Prvočísla

2. PODZIMNÍ SÉRIE — TERMÍN ODESLÁNÍ: 7. LISTOPADU 2016

Číslem rozumíme vždy celé číslo větší než nula. Prvočíslo je číslo větší než jedna, které je dělitelné jen jedničkou a sebou samým. Číslo nazveme složeným, pokud je větší než jedna a není to prvočíslo.

ÚLOHA 1. (3 BODY)
Čarodějnice Marta si povšimla, že se jí na zahrádce přemnožila prvočísla. Vyslovila tedy složité zaklínadlo a co se nestalo: Nejprve se vypařila všechna prvočísla a na zahrádce je nahradily součty každých dvou z nich, načež všechna složená čísla odletěla pryč. Dokažte, že po dvou provedeních zaklínadla se Marta všech prvočísel zbavila.

ÚLOHA 2. (3 BODY)
Nalezněte všechna prvočísla, která **nelze** zapsat jako součet dvou složených čísel.

ÚLOHA 3. (3 BODY)
Když se Marian vrátil ze svých cest, chlubil se kamarádům: „Dojel jsem až k jezeru, na jehož obvodu leželo 1001 měst. Přitom poměr počtu obyvatel každých dvou sousedních měst (větší ku menšímu) byl přirozené číslo a navíc prvočíslo.“ „To kecáš“, podivila se Áďa. Dokažte, že měla pravdu.

ÚLOHA 4. (5 BODŮ)
Rozhodněte, zda pro každých šest po sobě jdoucích čísel existuje prvočíslo, které dělí právě jedno z těchto čísel.

ÚLOHA 5. (5 BODŮ)
Číslo n má tu vlastnost, že $2n+1$ i $3n+1$ jsou druhé mocniny přirozených čísel. Ukažte, že $5n+3$ není prvočíslo.

ÚLOHA 6. (5 BODŮ)
David má n hrušek a Martin s Tondou mu je střídavě ujídají. Martin začíná a ten, kdo je na řadě, si vybere nějaké prvočíslo p a sní $p-1$ hrušek. Oba loupežníci se snaží sníst poslední hrušku. Dokažte, že pro nekonečně mnoho n toho může dosáhnout Tonda, ať se mu v tom Martin snaží sebevíc zabránit.

ÚLOHA 7. (5 BODŮ)
Nalezněte všechny 2016-tice ne nutně různých přirozených čísel, pro které platí, že kdykoli z nich vybereme[1] čtveřici (a,b,c,d), tak splňuje $abcd \mid a^4+b^4+c^4+d^4$.

ÚLOHA 8. (5 BODŮ)
Nechť $p(n)$ je nejvyšší prvočíselný dělitel čísla $n>1$. Ukažte, že existuje nekonečně mnoho čísel $n>2$, pro která platí $p(n-1)<p(n)<p(n+1)$.

[1] Jedno číslo můžeme vybrat jen tolikrát, kolikrát se vyskytuje v naší 2016-tici.

Prvočísla

2. PODZIMNÍ SÉRIE — VZOROVÉ ŘEŠENÍ

Úloha 1.

Čarodějnice Marta si povšimla, že se jí na zahrádce přemnožila prvočísla. Vyslovila tedy složité zaklínadlo a co se nestalo: Nejprve se vypařila všechna prvočísla a na zahrádce je nahradily součty každých dvou z nich, načež všechna složená čísla odletěla pryč. Dokažte, že po dvou provedeních zaklínadla se Marta všech prvočísel zbavila.

(Martin „E.T.“ Sýkora)

ŘEŠENÍ:

Součet dvou prvočísel je určitě větší než dva. Mezi součty vzniklými po prvním vyslovení zaklínadla proto dvojka není. Poté, co zmizí složená čísla, zůstanou na zahrádce pouze prvočísla, která jsou všechna větší než dva a jsou tedy určitě všechna lichá. Po druhém vyslovení zaklínadla dostáváme pouze součty dvou lichých prvočísel, tedy čísla sudá a větší než dva. Ta jsou složená a musí zmizet. Marta se tak po dvou provedeních zaklínadla zbaví všech prvočísel na své zahrádce.

