p$.

Označme S_k výraz ze zadání pro pevně dané k. Potom z Viètových vztahů dostáváme, že:

$$P(x) = x^{p-1} - S_1 x^{p-2} + S_2 x^{p-3} - \cdots + (-1)^{p-1} S_{p-1}.$$

Odtud porovnáním koeficientů v definici $P(x)$ a v novém vyjádření dostáváme, že $S_k \equiv 0 \pmod{p}$ pro $k < p-1$ a dále $S_{p-1} \equiv -1 \pmod{p}$ (rozliší se případy $p = 2$ a p liché).

[6] Řečeno lidskou řečí, S dostaneme tak, že vezmeme libovolnou podmnožinu I množiny $\{1, 2, \ldots, p-1\}$, vynásobíme všechny její prvky, a nakonec sečteme tyto součiny pro všechny možné podmnožiny I. Například pro $p = 5$ a $k = 2$ jde tedy o součet $S = 1{\cdot}2 + 1{\cdot}3 + 1{\cdot}4 + 2{\cdot}3 + 2{\cdot}4 + 3{\cdot}4$.