Teorie čísel

2. seriálová série — Termín odeslání: 10. února 2014

Úloha 1. (5 bodů)

Najděte všechny dvojice (m, n) přirozených čísel, které splňují rovnosti

$$m^{m+n} = n^{12},$$
$$n^{m+n} = m^3.$$

Úloha 2. (5 bodů)

Čísla $a, b, c, d \in \{1, 2, \ldots, 40\}$ splňují kongruenci

$$41a - 40 \cdot 6^a + 41b - 40 \cdot 6^b \equiv 41c - 40 \cdot 6^c + 41d - 40 \cdot 6^d \pmod{1640}.$$

Dokažte, že čísla a, b se v nějakém pořadí rovnají číslům c, d.

Úloha 3. (5 bodů)

Dá se ukázat, že číslo $p = 2^{127} - 1$ je prvočíslo.[1] S využitím tohoto faktu dokažte, že 2014 je kvadratický zbytek modulo p.

[1] Milou zajímavostí je, že nejen $2^{127} - 1$ je Mersennovo prvočíslo, ale dokonce $127 = 2^7 - 1$ je také Mersennovo prvočíslo.

Teorie čísel

2. seriálová série — Vzorové řešení

Úloha 1. (46; 41; 3,89; 4,5)

Najděte všechny dvojice (m, n) přirozených čísel, které splňují rovnosti

$$m^{m+n} = n^{12},$$
$$n^{m+n} = m^3.$$

(Štěpán Šimsa)

Řešení:
První rovnici umocníme na $(m+n)$, druhou na dvanáctou. Dostaneme

$$m^{(m+n)^2} = n^{12(m+n)} = m^{36}.$$

Aby platila tato rovnost, musí nastat jedna ze dvou možností:

(i) Platí $m = 1$, pak z první rovnice ze zadání okamžitě plyne i $n = 1$, což je řešením soustavy.

(ii) Platí $(m+n)^2 = 36$. Tedy

$$|m+n| = m+n = 6. \qquad (\clubsuit)$$

Dosazením do první rovnice ze zadání dostaneme $m^6 = n^{12}$ neboli $m = n^2$. Tento vztah dosadíme do $(\clubsuit)$. Kvadratická rovnice $n^2 + n = 6$ má kořeny $n = -3$ a $n = 2$, přitom první nevyhovuje, protože po n požadujeme, aby bylo přirozené. Dopočteme $m = 2^2 = 4$, což je opět řešením soustavy.

Zadání vyhovují dvojice $(1, 1)$ a $(4, 2)$.

Poznámky:
Úloha byla jednoduchá a vzdala se takřka jakémukoli pokusu o vyřešení. Původně byla myšlena jako úloha na p-valuace a z toho, že valná část řešitelů p-valuace skutečně použila, usuzuji alespoň tu pozitivní informaci, že se do seriálu díváte. Po provedení p-valuace se rovnice totiž zjednoduší na

$$(m+n) \cdot v_p(m) = 12 \cdot v_p(n), \quad (m+n) \cdot v_p(n) = 3 \cdot v_p(m).$$

Manipulace s takovými rovnicemi je pak analogická postupu ve vzorovém řešení, ale pro řešitele patrně o něco přehlednější. Jiní řešitelé soustavu zlogaritmovali, čímž dostali stejnou soustavu jako v případě p-valuací, jenom místo symbolu v_p psali log. A jako třetí možnost se taky dalo usoudit, že čísla m, n nejsou příliš velká (případ $m + n \geq 12$ vede ke sporu), čímž zbývá už jen konečné množství možností, které se více či méně inteligentně prozkoušejí. *(Mirek Olšák)*

Úloha 2. (22; 20; 3,41; 4,0)

Čísla $a, b, c, d \in \{1, 2, \ldots, 40\}$ splňují kongruenci

$$41a - 40 \cdot 6^a + 41b - 40 \cdot 6^b \equiv 41c - 40 \cdot 6^c + 41d - 40 \cdot 6^d \pmod{1640}.$$

Dokažte, že čísla a, b se v nějakém pořadí rovnají číslům c, d. *(Štěpán Šimsa)*

Řešení:

Díky tomu, že $1640 = 40 \cdot 41$ a $(40, 41) = 1$, je kongruence ze zadání splněna právě tehdy, je-li splněna tatáž kongruence modulo 40 a 41. Jejich úpravou („vyškrtnutím“ členů dělitelných modulem) dostáváme následující dvě kongruence:

$$a + b \equiv c + d \pmod{40}, \qquad (\heartsuit)$$
$$6^a + 6^b \equiv 6^c + 6^d \pmod{41}. \qquad (\spadesuit)$$

Všimněme si, že dvě čísla $x, y \in \{1, 2, \ldots, 40\}$ se rovnají právě tehdy, když $x \equiv y \pmod{40}$; to je dále ekvivalentní s kongruencí $6^x \equiv 6^y \pmod{41}$, je-li 6 primitivní prvek modulo 41 (je totiž $\varphi(41) = 40$), což budeme dále předpokládat. Chceme-li tedy ukázat, že $a \in \{c, d\}$, stačí nám ukázat, že $(6^a - 6^c)(6^a - 6^d) \equiv 0 \pmod{41}$ – zde využíváme, že 41 je prvočíslo. Upravujme:

$$(6^a - 6^c)(6^a - 6^d) \equiv 6^{2a} - 6^a(6^c + 6^d) + 6^{c+d} \equiv 6^{2a} - 6^a(6^a + 6^b) + 6^{a+b} \equiv 0 \pmod{41},$$

kde jsme v druhém kroku využili $(\heartsuit)$ i $(\spadesuit)$. Vidíme tedy, že a se rovná jednomu z čísel c, d; dosazením do $(\heartsuit)$ pak dostáváme, že b se rovná druhému z těchto dvou čísel.

