Az első részben az idei Nemzetközi Matematikai Diákolimpia 2. feladatára mutattunk egy lehetséges megoldást. Most a 6. feladatot vizsgáljuk meg közelebbről. A feladatra két megoldást is mutatunk.

Az első – hasonlóan a 2. feladat megoldásához – nem használ semmilyen különleges ötletet vagy a középiskolai anyagon túlmutató ismeretet. Viszont egy olyan lépéssel kezdődik, amely első pillantásra talán túl ijesztő lehet.

A második megoldás jóval több ismeretet igényel. Ez a megoldás az egész számok halmazának egy kiterjesztése, az úgynevezett Euler-egészek elméletét használja fel. Cserébe viszont megmutatja a feladat valószínű eredetét.

A 6. feladat. *Legyenek a, b, c, d egészek, amelyekre $a > b > c > d > 0$. Tegyük fel, hogy*

$$ac + bd = (b + d + a - c)(b + d - a + c). \tag{6}$$

Bizonyítsuk be, hogy $ab + cd$ nem prímszám.

A (6) egyenletet átrendezve,

$$a^2 - ac + c^2 = b^2 + bd + d^2. \tag{7}$$

A továbbiakban mindig ezt az alakot fogjuk használni.

1. megoldás: Helyettesítsünk be!

A megoldás indirekt. Feltételezzük, hogy $ab+cd = p$, ahol p egy prímszám. Ezzel már egy egész egyenletrendszerünk van:

$$a^2 - ac + c^2 = b^2 + bd + d^2, \qquad ab + cd = p. \tag{8}$$

Az ismeretlenek és az egyenletek számát úgy csökkenthetjük, hogy az egyik egyenletből kifejezünk egy alkalmas kifejezést, és behelyettesítjük a másik egyenletbe. Hogy mindez még kényelmesebb legyen, először csak modulo p fogunk számolni.

A második egyenlet szerint $ab \equiv -cd \pmod p$. Szorozzuk meg a (7) egyenletet b^2-tel, és helyettesítsünk be ab helyére $(-cd)$-t:

$$0 = b^2(b^2 + bd + d^2 - a^2 + ac - c^2) = b^4 + b^3d + b^2d^2 - (ab)^2 + ab \cdot bc - b^2c^2 \equiv$$
$$\equiv b^4 + b^3d + b^2d^2 - (cd)^2 - cd \cdot bc - b^2c^2 = (b + c)(b - c)(b^2 + bd + d^2) \pmod p.$$

A behelyettesítés nyomán kapott kifejezés három tényező szorzatára bomlik, és ezek egyike éppen a (7) egyenletben szereplő mennyiség.

A kapott kongruencia szerint az utolsó három tényező: $b + c$, $b - c$ és $b^2 + bd + d^2$ valamelyike osztható p-vel, hiszen feltevésünk szerint p prímszám. A $b + c$ és $b - c$ számok pozitívak és kisebbek, mint $ab + cd = p$, ezért nem lehetnek p-vel oszthatók; marad az az eset, hogy $b^2 + bd + d^2$ osztható p-vel. Mivel

$$0 < b^2 + bd + d^2 < ab + ab + cd < 2(ab + cd) = 2p,$$

a $b^2 + bd + d^2$ szám csak úgy lehet p-vel osztható, ha egyenlő vele. Ezzel a következtetéssel az egyenletrendszer a következőképpen alakul:

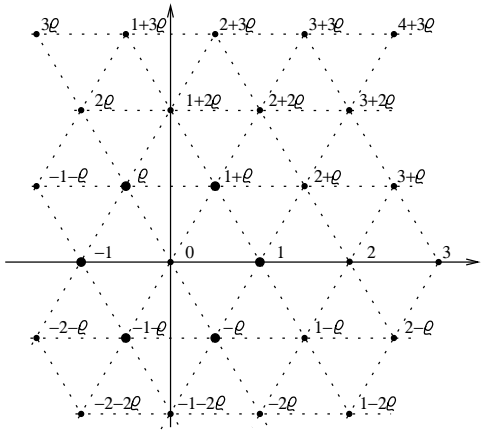
$$a^2 - ac + c^2 = b^2 + bd + d^2 = ab + cd = p. \tag{9}$$

Ebből már nem nehéz ellentmondásra jutni. Ha a (9) egyenletet modulo a vizsgáljuk (az ismeretlenek között az a a legnagyobb), láthatjuk, hogy $c(c - d) = ab + ac - a^2$ osztható a-val. Mivel azonban a és c relatív prímek – másképpen $ab + cd$ nem lenne prímszám – és $0 < c - d < a$, ez nem lehetséges.

