1. Euler-egészek — emlékeztető

Az Euler-egészek az $\alpha = a + b\varepsilon$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\varepsilon = -1/2 + i\sqrt{3}/2$ primitív harmadik egységgyök. Ezek egy $\mathbb{E}$ euklideszi gyűrűt alkotnak az $N(\alpha) = |\alpha|^2 = a^2 - ab + b^2$ normára nézve. A bizonyítás hasonló, mint Gauss-egészekre: az $\alpha : \beta$ osztásnál az α/β számhoz kell közeli rácspontot találni a szabályos háromszögrácsban. Legyen $\lambda = i\sqrt{3} \in \mathbb{E}$.

1.1. Állítás. *Az $\mathbb{E}$ egységei az 1 normájú Euler-egészek, amik éppen a hatodik egységgyökök. Ezek páronként inkongruensek mod $\lambda^2 = -3$, de ε és ε^2 is 1-gyel kongruens mod λ.* □

1.2. Lemma. *Legyen $p > 3$ prímszám. Az $a^2 - ab + b^2 \equiv 0$ (p) kongruenciának akkor és csak akkor van nem nulla megoldása, ha $p \equiv 1$ (3).*

Az alábbi bizonyítás használja a kvadratikus reciprocitási tételt, cserébe általánosítható más számgyűrűkre is. Az állítás elemien is könnyen bizonyítható.

Bizonyítás. A kongruenciát b^2-tel mod p osztva $x^2 - x + 1 \equiv 0$ (p) adódik, ahol $x = a/b$. A másodfokú egyenlet megoldóképletét alkalmazzuk. A négyzetgyök alatti szám -3, az kell, hogy ez kvadratikus maradék legyen. A reciprocitási tétel miatt

$$\left(\frac{-3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right).$$

Ez pontosan akkor 1, ha $p \equiv 1$ (3). □

1.3. Állítás. *Az $\mathbb{E}$-beli prímek a következő számok asszociáltjai.*

a) $\lambda = i\sqrt{3} = 1 + 2\varepsilon$.
b) A pozitív, $3k + 2$ alakú $\mathbb{Z}$-beli prímek.
c) A π és $\overline{\pi}$ számok, ahol $p = \pi\overline{\pi}$ egy $\mathbb{Z}$-beli, pozitív, $3k + 1$ alakú prím. Minden ilyen p-hez egyetlen $\{\pi, \overline{\pi}\}$ pár tartozik.

Bizonyításvázlat. Az alaptételesség miatt $\mathbb{E}$-ben a felbonthatatlanok ugyanazok, mint a prímek. Mivel $\pi \mid N(\pi)$, minden Euler-prím osztója egy $\mathbb{Z}$-beli prímnek, tehát elegendő ezek felbontásait megkeresni. A prím normájú Euler-egészek könnyen láthatóan Euler-prímek. Hasonló gondolatmenet adja, hogy egy $p = 3k + 2$ alakú prím nemtriviális felbontása csak p normájú számokra történhet, de az előző lemma szerint ilyenek nincsenek, így p prím $\mathbb{E}$-ben is. Ugyanez a lemma mutatja, hogy ha $p > 0$ egy $3k + 1$ alakú prím, akkor $p \mid N(a + b\varepsilon) = (a + b\varepsilon)(\overline{a + b\varepsilon})$ teljesül alkalmas, p-vel nem osztható a-ra és b-re. Ezért p nem prím $\mathbb{E}$-ben, és akkor a normája miatt két prím szorzatára bomolhat csak. □

1.4. Állítás. *Az $\mathbb{E}/(\lambda^k)$ gyűrű elemszáma 3^k, a (λ) főideál elemszáma 3^{k-1}, és minden ezen kívüli elem egység.*

Bizonyítás. Mivel $a + b\varepsilon \equiv a + b$ (λ), ezért $\mathbb{E}$ minden eleme felírható $n + \beta\varepsilon$ alakban, ahol $n \in \{0, 1, -1\}$ és $\beta \in \mathbb{E}$. Ez a felírás egyértelmű, mert ha $\lambda \mid n_1 - n_2$, akkor $N(\lambda) \mid N(n_1 - n_2)$, ahonnan $3 \mid n_1 - n_2$. A β számot hasonlóképpen felbontva minden Euler-egész egyértelműen felírható $\alpha = n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1} + \beta_k\lambda^k$ alakban. Ezért $|\mathbb{E}/(\lambda^k)| = 3^k$. Az α elem akkor és csak akkor osztható λ-val, ha $n_0 = 0$, amiből a (λ) főideál elemszámát is megkapjuk. Végül az ismert azonosság miatt

$$\frac{n^k - (\alpha\lambda)^k}{n - \alpha\lambda} = \gamma \in \mathbb{E},$$

ezért ha $n \in \{1, -1\}$, akkor $n - \alpha\lambda$ inverze $\mathbb{E}/(\lambda^k)$-ban γ/n^k (maradékosztálya). □

