22. SÚČTY MOCNÍN

Je úplne jasné, že nie každé prirodzené číslo je druhou mocninou iného prirodzeného čísla. To isté platí aj pre ostatné mocniny (tretiu, štvrtú, piatu, ...). Dokonca podľa vety 19 platí, že množina týchto prirodzených čísel má asymptotickú hustotu 0. Môže sa nám teda zdať, že týchto čísel je zanedbateľne málo. Ktoré čísla môžeme získať, ak uvažujeme všetky súčty tvaru $a^2 + b^2$?

Úloha 505. Dokážte, že žiadne prirodzené číslo tvaru $4k + 3$ nemožno vyjadriť v tvare súčtu druhých mocnín dvoch prirodzených čísel.

O to zaujímavejšie je tvrdenie vety, ktorú dokážeme v nasledujúcej časti.

Veta 29. Každé prirodzené číslo n môžeme vyjadriť v tvare

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n.$$

Pri dôkaze tejto vety bude hrať dôležitú úlohu nasledujúca rovnosť.

Úloha 506. Dokážte, že pre ľubovoľné čísla $x_1, ..., x_4$, $y_1, ..., y_4$ platí

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = A_1^2 + A_2^2 + A_3^2 + A_4^2,$$

kde

$$A_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4,\ A_2 = -x_1y_2 + x_2y_1 - x_3y_4 + x_4y_3,$$
$$A_3 = -x_1y_3 + x_3y_1 - x_4y_2 + x_2y_4,\ A_4 = -x_1y_4 + x_4y_1 - x_2y_3 + x_3y_2.$$

Ďalej budeme používať čísla A_1, A_2, A_3, A_4 z úlohy 506 ako štandardné označenie. Rovnosť z tejto úlohy nazývame *Eulerova identita*. Dokážeme ju jednoduchou úpravou.

Úloha 507. Dokážte, že veta 29 platí, ak sa každé prvočíslo dá vyjadriť v tvare súčtu mocnín štyroch nezáporných celých čísel.

(Návod: Použite úlohu 506 a základnú vetu aritmetiky.)

Teraz se budeme zaoberať iba vyjadrením prvočísel v tvare súčtu druhých mocnín štyroch nezáporných celých čísel. Využijeme nasledujúce pomocné tvrdenie.

Lema 3 Pre každé prvočíslo p kongruencia

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

má riešenie.

Úloha 508. Dokážte lemu 3 pre $p = 2$.

Úloha 509. Nech p je prvočíslo. Dokážte:

a) Ak $p = 4k + 1$, potom kongruencia $x^2 + 1 \equiv 0 \pmod{p}$ má riešenie.
b) Ak $p = 4k + 3$ a c je najmenší kvadratický nezvyšok modulo p, potom $c - 1, -c$ sú kvadratické zvyšky modulo p.

Úloha 510. Pomocou úlohy 509 dokážte lemu 3.

Úloha 511. Dokážte, že pre každé prvočíslo p existuje také prirodzené číslo $n_0 > 0$, že

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n_0 p \tag{32}$$

pre nejaké celé čísla $x_i, i = 1, 2, 3, 4$.

(Návod: Použite lemu 3 a zvoľte si napríklad $x_4 = 0$.)

Aby sme dokázali, že každé prvočíslo môžeme vyjadriť v tvare súčtu druhých mocnín štyroch nezáporných celých čísel, stačí dokázať, že najmenšie n_0, ktoré spĺňa vzťah (32) sa rovná 1. Na to použijeme nasledujúce tvrdenie.

Úloha 512. Nech $m \in \mathbb{N}$. Potom pre každé $a \in \mathbb{Z}$ existuje také celé číslo b, že

$$a \equiv b \pmod{m} \tag{33}$$

a

$$|b| \leq \frac{m}{2}. \tag{34}$$

Dokážte.

Teraz budeme predpokladať, že $n_0 p$ z rovnosti (32) je najmenší násobok prvočísla p, ktorý môžeme vyjadriť v tvare súčtu druhých mocnín štyroch nezáporných čísel. Budeme to dokazovať pre $n_0 = 1$. Je zrejmé, že číslo 2 sa dá vyjadriť ako súčet druhých mocnín štyroch nezáporných čísel. Preto predpokladajme, že $p > 2$.