2. megoldás az Euler-egészek felől

Aki olvasott már az Euler-egészekről, az a (7) egyenletre nézve azonnal sejtheti, hogy ez a feladat szorosan kapcsolódik hozzájuk.

Legyen ϱ az egyik komplex harmadik egységgyök. Az $x + y\varrho$ alakú komplex számokat, ahol x és y egész számok, *Euler-egészeknek* nevezzük. Az Euler-egészek a komplex számsíkon szabályos háromszögrácsot alkotnak (*1. ábra*).



1. ábra

Ennek a számhalmaznak nagyon sok érdekes és hasznos számelméleti tulajdonsága van. Ezek segítségével bizonyította be annak idején Leonhard Euler a Fermat-sejtést a 3-as kitevőre. Akit a téma részletesebben érdekel, annak *Turán Pál–Gyarmati Edit:* Bevezetés a számelméletbe című jegyzetét ajánljuk. Most csak röviden foglaljuk össze az Euler-egészekkel kapcsolatos, a megoldáshoz szükséges legfontosabb fogalmakat és tételeket.

Az Euler-egészek körében is értelmezzük az összeadást, a kivonást és a szorzást. Ezeket teljesen természetes módon definiáljuk, a szorzásnál figyelembe véve, hogy $\varrho^2 = -\varrho - 1$:

$$(x + y\varrho) \pm (u + v\varrho) = (x \pm u) + (y \pm v)\varrho;$$
$$(x + y\varrho)(u + v\varrho) = xu + (xv + yu)\varrho + yv\varrho^2 = (xu - yv) + (xv + uy - yv)\varrho.$$

Az összeadásnak és a szorzásnak az egész vagy a valós számok esetében megszokott kommutatív, asszociatív és disztributív tulajdonságai az Euler-egészek körében is igazak. Ugyancsak fennállnak a 0 és az 1 számok alapvető tulajdonságai, például bármelyik Euler-egészhez 0-t adva magát a számot kapjuk eredményül, vagy minden Euler-egész 0-szorosa a 0.

Az $\alpha = x + y\varrho$ Euler-egész *konjugáltja* az $\overline{\alpha} = x + y\varrho^2 = (x - y) - y\varrho$ szám.

Egy nagyon fontos mennyiség az Euler-egészek *normája.* Az $\alpha = x + y\varrho$ Euler-egész normáját $N(\alpha)$-val jelöljük és a következőképpen definiáljuk:

$$N(\alpha) = \alpha \cdot \overline{\alpha} = x^2 - xy + y^2.$$

A norma mindig nemnegatív egész szám, és csak a 0 normája 0.

A norma nem más, mint a komplex értelemben vett abszolút érték négyzete. Ebből is következik, hogy szorzat normája a tényezők normáinak szorzata:

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta).$$

Az α Euler-egész *osztója* a β Euler-egésznek, ha létezik olyan γ Euler-egész, amelyre $\alpha\gamma = \beta$. A norma multiplikativitása miatt igaz, hogy ha $\alpha|\beta$, akkor $N(\alpha)|N(\beta)$. (Az utóbbi oszthatóság a racionális egész számok körében értendő.)

Hat olyan Euler-egész van, amelynek a normája 1. Ezeket *egységeknek* nevezzük és az *1. ábrán* kiemeltük. Az egységek minden Euler-egésznek osztói.

Két Euler-egészt *asszociáltnak* nevezünk, ha egymás egységszeresei, vagyis egymásból a 0 körüli, a $60°$ többszörösével történő forgatással kaphatók.