1.5. Állítás. *Az $\mathbb{E}/(\lambda^4)$ gyűrűben minden egység köbe ± 1.*

Bizonyítás. Legyen $\alpha = a + b\lambda + \beta\lambda^2$, ahol $a = \pm 1$, $b \in \{0, 1, -1\}$ és $\beta \in \mathbb{E}$. Modulo λ^4 számolva, és felhasználva, hogy $3 = -\lambda^2$,

$$\alpha^3 \equiv (a + b\lambda)^3 \equiv a^3 + (b^3 - a^2 b)\lambda^3 = a^3 = a\,,$$

hiszen $a^2 = 1$ és $b^3 = b$. □

2. A Fermat-sejtés $n = 3$ esete

2.1. Lemma. *Ha $x, y \in \mathbb{E}$ relatív prímek, akkor az $x - y$, $x - \varepsilon y$ és $x - \varepsilon^2 y$, számok páronként kongruensek modulo λ, de bármely kettő legnagyobb közös osztója csak 1 vagy λ lehet.*

Bizonyítás. Az első állítás adódik abból, hogy 1, ε és ε^2 kongruensek mod λ. Elég megmutatni, hogy $(x - y, x - \varepsilon y) \in \{1, \lambda\}$, mert a másik két hasonló állítás következik úgy, hogy ezt y helyett εy-ra alkalmazzuk. Tegyük föl, hogy egy π Euler-prím osztja $x - y$-t és $x - \varepsilon y$-t is, akkor $\pi \mid y(1 - \varepsilon)$. Itt $\pi \mid y$ lehetetlen, mert akkor $\pi \mid x$ is teljesülne. Ezért $\pi \mid 1 - \varepsilon$, azaz $N(\pi) \mid N(1 - \varepsilon) = 3$, vagyis $\pi = \lambda$. A gondolatmenetet π helyett λ^2-re elmondva $\lambda \nmid y$ miatt $3 \mid 1 - \varepsilon$ adódna, ami már nem teljesül a normák miatt. □

2.2. Tétel. *A $\rho x^3 + \sigma y^3 + \tau z^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol ρ, σ és τ egységek, $z \neq 0$ osztható λ-val, de x és y nem.*

Megjegyezzük, hogy a $\rho x^3 + \sigma y^3 + \tau z^3 = 0$ egyenletnek lehet nemtriviális megoldása, például $x = y = z = 1$, $\rho = 1$, $\sigma = \varepsilon$, $\tau = \varepsilon^2$.

Bizonyítás. Feltehető $N(x)$ szerinti indukcióval, hogy x, y és z páronként relatív prímek. Vegyünk egy olyan ellenpéldát, amelyre z-ben a λ kitevője a lehető legkisebb.

Az 1.5. Állítás miatt x^3 és y^3 kongruens ± 1-gyel modulo λ^4. Az x és y előjelét szükség szerint megváltoztatva feltehető, hogy mindketten 1-gyel kongruensek. Mivel $\lambda^3 \mid z^3$, ezért $\rho \equiv -\sigma\ (\lambda^3)$. Az $\mathbb{E}$ egységei páronként inkongruensek modulo λ^2, tehát $\rho = -\sigma$. Ismét modulo λ^4 nézve az egyenletet azt kapjuk, hogy $\lambda^4 \mid \tau z^3$, vagyis $\lambda^2 \mid z$.

Az egyenletet ρ-val osztva az adódik, hogy $x^3 - y^3$ a z^3 egységszerese. De

$$x^3 - y^3 = (x - y)(x - \varepsilon y)(x - \varepsilon^2 y)\,,$$

így ez a szorzat osztható λ-val. A 2.1. Lemma miatt mindegyik tényező osztható λ-val, de ezzel őket elosztva páronként relatív prím számokat kapunk. Ezért

$$x - y = \rho_1 \lambda x_1^3\,, \qquad x - \varepsilon y = \sigma_1 \lambda y_1^3\,, \qquad x - \varepsilon^2 y = \tau_1 \lambda z_1^3$$

alkalmas Euler-egészekre, ahol ρ_1, σ_1, τ_1 egységek. Az első egyenlethez a második ε-szorosát és a harmadik ε^2-szeresét adva a bal oldalon nullát kapunk, ezért

$$\rho_1 x_1^3 + \varepsilon \sigma_1 y_1^3 + \varepsilon^2 \tau_1 z_1^3 = 0\,.$$

Ez ugyanolyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$, ezért x_1, y_1 és z_1 közül az egyik, mondjuk z_1, osztható lesz λ-val (de a másik kettő nem). Ha z-ben a λ kitevője k volt, akkor z_1-ben $k - 1$ lesz. Ez ellentmond k minimalitásának. □

2.3. Következmény. *A Fermat-sejtésnek nincs nemtriviális megoldása a 3 kitevőre.*

Bizonyítás. Ha $x^3 + y^3 = z^3$, ahol $(x, y, z) = 1$, akkor az előző tétel miatt x, y és z egyike sem osztható λ-val. Ez modulo $9 = \lambda^4$ ellentmondást ad az 1.5. Állítás miatt. □