Úloha 513. Podľa úlohy 512 dokážte, že $n_0 < p$.

Úloha 514. Ak číslo n_0 v rovnosti (32) je párne, potom čísla x_i sú nepárne pre 0, 2 alebo 4 indexy.

Úloha 515. Pomocou úlohy 513 dokážte: Ak číslo n_0 v rovnosti (32) je párne, potom čísla x_i môžeme označiť tak, aby $x_1 + x_2$ a $x_3 + x_4$ boli párne. V tomto prípade dokážte pomocou čísel $z_1 = \frac{x_1+x_2}{2}$, $z_2 = \frac{x_1-x_2}{2}$, $z_3 = \frac{x_3+x_4}{2}$, $z_4 = \frac{x_3-x_4}{2}$ spor s minimalitou n_0.

Teraz budeme predpokladať, že n_0 je nepárne a $n_0 > 1$.

Úloha 516. Dokážte, že k číslu x_i z rovnosti (32) existujú také celé čísla y_i pre $i = 1, 2, 3, 4$, že

$$x_i \equiv y_i \pmod{n_0}$$

a

$$|y_i| \leq \tfrac{n_0}{2}.$$

Úloha 517. Dokážte, že pre čísla y_i z úlohy 516 platí:

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = n_1 n_0,\ 0 < n_1 < n_0.$$

(Návod: Použite úlohu 513 a rovnosť (32). Uvedomte si, že ak pre všetky i $y_i = 0$, potom $n_0 = p$, čo je spor s úlohou 513.)

Úloha 518. Uvažujme Eulerovu identitu

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = A_1^2 + A_2^2 + A_3^2 + A_4^2$$

kde čísla x_i sú z rovnosti (32) a čísla y_i sú z úlohy 515 pre $i = 1, 2, 3, 4$. Označenie A_1, A_2, A_3, A_4 je rovnaké ako v úlohe 505. Dokážte, že $n_0 | A_i$ pre $i = 1, ..., 4$.

(Návod: Použite úlohu 516 a rovnosť (32).)

Úloha 519. Nech A_1, A_2, A_3, A_4 sú z predchádzajúcej úlohy. Nech $A_i = n_0 z_i$ pre $i = 1, 2, 3, 4$. Dokážte, že

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = n_1 p.$$

Úloha 520. Dokážte, že $n_0 = 1$.

(Návod: Použite spor s minimalitou, ktorý získate použitím úloh 517 a 519.)

Úloha 521. Dokážte vetu 29.

Na začiatku tejto kapitoly sme si ukázali, že nie každé číslo môžeme vyjadriť v tvare súčtu druhých mocnín dvoch nezáporných celých čísel. Existuje ale rozsiahla množina takých prirodzených čísel, ktoré sa dajú v tomto tvaru vyjadriť.

Veta 30. Každé prvočíslo tvaru $4k + 1$ sa dá jednoznačne vyjadriť v tvare súčtu druhých mocnín dvoch nezáporných celých čísel.

Použijeme identitu, ktorá sa podobá na Eulerovu, ale ktorá je pre prípad súčtu dvoch druhých mocnín nezáporných celých čísel jednoduchšia.

Úloha 522. Dokážte, že pre všetky čísla x, y, x_1, y_1 platí

$$(x^2+y^2)(x_1^2+y_1^2) = (xx_1+yy_1)^2 + (xy_1-yx_1)^2.$$

Budeme používať označenie

$$B_1 = xx_1 + yy_1,\ B_2 = xy_1 - x_1y. \tag{35}$$

Úloha 523. Ak p je prvočíslo v tvare $4k+1$, potom kongruencia

$$x^2 + y^2 \equiv 0 \pmod{p}$$

má nenulové riešenie.

(Návod: Je to vlastne časť a) úlohy 509.)

Úloha 524. Ak p je prvočíslo tvaru $4k+1$, potom existuje také číslo $g_0 > 0$, pre ktoré

$$x^2 + y^2 = g_0 p. \tag{36}$$

(Návod: Je to iba prepis úlohy 523.)