Egy egységtől különböző π Euler-egészt *felbonthatatlannak,* idegen szóval *irreducibilisnek* nevezünk, ha csak az egységekkel és a saját asszociáltjaival osztható.

Egy egységtől és 0-tól különböző π Euler-egészt *prímnek* nevezünk, ha tetszőleges α, β Euler-egészek esetén, ha $\pi|\alpha\beta$, akkor $\pi|\alpha$ vagy $\pi|\beta$. A továbbiakban, hogy megkülönböztessük az Euler-egészek körében prím számokat a valós prímszámoktól, az előbbieket *Euler-prímeknek* fogjuk hívni.

Az Euler-egészek számelméletének legalapvetőbb tételei a következők:

1. A felbonthatatlan Euler-egészek és az Euler-prímek ugyanazok.

2. Az Euler-egészek körében is igaz a számelmélet alaptétele. Minden 0-tól és egységtől különböző Euler-egész az asszociáltságtól eltekintve egyféleképpen írható fel Euler-prímek és egységek szorzataként, azaz két tetszőleges felírásban a megfelelő prímtényezők egymás asszociáltjai.

3. A $3k+2$ alakú prímszámok egyben Euler-prímek is. A $3k+1$ alakú prímszámok felbomlanak két konjugált, egymással nem asszociált Euler-prím szorzatára (pl. $7 = (3 + \varrho)(2 - \varrho)$). A 3 prímtényezős felbontása pedig $3 = -\varrho^2(1 - \varrho)^2$.

A tételekből látható, hogy egy α Euler-egész prímtényezős felbontása és $N(\alpha)$ prímtényezős felbontása között szoros kapcsolat van. Az α minden egyes $3k + 2$ alakú prímtényezőjének négyzete szerepel az $N(\alpha)$ felbontásában, a további prímtényezőknek pedig a normája, ami vagy 3, vagy pedig egy-egy $3k + 1$ alakú prímszám.

Például az $\alpha = 10 + 8\varrho$ Euler-egész prímtényezős felbontása $2 \cdot (2 + \varrho)(3 + \varrho)$, normájáé pedig $N(\alpha) = N(2) \cdot N(2 + \varrho) \cdot N(3 + \varrho) = 2^2 \cdot 3 \cdot 7$.

Megfordítva, $N(\alpha)$ prímtényezős felbontása „majdnem egyértelműen" meghatározza α prímtényezős felbontását. Az $N(\alpha)$ minden $3k + 2$ alakú prímosztója α-nak is prímosztója (feleakkora kitevővel), és $N(\alpha)$ felbontásában minden egyes 3-as tényező az $1 - \varrho$ Euler-prím normája. Az $N(\alpha)$ $3k + 1$ alakú prímosztói is α egy-egy prímosztójának normái, de ez a prímosztó – az asszociáltságtól eltekintve is – kétféle lehet.

Visszatérve a feladathoz, legyen $\alpha = a + c\varrho$ és $\beta = b - d\varrho$. A feltétel szerint $a^2 - ac + c^2 = b^2 + bd + d^2$, azaz $N(\alpha) = N(\beta)$; a bizonyítandó állítás pedig az, hogy $ab + cd$, ami nem más, mint $\alpha\beta = (ab + cd) + (bc + cd - ad)\varrho$ „valós része", nem lehet prímszám.

Mivel $N(\alpha) = N(\beta)$, a két szám Euler-prímtényezős felbontása „majdnem" ugyanaz. A prímosztók egy része közös, a további prímtényezők pedig egymás konjugáltjai a két felbontásban. Formálisan felírva,

$$\alpha = \varepsilon_1 \cdot \pi_1 \dots \pi_k \cdot \mu_1 \dots \mu_l \quad \text{és} \quad \beta = \varepsilon_2 \cdot \pi_1 \dots \pi_k \cdot \overline{\mu}_1 \dots \overline{\mu}_l, \tag{10}$$

ahol $\pi_1, \dots, \pi_k$ és $\mu_1, \dots, \mu_l$ Euler-prímek, ε_1 és ε_2 pedig egységek.