POZNÁMKY:

Úloha byla dost lehká, což mnohé řešitele svádělo k nepřesnostem. Celkem oblíbené tvrzení bylo, že součet dvou lichých čísel je číslo sudé, a tedy složené. Bylo jasné, že dvojka nám vzniknout nemůže, ale málokdo to i napsal do řešení. Pár řešitelů si zadání vysvětlilo tak, že prvočísla sčítáme po dvojicích a ne každé s každým, nicméně pokud se v jejich řešení i tak objevily všechny myšlenky potřebné na vyřešení původní úlohy, body jsem neodečítala. *(Karolína Kuchyňová)*

Úloha 2.

Nalezněte všechna prvočísla, která **nelze** *zapsat jako součet dvou složených čísel.*

(Anh Dung „Tonda“ Le)

ŘEŠENÍ:

Nejprve si uvědomme, že všechna sudá čísla větší než dva jsou složená, a tudíž i všechna prvočísla větší než dva jsou lichá. Číslo dva zjevně nelze zapsat jako součet dvou složených čísel (nejmenší složené číslo je čtyři). Dále tedy všechna prvočísla, která nám zbývá vyřešit, jsou lichá.

Jelikož liché číslo lze zapsat pouze jako součet sudého a lichého čísla, všechna prvočísla menší než součet nejmenšího sudého složeného čísla a nejmenšího lichého složeného čísla (tj. čtyři a devět) takto zapsat nelze. Ovšem každé prvočíslo $p \geq 13$ lze zapsat jako $p = 9 + (p - 9)$, kde devět je složené číslo a $p - 9$ je sudé číslo větší než dva, tudíž rovněž složené. Proto žádné takové prvočíslo nebude hledaným řešením.

Řešeními jsou tedy právě ta prvočísla, která jsou ostře menší než 13, tj. 2, 3, 5, 7 a 11.

POZNÁMKY:

Úloha byla poměrně snadná a šlo ji vyřešit mnoha různými způsoby lišícími se především v postupu nalezení rozkladu pro prvočíslo $p \geq 13$. Nejoblíbenější a nejkratší variantou byl rozklad uvedený ve vzorovém řešení. Častý byl také rozklad založený na rozboru možných zbytků po dělení p třemi

(konkrétně pro zbytek jedna rozklad $p = 4 + (p - 4)$ a pro zbytek dva rozklad $8 + (p - 8)$, kde druhý člen součtu je složené číslo dělitelné třemi) či na rozboru podle poslední číslice prvočísla p.

Bohužel kromě mnoha správných řešení přišlo i několik takových, která bez důkazu tvrdila, že žádné další řešení neexistuje, nebo se dokonce o neexistenci dalšího řešení vůbec nezmiňovala (extrémním případem bylo řešení se zapsaným výsledkem bez jediného slova). Takovým řešením jsem musel dát pouze bod, neboť pokud úloha požaduje nalezení **všech** řešení, je třeba dokázat, že jste skutečně všechna nalezli. *(Tomáš Novotný)*

Úloha 3.

Když se Marian vrátil ze svých cest, chlubil se kamarádům: „Dojel jsem až k jezeru, na jehož obvodu leželo 1001 *měst. Přitom poměr počtu obyvatel každých dvou sousedních měst (větší ku menšímu) byl přirozené číslo a navíc prvočíslo.“ „To kecáš“, podivila se Áďa. Dokažte, že měla pravdu.*

(Anh Dung „Tonda“ Le)

Řešení:

Uvažujme dvě sousední města a o_1, o_2 počty obyvatel těchto dvou měst. Fakt, že poměr většího ku menšímu z těchto čísel je prvočíslo, říká, že součty exponentů v prvočíselných zápisech o_1 a o_2 se liší o jedna.

Úlohu dokážeme sporem. Nechť platí to, co řekl Marian. Zvolme libovolné město u jezera. Bez újmy na obecnosti, nechť součet exponentů v jeho prvočíselném rozkladu je sudý (pokud je lichý, vezmeme vedlejší město). Obejdeme-li po kruhu všechna města, vrátíme se do původního po navštívení 1000 dalších měst. Potom z úvahy na začátku je součet exponentů v jeho prvočíselném rozkladu lichý (1001krát se změní parita). To je ovšem spor s předpokladem, že tento součet je sudý.

