

# Algebrai Számelmélet

## 7. feladatsor

beadható 2018. november 15-ig

A következő feladatok némileg egymásra épülnek. A cél itt a Fermat-sejtés első esetének igazolása reguláris prímekekre.

1. (3 pont) Igazoljuk, hogy  $\frac{u}{v}$  egységgyök tetszőleges  $u \in \mathcal{O}_n^\times$  egységre, ha  $\mathcal{O}_n$  az  $n$ -edik körosztási test egészeinek gyűrűjét jelöli. Mutassuk meg továbbá, hogy ha  $n = p^k$  valamely páratlan  $p$  prímre, akkor  $\frac{u}{v}$  egy  $p^k$ -adik egységgyök is, azaz létezik egy

$$\begin{aligned} \mathcal{O}_{p^k}^\times &\rightarrow \mu_{p^k} \\ u &\mapsto \frac{u}{v} \end{aligned}$$

csoporthomomorfizmus.

2. (3 pont) Legyen  $p$  egy páratlan prímszám és jelöljük  $\mathcal{O}_{p^k}$ -nak a  $p^k$ -adik körosztási testet. Igazoljuk, hogy  $\mathcal{O}_{p^k}^\times$ -ben minden  $u$  elem felírható  $u = \zeta v$  alakban, ahol  $\zeta$  egy alkalmas  $p^k$ -adik egységgyök,  $v \in \mathbb{Z}[\zeta] \cap \mathbb{R}$  pedig valós.

Tegyük fel, hogy  $p \nmid xyz$  olyan egész számok, melyekre  $x^p + y^p = z^p$  ( $2 < p$  prím).

3. (1+1 points) Modulo 9 vizsgálódva igazoljuk, hogy  $p \neq 3$ . Modulo 25 vizsgálódva igazoljuk, hogy  $p \neq 5$ .

Legyen tehát mostantól  $p > 5$  és jelöljük  $\zeta$ -val egy fix primitív  $p$ -edik egységgyököt.

4. (1 point) Feltehetjük, hogy az  $x, y, z$  számok páronként relatív prímekek, továbbá azt is, hogy  $p \nmid x - y$ .
5. (2 pont) Igazoljuk, hogy az  $x + y, x + y\zeta, \dots, x + y\zeta^{p-1}$  számok páronként relatív prímekek  $\mathcal{O}_p$ -ben.
6. (2 pont) Igazoljuk, hogy minden  $\alpha \in \mathcal{O}_p$ -re  $\alpha^p \in \mathbb{Z} + p\mathcal{O}_p$  (azaz van olyan  $a \in \mathbb{Z}$ , melyre  $a - \alpha^p$  osztható  $p$ -vel).
7. (2 pont) Legyen  $\alpha = a_0 + a_1\zeta + \dots + a_{p-1}\zeta^{p-1}$ , ahol  $a_i \in \mathbb{Z}$  ( $i = 0, \dots, p-1$ ) és legalább az egyik  $a_i = 0$ . Igazoljuk, hogy ha  $\alpha \in n\mathcal{O}_p$  alkalmas  $n \in \mathbb{Z}$  egész számmal, akkor  $n \mid a_i$  minden  $i = 0, \dots, p-1$ -re.
8. (2 pont) Ha egy számtest osztályszámát nem osztja  $p$  és egy ideál  $p$ -edik hatványa főideál, akkor az ideál maga is főideál.

9. (3 pont) Tegyük fel, hogy  $p$  nem osztja  $\mathcal{O}_p$  osztályszámát. Lássuk be, hogy a fenti  $x^p + y^p = z^p$  egyenletnek nincs olyan megoldása, amire  $p \nmid xyz$ . Segítség: alakítsuk az egyenletet  $\prod_{j=0}^{p-1} (x + y\zeta^j) = (z)^p$  alakba. Mindkét oldalt bontsuk  $\mathcal{O}_p$ -ben prímeideálok szorzatára. Vegyük észre, hogy feltételek miatt  $x + \zeta^j y = u_j \alpha_j^p$  alakú, ahol  $u_j \in \mathcal{O}_p^\times$  egység,  $\alpha_j \in \mathcal{O}$ . Most  $\alpha_1$ -re alkalmazzuk a 6. Feladatot,  $u_1$ -re pedig a 2. Feladatot, hogy találhassunk egy olyan  $r \in \mathbb{Z}$  egész számot, melyre  $x + \zeta y \equiv \zeta^r v a \pmod{p}$ , ahol  $v \in \mathbb{R}$ ,  $a \in \mathbb{Z}$ . Az előző kongruenciát megkonjugálva kapjuk, hogy  $p \mid x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y$ . A 7. Feladat segítségével jussunk ellentmondásra.