Aby sme dokázali vetu 30 stačí dokázať, že minimálne číslo g_0, ktoré vyhovuje rovnici (36) sa rovná 1. Predpokladajme, že g_0 je minimálne nenulové prirodzené číslo, ktoré vyhovuje rovnici (36).

Úloha 525. Dokážte, že $g_0 < p$.

(Návod: Použite úlohu 512.)

Úloha 526. Dokážte, že číslo g_0 je nepárne.

(Návod: Postupujte analogicky ako v úlohe 514.)

Predpokladajme, že $g_0 \geq 3$ je nepárne číslo.

Úloha 527. Dokážte, že existujú také celé čísla x_1, y_1, že

$$x \equiv x_1 \pmod{g_0},\ y \equiv y_1 \pmod{g_0}$$

pre ktoré platí $|x_1|, |y_1| < \frac{g_0}{2}$ a $x_1^2 + y_1^2 > 0$.

(Návod: Na dôkaz poslednej nerovnosti použite úlohu 525.)

Úloha 528. Nech x_1, y_1 sú celé čísla z úlohy 527. Dokážte, že

$$x_1^2 + y_1^2 = g_1 g_0,\ 0 < g_1 < g_0.$$

Úloha 529. Nech B_1, B_2 sú určené vzťahom (35). Dokážte, že $B_1 = g_0 z_1, B_2 = g_0 z_2$, kde z_1, z_2 sú celé čísla a

$$z_1^2 + z_2^2 = g_1 p.$$

(Návod: Použite úlohy 522 a 528.)

Úloha 530. Dokážte existenciu z vety 30.

(Návod: Úloha 529 nám dáva spor s minimalitou g_0.)

Teraz budeme dokazovať jednoznačnosť. Predpokladajme, že

$$x^2 + y^2 = p,\ x_1^2 + y_1^2 = p,\ x < y, x_1 < y_1 \tag{37}$$

pre nejaké prirodzené čísla x, y, x_1, y_1.

Úloha 531. Dokážte, že $0 < x, y, x_1, y_1 < \sqrt{p}$.

Úloha 532. Dokážte, že

$$(xy_1 - yx_1)(xy_1 + yx_1) = p(y_1^2 - y^2).$$

Úloha 533. Dokážte, že $(x, y) = 1 = (x_1, y_1)$.

Úloha 534. Dokážte, že

$$p | xy_1 - yx_1 \implies x = x_1,\ y = y_1.$$

(Návod: Použite úlohy 531 a 533.)

Úloha 535. Dokážte, že

$$p | xy_1 + yx_1 \implies p = xy_1 + yx_1.$$

(Návod: Použite úlohu 531.)

Úloha 536. Dokážte, že

$$(x^2 + y^2)(x_1^2 + y_1^2) = (xx_1 - yy_1)^2 + (xy_1 + yx_1)^2.$$

Úloha 537. Dokážte, že prípad $p | xy_1 + yx_1$ nemôže nastať.

(Návod: Použite úlohy 536, 535 a nerovnosti v (37).)

Úloha 538. Dokážte jednoznačnosť vo vete 30.

(Návod: Použite úlohy 532 a 534.)

Úloha 539. Dokážte, že každé prirodzené číslo, ktoré má vo svojom kanonickom rozklade iba prvočísla tvaru $4k + 1$, môžeme vyjadriť ako súčet druhých mocnín dvoch nezáporných celých čísel.

V závere tejto kapitoly poznamenajme, že otázky spojené s vyjadrovaním čísel v tvare súčtu druhých mocnín prirodzených čísel siahajú hlboko do histórie. Vetu 29 dokázal v roku 1770 Lagrange. V tom istom roku Waring dokázal, že každé prirodzené číslo môžeme vyjadriť ako súčet deviatich tretích mocnín. Podobnú vlastnosť dokázal aj pre štvrté mocniny. Neskôr bola sformulovaná nasledujúca hypotéza známa ako *Waringov problém*:

Ku každému celému číslu $k > 1$ existuje také prirodzené číslo $g(k)$, že každé prirodzené číslo môžeme vyjadriť ako súčet $g(k)$ k-tych mocnín.

Tento problém úplne vyriešil Hilbert. V súčasnosti sa značné úsilie venuje výskumu vlastností funkcie $g(k)$.