Legyen $\gamma = \pi_1 \cdot \dots \cdot \pi_k$ és $\delta = \mu_1 \cdot \dots \cdot \mu_l$; a fentiek szerint ekkor

$$\alpha = \varepsilon_1 \gamma \delta \quad \text{és} \quad \beta = \varepsilon_2 \gamma \overline{\delta}.$$

(Előfordulhat, hogy a két felbontásban csak közös vagy csak konjugált prímtényezők szerepelnek; ezekben az esetekben $\gamma = 1$, illetve $\delta = 1$.)

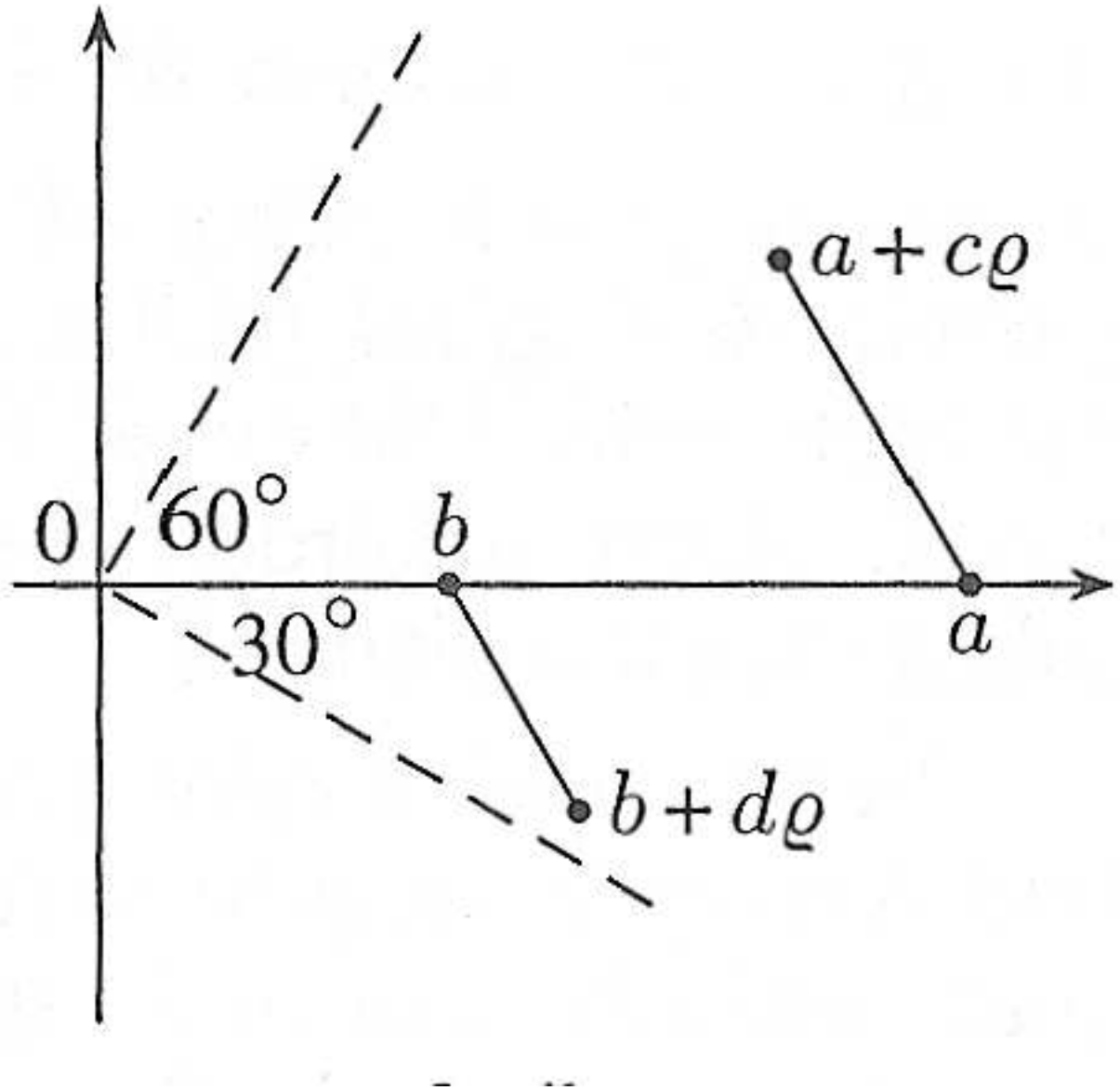
Vizsgáljuk most az

$$\alpha\beta = (ab + cd) + (bc + cd - ad)\varrho = \varepsilon_1 \varepsilon_2 \gamma^2 \cdot N(\delta) \tag{11}$$

számot. Ez a szám osztható $N(\delta)$-val; ebből következik, hogy $ab + cd$ és $bc + cd - ad$ is osztható $N(\delta)$-val. Már csak az hiányzik a bizonyítás befejezéséhez, hogy sem $N(\delta) = 1$, sem $ab + cd = N(\delta)$ nem lehetséges.