Poznámky:

Většina řešení myšlenkou odpovídala vzorovému. Co se týče nejčastějších chyb, našlo se několik řešení, která předpokládala, že se po kruhu musí střídat dva počty obyvatel nebo počet obyvatel musí (při pohybu jedním směrem) růst. Tento předpoklad ovšem nezahrnuje všechny možnosti. Například pokud by kolem jezera byla čtyři města, čtveřice 30, 150, 30, 60 splňuje podmínky zadání (krom faktu, že počet měst není roven 1001), ale nestřídají se v ní dvě různá čísla a také netvoří rostoucí posloupnost čísel.

Často jsem v řešeních narazil na to, že se pracuje s očíslovanými městy, aniž by bylo řečeno, jak očíslování má vypadat. Člověk si domyslí, že očíslování bude fungovat tak, že jedno z měst bude první a zbytek měst se postupně očísluje buď po směru nebo proti směru hodinových ručiček, ale je třeba to alespoň trochu popsat. Stejně tak se objevovaly snahy mluvit o „sudých“ a „lichých“ městech, kde je problém úplně stejný, protože jedno město může být (podle zvoleného očíslování) sudé nebo liché. *(Honza Krejčí)*

Úloha 4.

Rozhodněte, zda pro každých šest po sobě jdoucích čísel existuje prvočíslo, které dělí právě jedno z těchto čísel.

(David Hruška)

Řešení:

Je zřejmé, že z každých šesti po sobě jdoucích čísel jsou právě tři lichá. Dále dokážeme sporem, že z těchto tří lichých čísel je maximálně jedno dělitelné třemi. Předpokládejme, že jsou dvě z nich dělitelná třemi. Pak je jejich rozdíl také dělitelný třemi a jelikož jsou obě lichá, tak jejich rozdíl je sudý. Tento rozdíl je tedy dělitelný šesti a jelikož jde o různá čísla, tak se musí lišit alespoň o šest. Pak ale nemohou být obě v šestici po sobě jdoucích čísel.

Analogicky dokážeme, že maximálně jedno z těchto tří lichých čísel je dělitelné pěti. Maximálně dvě z nich jsou proto dělitelná třemi nebo pěti, tedy v každých šesti po sobě jdoucích číslech existuje číslo, které není dělitelné dvěma, třemi ani pěti. Toto číslo je buďto rovno jedné, nebo má ve svém prvočíselném rozkladu prvočíslo větší nebo rovno sedmi (pro všechna čísla větší než jedna existuje prvočíselný rozklad). Nejprve vyřešíme první případ. Číslo jedna je obsaženo jen v šestici čísel 1, 2, 3, 4, 5, 6. Pro tuto šestici je číslo pět prvočíslem, které dělí právě jedno z čísel v ní. Ve druhém případě toto prvočíslo nemůže dělit žádné další číslo ze šestice, jelikož rozdíl každých dvou jeho násobků je větší nebo roven sedmi.

Tedy pro každých šest po sobě jdoucích čísel existuje prvočíslo, které dělí právě jedno z nich.

Poznámky:
Většina došlých řešení byla správná. Několik řešitelů bohužel špatně pochopilo zadání a hledalo prvočíslo, které by dělilo právě jedno číslo z každých šesti po sobě jdoucích čísel (takové však neexistuje). Dále bylo potřeba dát si pozor na číslo jedna, které nemá žádné prvočíselné dělitele.

(Lucien Šíma)

Úloha 5.

Číslo n má tu vlastnost, že $2n+1$ i $3n+1$ jsou druhé mocniny přirozených čísel. Ukažte, že $5n+3$ není prvočíslo.

(Rado Švarc)

Řešení:
Označme a, b přirozená čísla, pro která platí $a^2 = 2n+1$ a $b^2 = 3n+1$. Pak

$$5n+3 = 4(2n+1) - (3n+1) = 4a^2 - b^2 = (2a-b)(2a+b).$$

Tedy jsme vyjádřili $5n+3$ jako součin dvou přirozených čísel. Abychom dokázali, že $5n+3$ není prvočíslo, zbývá ukázat, že $2a-b$ a $2a+b$ nejsou rovna jedné. Číslo $2a+b$ je určitě různé od jedné, protože a a b jsou přirozená.