Zbývá ukázat, že 6 je skutečně primitivní prvek modulo 41, neboli že jeho řád (označme ho r) je roven 40. Určitě platí $r \mid 40$, stačí tedy vyloučit případy $r \mid 20$ a $r \mid 8$ (každý vlastní dělitel 40 je už dělitelem jednoho z těchto dvou čísel). Platí

$$6^4 = 36^2 \equiv (-5)^2 = 25 \pmod{41},$$

odkud dále máme

$$6^8 \equiv 25^2 \equiv (-16)^2 = 256 \equiv 10,$$
$$6^{20} \equiv (-16)^5 \equiv 10^2 \cdot (-16) \equiv -18 \cdot 16 \equiv -1 \pmod{41}.$$

Řád 6 je tedy vskutku 40, což jsme potřebovali.

Poznámky:

Téměř všichni řešitelé odhalili výhodnou úpravu na dvě kongruence, která úlohu značně zpřehlednila. Zhruba polovina se pak pomocí více či méně efektivních úprav dopočetla ke kýženému výsledku. Za nezdůvodnění konstatování, že 6 je primitivní prvek modulo 41, jsem se nakonec rozhodl body nestrhávat, jelikož mi to přišlo jako čistě manuální a nepříliš náročný výpočet (i bez použití výše uvedeného „triku“). Kladný imaginární bod získal *František Couf*, který v úloze vypozoroval Viètovy vztahy a vyhnul se tak jakýmkoliv úpravám.

(Alexander „Olin“ Slávik)

Úloha 3. (24; 22; 4,46; 5,0)

Dá se ukázat, že číslo $p = 2^{127} - 1$ je prvočíslo.[2] *S využitím tohoto faktu dokažte, že* 2014 *je kvadratický zbytek modulo p.* *(Štěpán Šimsa)*

Řešení:

Využijeme vlastností Legendreových symbolů a kvadratické reciprocity. Naším cílem je dokázat

$$\left(\frac{2014}{2^{127}-1}\right) = 1.$$

Díky multiplikativitě máme

$$\left(\frac{2014}{p}\right) = \left(\frac{2 \cdot 19 \cdot 53}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{19}{p}\right)\left(\frac{53}{p}\right).$$

Platí $\frac{p^2-1}{8} = 2^{251} - 2^{125}$, což je sudé, takže s využitím dodatku ke kvadratické reciprocitě dostáváme

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1.$$

Jelikož p je tvaru $4k+3$, 19 je tvaru $4k+3$ a 53 je tvaru $4k+1$, tak podle věty o kvadratické reciprocitě

$$\left(\frac{19}{p}\right) = -\left(\frac{p}{19}\right) \qquad \text{a} \qquad \left(\frac{53}{p}\right) = \left(\frac{p}{53}\right).$$

Podle MFV platí $2^{18} \equiv 1 \pmod{19}$, takže $2^{127} - 1 \equiv (2^{18})^7 \cdot 2 - 1 \equiv 1 \pmod{19}$. Odtud plyne

$$\left(\frac{p}{19}\right) = \left(\frac{1}{19}\right) = 1,$$

protože 1 je vždy kvadratický zbytek (speciálně modulo 19).

Opět podle MFV $2^{52} \equiv 1 \pmod{53}$. Takže $2^{127} - 1 \equiv 2^{23} \cdot (2^{52})^2 - 1 \equiv 2^{23} - 1 \pmod{53}$. Nyní stačí nějak postupně zjistit tuto hodnotu:

$$2^{23} \equiv \frac{1}{2} \cdot 2^{24} \equiv \frac{1}{2}(2^8)^3 \equiv \frac{1}{2} \cdot 256^3 \equiv \frac{1}{2}(-9)^3 \equiv \frac{1}{2} \cdot 81 \cdot (-9) \equiv \frac{1}{2} \cdot 28 \cdot (-9) \equiv$$
$$\equiv 14 \cdot (-9) \equiv -126 \equiv 33 \pmod{53}.$$

Proto

$$\left(\frac{p}{53}\right) = \left(\frac{32}{53}\right) = \left(\frac{2}{53}\right)^5 = (-1)^{5 \cdot \frac{52 \cdot 54}{8}} = (-1)^{5 \cdot 13 \cdot 27} = -1.$$

Zbývá již jen dát vše dohromady a dostáváme, co jsme chtěli:

$$\left(\frac{2014}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{19}{p}\right)\left(\frac{53}{p}\right) = 1 \cdot (-1) \cdot \left(\frac{p}{19}\right) \cdot \left(\frac{p}{53}\right) = (-1) \cdot 1 \cdot (-1) = 1.$$

Poznámky:

Nejdůležitějším krokem bylo uvědomit si, že se dá vhodně využít reciprocita. Potom už jen stačilo využívat vlastností, které se objevily v seriálu. Někteří bez zdůvodnění uvedli, že $2^{127} - 1$ dává zbytek 1 modulo 19, resp. 32 modulo 53. To se neobešlo bez ztráty bodu. Jiní sice výraz značně zjednodušili (například pomocí MFV na $2^{23} - 1$), ale stejně se neobešli bez složitých výpočtů. Přitom nějakým částečným modulením se dá práce výrazně ulehčit. (Ne nutně tak, jak je to ve vzoráku – pomohlo by například i $(2^6)^3 \cdot 2^5$ nebo alespoň $(2^{11} \bmod 53) \cdot (2^{12} \bmod 53)$.)

(Štěpán Šimsa)

[2] Milou zajímavostí je, že nejen $2^{127} - 1$ je Mersennovo prvočíslo, ale dokonce $127 = 2^7 - 1$ je také Mersennovo prvočíslo.