Ha $N(\delta) = 1$, azaz $\delta = 1$, akkor α és β asszociáltak, vagyis 0 körüli, valahányszor 60°-os elforgatottjai egymásnak. Azt, hogy az elforgatás pontosan hányszor 60°-os, az α és β argumentumának vizsgálatával dönthető el.

Az $a > b > c > d > 0$ feltételből következik, hogy α argumentuma 0° és 60° között, β argumentuma pedig −30° és 0° között van (*2. ábra*). A két szám argumentumának különbsége tehát 0 és 90° közé esik, az elforgatás szöge pontosan 60°, azaz $\alpha = (1 + \varrho)\beta$.



2. ábra

Ebben az esetben viszont

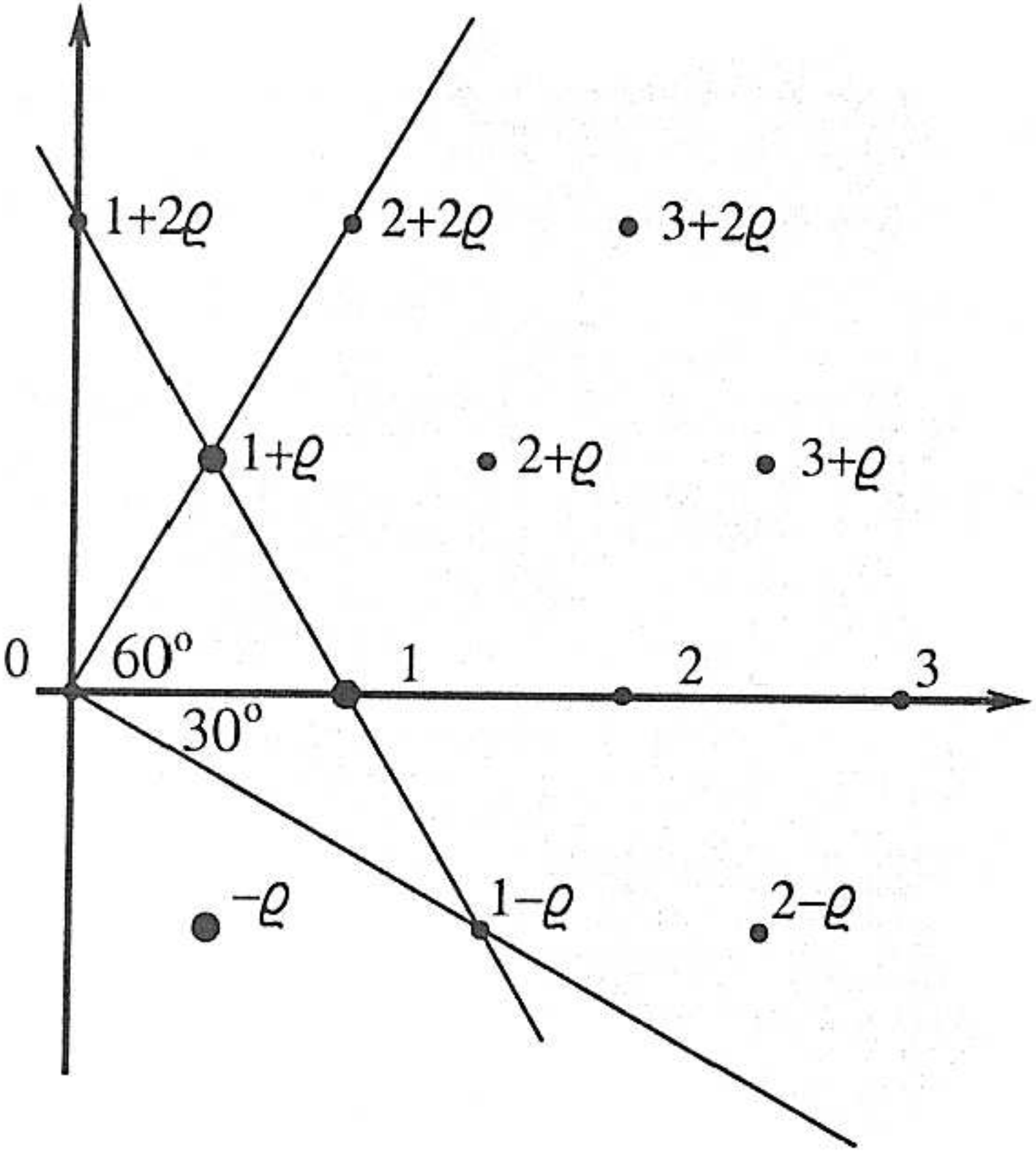
$$\alpha = a + c\varrho = (1 + \varrho)(b - d\varrho) = (b + d) + b\varrho,$$