Předpokládejme pro spor, že $2a-b=1$. Pak $5n+3 = (2a-b)(2a+b) = 1(b+1+b) = 2b+1$, tedy $5n+2 = 2b$. Odtud a z definice b dostáváme $\left(\frac{5n+2}{2}\right)^2 = b^2 = 3n+1$. To upravíme na $25n^2+20n+4 = 12n+4$, tedy $n(25n+8)=0$. Poslední uvedená rovnost je ve sporu s tím, že n je celé číslo větší než nula. Proto ani $2a-b$ není rovno jedné, tudíž $5n+3$ není prvočíslo.

Poznámky:
Někteří řešitelé odhalili nejmenší přirozené číslo vyhovující zadání, tím je $n=40$. Je ale třeba uvědomit si, že nalezení jednoho čísla, které splňuje zadané vlastnosti, není požadovaným důkazem daného tvrzení. Důkaz je samozřejmě třeba provést **pro všechna** přípustná n.

(Míša Hubatová)

Úloha 6.

David má n hrušek a Martin s Tondou mu je střídavě ujídají. Martin začíná a ten, kdo je na řadě, si vybere nějaké prvočíslo p a sní $p-1$ hrušek. Oba loupežníci se snaží sníst poslední hrušku. Dokažte, že pro nekonečně mnoho n toho může dosáhnout Tonda, ať se mu v tom Martin snaží sebevíc zabránit.

(David Hruška)

Řešení:
Hra je určitě konečná (hráči zřejmě hrušky někdy dojí, vždy musí sníst alespoň jednu). Definujme pozici, ve které se hra nachází, jako počet zbývajících hrušek. Můžeme si tedy jednotlivé pozice rozdělit do dvou skupin. Pozice n je *vyhrávající*, jestliže hráč, který je na tahu na pozici n, má vyhrávající strategii (tedy umí určitě vyhrát nezávisle na tazích protihráče). Naopak n označíme

jako *prohrávající*, pokud hráč nacházející se na tahu nemá při správné hře druhého hráče šanci na vítězství. Platí, že můžeme-li z pozice n přípustným tahem přejít na nějakou prohrávající pozici, pak je pozice výherní. Naopak, pokud z nějakého n neexistuje žádný přípustný tah do prohrávající pozice, je toto n pozice prohrávající. Pozici 0 definujeme jako triviální prohrávající pozici – hráč, před kterým je nula hrušek, je ten, který právě sledoval, jak je ten druhý dojedl – tedy prohrávající.

Chceme dokázat, že existuje nekonečně mnoho prohrávajících pozic (to jsou přesně ty, ve kterých vyhraje Tonda, protože Martin začíná). Není těžké si všimnout, že pozice 3 je prohrávající, stejně jako např. 8 a 11. Předpokládejme, že prohrávajících pozic je jen konečně mnoho. Potom zřejmě existuje nějaká nejvyšší z nich, označme si ji třeba x. Všechny vyšší pozice než x jsou z tohoto předpokladu vyhrávající.

Nyní zkoumejme pozici $(x+2)! + (x+1)$. Je to zřejmě větší hodnota než x, měla by tedy být vyhrávající, tj. měl by z ní existovat tah do jedné z prohrávajících pozic. Prohrávající pozice jsou některá čísla z čísel $0, 1, 2, \ldots, x$. Rozdíl $(x+2)! + (x+1)$ a některého z těchto čísel tedy nutně musí být roven $p-1$ pro nějaké prvočíslo p. Pro nějaké i od 0 do x tedy máme

$$(x+2)! + (x+1) - i = p - 1.$$

To se dá upravit na

$$(x+2)! + (x+2) - i = p.$$

Pro každé i z určeného intervalu se bude rozdíl $(x+2) - i$ nacházet v rozmezí od 2 do $(x+2)$ a tímto číslem bude dělitelné i $(x+2)!$, které je větší než $(x+2)$. Po vytknutí tedy na levé straně dostaneme součin dvou čísel větších než jedna, což se nikdy nemůže rovnat prvočíslu.

Dostali jsme spor, a prohrávajících pozic tedy nemůže být konečně mnoho. Existuje tedy nekonečně mnoho pozic, pro které Tonda vyhraje nezávisle na Martinových tazích!

Poznámky:
Ten, kdo dokazoval sporem, tj. vybral nějaké nejvyšší prohrávající n, úlohu zpravidla vyřešil. Konstrukcí pro nalezení sporu v podobě „ještě větší“ prohrávající pozice bylo více, ve vzoráku je popsaná ta nejčastější. Někteří řešitelé si mysleli, že pokud má hráč na tahu před sebou n hrušek a nemůže je všechny sníst (aneb $n \neq p-1$), pak „nevyhraje“. To, že hráč zrovna nemůže sníst všechny hrušky najednou, ještě neznamená, že nemůže udělat takovou sekvenci tahů, aby toho po nějaké době skutečně dosáhl.

(Marian Poljak)

Úloha 7.

Nalezněte všechny 2016*-tice ne nutně různých přirozených čísel, pro které platí, že kdykoli z nich vybereme*[1] *čtveřici* (a, b, c, d)*, tak splňuje* $abcd \mid a^4 + b^4 + c^4 + d^4$.

(David Hruška)

Řešení:
Nejdříve vypozorujeme, že kdyby byla všechna čísla 2016-tice dělitelná nějakým číslem větším než jedna, pak tímto dělitelem můžeme každé z čísel vydělit a na platnosti tvrzení nic nezměníme. Uvažujme tedy nyní jenom 2016-tice čísel, která nejsou všechna dělitelná číslem větším než jedna. Jistě si hned všimneme, že všechny jedničky vyhovují zadání.

Dále mějme nějakou 2016-tici splňující zadání a předpokládejme, že v ní existuje nějaké číslo větší než jedna, označme jej a. Potom je toto číslo a zřejmě dělitelné nějakým prvočíslem p. Nyní pro spor předpokládejme, že v 2016-tici existují nějaká dvě čísla x, y, jejichž čtvrté mocniny nedávají stejný zbytek modulo p. Potom můžeme vzít nějaká b, c ze zbývajících 2013 čísel (tedy všech různých od a, x, y).

$$p \mid abcx \mid a^4 + b^4 + c^4 + x^4$$

[1] Jedno číslo můžeme vybrat jen tolikrát, kolikrát se vyskytuje v naší 2016-tici.

$$p \mid abcy \mid a^4 + b^4 + c^4 + y^4$$

Odečtením dělitelností od sebe dostaneme $p \mid x^4 - y^4$, což je spor s tím, že čtvrté mocniny čísel x, y dávají různý zbytek modulo p. Čtvrté mocniny všech čísel kromě a tedy musí nutně být kongruentní modulo p. Označme jejich společný zbytek po dělení p písmenkem z. Nyní uvažujme obecnou čtveřici s číslem a:

$$p \mid abcd \mid a^4 + b^4 + c^4 + d^4$$

Všechny hodnoty z pravé strany dělitelnosti můžeme ekvivalentně nahradit jejich zbytkem po dělení p, dostáváme tedy (a je z předpokladu dělitelné p):

$$p \mid 0 + z + z + z = 3z$$

Jelikož je p z předpokladu prvočíslo, dostáváme dvě možnosti:

(1) $p \mid z$. Potom p dělí čtvrté mocniny všech čísel, musí tedy nutně dělit všechna čísla – tady se dostáváme do sporu s naším předpokladem, že 2016-tice čísel nemá mít žádného dělitele většího než jedna společného všem.

(2) $p \nmid z \implies p \mid 3$. Potom je trojka nutně jediným prvočíslem, které může dělit nějaký prvek naší 2016-tice. Námi vybrané číslo a je přitom jediné číslo, které může být touto trojkou dělitelné. Kdyby totiž bylo ještě nějaké jiné číslo než a dělitelné třemi, tak jeho čtvrtá mocnina dává zbytek nula po dělení třemi – všechna čísla mimo a ale mají tento zbytek společný, dostaneme tedy 2016-tici čísel, z nichž každé je dělitelné třemi, což je opět spor se stejným předpokladem. Všechna čísla různá od a tedy mohou být jedině jedničky, zato a musí nutně být mocnina trojky.