ami nem lehetséges, mert $b > c$. Az $N(\delta) = 1$ feltevés tehát ellentmondásra vezet.

Ha $ab + cd = N(\delta)$, akkor a (11) egyenletet $N(\delta)$-val osztva,

$$\frac{\alpha\beta}{N(\delta)} = \frac{ab + cd}{N(\delta)} + \frac{ad + bc - cd}{N(\delta)} \cdot \varrho = \varepsilon_1\varepsilon_2 \cdot \gamma^2.$$

Ez a szám, mint a jobb oldal mutatja, egy Euler-egész. Az argumentuma α és β argumentumának öszege, tehát -30° és 60° közé esik, a „valós része" pedig a feltevés szerint $\dfrac{ab + cd}{N(\delta)} = 1$. Az egyetlen ilyen Euler-egész az 1 (*3. ábra*), tehát $\varepsilon_1\varepsilon_2\gamma^2 = 1$ és $\alpha\beta = N(\delta)$.



3. ábra

Az α és β számok szorzata tehát az $N(\delta)$ valós pozitív szám. Mivel $N(\alpha) = N(\beta)$, ebből következik, hogy a két szám egymás konjugáltja. Ekkor azonban

$$\alpha = a + c\varrho = \overline{\beta} = \overline{b - d\varrho} = b + d(1 + \varrho) = (b + d) + d\varrho,$$

ami nem lehetséges, mert $c > d$. Tehát az $ab + cd = N(\delta)$ feltevés is ellentmondásra vezet. Ezzel az állítást igazoltuk.

A második megoldás nem csupán bebizonyítja a feladat állítását, hanem egy eljárást is ad olyan a, b, c, d számnégyesek keresésére, amelyekre $a > b > c > d$ és $a^2 - ac + c^2 = b^2 + bd + d^2$. Csupán megfelelő argumentumú γ és δ Euler-egészeket kell választanunk.

Például az

$$\alpha = a + c\varrho = (4 + \varrho)(3 + \varrho) = 11 + 6\varrho, \quad \beta = b - d\varrho = (4 + \varrho)\overline{(3 + \varrho)} = 9 - \varrho$$

választással $a = 11$, $b = 9$, $c = 6$ és $d = 1$, továbbá $a^2 - ac + c^2 = b^2 + bd + d^2 = 91$. (Természetesen $ab + cd = 105$ nem prím.)

Kós Géza