Již víme, že je-li a nultá mocnina trojky, tak získáme řešení tvořené 2016 jedničkami. Je-li první mocnina trojky, dostaneme taky vyhovující řešení, protože $3 = 3 \cdot 1 \cdot 1 \cdot 1 \mid 3^4 + 1^4 + 1^4 + 1^4 = 84$. Je-li a vyšší mocninou trojky, pak je dělitelné devíti. Potom ovšem výběrem a spolu s třemi jedničkami získáváme dělitelnost $9 \mid a \cdot 1 \cdot 1 \cdot 1 \mid a^4 + 1^4 + 1^4 + 1^4 = a^4 + 3$, která vzhledem k $9 \mid a^4$ neplatí. Jediné vyhovující 2016-tice za předpokladu nesoudělnosti jsou (1,1, ... ,1) a (3,1, ... ,1). Všechna vyhovující řešení jsou tedy 2016-tice tvaru $(n, n, \ldots, n)$ nebo $(3n, n, \ldots, n)$, kde $n \in \mathbb{N}$.

Poznámky:
Kdo pracoval s kongruencemi čtvrtých mocnin, úlohu zpravidla vyřešil. Někteří z vás mlčky předpokládali, že když je součet dvou zlomků celé číslo, pak musí být i oba zlomky celá čísla. Jenomže např. $1/3 + 2/3 = 1$. Samozřejmě, že v některých speciálních případech toto tvrzení může platit, ale je to potřeba řádně odůvodnit. *(Marian Poljak)*

Úloha 8.

Nechť $p(n)$ je nejvyšší prvočíselný dělitel čísla $n > 1$. Ukažte, že existuje nekonečně mnoho čísel $n > 2$, pro která platí $p(n-1) < p(n) < p(n+1)$.

(Tonda Le)

Řešení:
Nejprve si dokážeme několik lemmat, potom si ukážeme, jak s úlohou souvisí.

Lemma. *Nechť a, b jsou přirozená čísla. Potom platí $p(ab) = \max\{p(a), p(b)\}$.*

Důkaz. Označme $q = p(ab)$. Jistě je q prvočíslo a platí $q \mid ab$ (z definice funkce $p(n)$). Potom ale $q \mid a$ nebo $q \mid b$, tedy $p(a) \geq q$ nebo $p(b) \geq q$, ale kdyby některé z $p(a)$, $p(b)$ bylo větší než q, tak by to byl spor s $q = p(ab)$. □

Všimněme si, že $q^{2^k} - 1 = (q-1)(q+1)(q^2+1)\ldots\left(q^{2^{k-1}}+1\right)$, což získáme postupným používáním vzorce $a^2 - b^2 = (a-b)(a+b)$.

Lemma. *Nechť $q \in \mathbb{N}$. Potom pro každá přirozená $a < b$ a každé liché prvočíslo r platí, že pokud $r \mid q^{2^a} + 1$, potom $r \nmid q^{2^b} + 1$.*

Důkaz. Předpokládejme, že $r \mid q^{2^a} + 1$. Podle vzorečku, který jsme odvodili výše, můžeme napsat

$$q^{2^b} + 1 = 2 + q^{2^b} - 1 = 2 + (q-1)(q+1)(q^2+1)\dots\left(q^{2^{b-1}} + 1\right),$$

přičemž protože $a < b$, tak se v součinu jistě vyskytuje i $q^{2^a} + 1$. Ale $r \mid q^{2^a} + 1$, a tedy i $r \mid (q-1)(q+1)(q^2+1)\dots\left(q^{2^{b-1}} + 1\right)$. To ale znamená, že $q^{2^b} + 1 = kr + 2$ pro nějaké přirozené k, ale protože r je liché prvočíslo, tak jistě $r \nmid kr + 2$, což jsme chtěli dokázat. □

Důsledek. *Nechť $q > 2$ je prvočíslo. Potom pro každé k přirozené existuje takové prvočíslo $r > 2$, že $r \mid q^{2^k} + 1$, ale $r \nmid q^{2^\ell} + 1$ pro všechna $\ell < k$ přirozená.*

Důkaz. Protože je $q > 2$, tak je q liché, a tedy $q^2 \equiv 1 \pmod 4$. To znamená, že $4 \nmid q^{2^k} + 1$ pro žádné k (protože $q^{2^k} = \left(q^2\right)^{2^{k-1}} \equiv 1 \pmod 4$, a tedy $q^{2^k} + 1 \equiv 2 \pmod 4$). A protože $q^{2^k} + 1 > 2$, tak jistě bude existovat nějaké liché prvočíslo r, které dělí $q^{2^k} + 1$.

Potom ale už stačí použít předchozí lemma – kdyby to liché prvočíslo r, které dělí $q^{2^k} + 1$, dělilo i nějaké $q^{2^\ell} + 1$, byl by to spor s předchozím lemmatem. □

Důsledek můžeme nahlédnout (a větší část úspěšných řešení to tak i udělala) i pomocí tzv. Zsigmondyho věty. Ale jak můžeme vidět, v tomto případě byl Zsigmondy zbytečně veliké kladivo.

Lemma. *Nechť $q > 2$ je prvočíslo. Potom existuje přirozené číslo $k > 0$ takové, že $p\left(q^{2^k} + 1\right) > q$.*

Důkaz. Uvědomme si, že z důsledku plyne, že pro $k \neq \ell$ nemůže nastat $p\left(q^{2^k} + 1\right) = p\left(q^{2^\ell} + 1\right)$. Víme, že každý výraz tvaru $q^{2^k} + 1$ je dělitelný nějakým lichým prvočíslem, tedy i $p\left(q^{2^k} + 1\right)$ bude nějaké liché prvočíslo. A důsledek říká, že žádné prvočíslo nedělí zároveň $q^{2^k} + 1$ a $q^{2^\ell} + 1$, tedy speciálně to platí i pro prvočíslo $p\left(q^{2^k} + 1\right)$, a proto $p\left(q^{2^\ell} + 1\right)$ bude jiné.

To znamená, že pokud se podíváme na čísla $p\left(q^{2^i} + 1\right)$ pro $1 \leq i \leq q+1$, tak dostaneme $q+1$ různých prvočísel, ale to znamená, že některé z nich jistě bude větší než q.[2] □

Nyní už máme připravené všechno pro dokázání úlohy. Ukážeme, že pro každé liché prvočíslo q existuje n (pro každé prvočíslo jiné n), které splňuje zadání úlohy. To společně s tím, že prvočísel je nekonečně mnoho, již úlohu řeší.

Mějme tedy nějaké pevné prvočíslo $q > 2$ a vezměme k nejmenší takové, že $p\left(q^{2^k} + 1\right) > q$. Jistě $k \geq 1$. Ukážeme, že $n = q^{2^k}$ vyhovuje. (Zřejmě pro různá prvočísla dostaneme různá n.)

Jistě platí $p(n) = p\left(q^{2^k}\right) = q$ a z volby k máme $p(n+1) = p\left(q^{2^k} + 1\right) > q$. Potřebujeme tedy dokázat, že $p(n-1) = p\left(q^{2^k} - 1\right) < q$.

Platí

$$q^{2^k} - 1 = (q-1)(q+1)(q^2+1)\dots\left(q^{2^{k-1}} + 1\right),$$

a tedy

$$p\left(q^{2^k} - 1\right) = \max\left\{p(q-1), p(q+1), p\left(q^2+1\right), \dots, p\left(q^{2^{k-1}} + 1\right)\right\}.$$

Jistě $p(q-1) < q$ a z volby k nejmenšího takového, že $p\left(q^{2^k} + 1\right) > q$ máme, že pro všechna $\ell < k$ platí $p\left(q^{2^\ell} + 1\right) < q$, přičemž nerovnost je ostrá, protože q jistě nedělí $q^{2^\ell} + 1$. To ale znamená, že i maximum z těchto výrazů je menší než q, a tedy skutečně $p(n-1) < p(n) < p(n+1)$.

[2] Samozřejmě by tu stačilo vzít si těch čísel i méně.

Poznámky:
Všechna správná řešení použila stejné myšlenky, jako jsme si zde ukázali. Několik řešitelů se snažilo najít prvočísla tvaru $2p + 1$, kde p je prvočíslo. Potom stačí zvolit $n = 2p$ a to splňuje zadání.

Takovým prvočíslům se říká *prvočísla Sophie Germainové* nebo také tzv. *bezpečná prvočísla* (protože mají dobré kryptografické vlastnosti[3]), ale nikdo zatím bohužel (nebo naštěstí?) neumí dokázat, že je jich nekonečně mnoho. Předpokládá se, že tomu tak je, ale důkaz zatím nemáme. (Což je ostatně také důvod, proč jsme tuhle úlohu mohli zadat. Kdyby měla takovéhle řešení, tak by to nebyla moc dobrá úloha.) *(Matěj Konečný)*

[3]Multiplikativní grupa čísel modulo $2p + 1$ má velkou podgrupu prvočíselného řádu.