Az érettségi vizsgára előkészülő tanulók figyelmébe!

EGYENLETEK ÉS EGYENLETRENDSZEREK
MEGOLDÁSA A Z_n HALMAZON

3. Az $\begin{cases} \hat{a}_1 x + \hat{b}_1 y = \hat{c}_1 \\ \hat{a}_2 x + \hat{b}_2 y = \hat{c}_2 \end{cases}$ egyenletrendszer megoldása a Z_n halmazon (**1. rész**)

Ebben és a következő két részben az elsőfokú kétismeretlenes egyenletnek a Z_n halmazon történő megoldásával foglalkozunk. Ez a látszatra egyszerűnek tűnő témakör a Z_n halmazon sokkal több változatosságot és meglepetést tartogat, mint az R halmazon. Éppen ezért tanulságosnak és szükségesnek látjuk párhuzamba állítani az R illetve Z_n halmazokon való megoldási eljárásokat és módszereket, majd részletezni az újonnan adódó sajátosságokat.

1. Az elsőfokú kétismeretlenes egyenletrendszer megoldási módszerei az R halmazon

A tanulók már a kisebb osztályokban (akár részben álcázottan) megismerkednek az ilyen egyenleteken alapuló feladatokkal és az egyenletrendszerek megoldási módszereivel, majd ezt követően a líceumi osztályokban tovább bővülnek az idevágó ismereteik.

Nézzük hát át a megoldási módszerek fontosabb mozzanatait:

a) A helyettesítési módszer. A módszer lényege az, hogy valamelyik egyenletből *kifejezzük* valamelyik ismeretlent (célszerű a legkönnyebben kifejezhető ismeretlent kifejezni, vagyis azt amelyiknek az együtthatója 1 vagy -1, vagy nem nagy szám, stb.). Amikor az együtthatók egyike sem 1 vagy -1, ekkor a *„kifejezési művelet”* abból áll, hogy a másik ismeretlent tartalmazó tagot *átvisszük* az ellentétes oldalra és *végigosztjuk* az egyenletet a kifejezendő ismeretlen együtthatójával. A kifejezett ismeretlent behelyettesítve a másik egyenletbe, egy 1 ismeretlenes elsőfokú egyenletet kapunk, amit megoldunk, és a kapott megoldást visszaírjuk oda, ahol kifejeztük a előző ismeretlent, innen kapjuk meg a második ismeretlen értékét.

b) A kiküszöbölés módszer. A módszer lényege az, hogy úgy *szorozzuk be* egyik, vagy akár mindkét egyenlet mindkét oldalát ugyanazzal a nullától különböző számmal, hogy a két egyenlet megfelelő oldalait *kivonva egymásból*, az egyik ismeretlen együtthatója 0 legyen, így meghatározható a másik ismeretlen. Ugyanezt megismételjük úgy, hogy a másik ismeretlent küszöböljük ki.

c) A kiküszöbölés és a helyettesítés kombinált módszere. A kiküszöbölés módszerével kiküszöböljük a könnyebben kiküszöbölhető ismeretlent, így megkapjuk az egyik ismeretlen értékét, amit visszahelyettesítünk valamelyik egyenletbe és megoldva a kapott egyismeretlenes egyenletet, megkapjuk a másik ismeretlen értékét is (abba az egyenletbe tanácsos visszahelyettesíteni, ahonnan az illető ismeretlen *kifejezése* egyszerűbb).

d) Különféle más eljárások. Ezek nagyon változatosak lehetnek, a végső céljuk az, hogy a 2 egyenletből egy olyan harmadik egyenletet *származtassunk*, amiből könnyebben *kifejezhető* valamelyik ismeretlen. Például a $2x+3y=1$, $3x+2y=4$ egyenlet esetén ha összeadjuk az egyenletek megfelelő oldalain levő kifejezéseket, és *végigosztunk* 5-tel, akkor az $x+y=1$ egyenletet kapjuk, ahonnan bármelyik ismeretlen könnyebben *kifejezhető*. De ha az összeadás helyett a második egyenletből kivonjuk az első egyenlet megfelelő oldalait, akkor $x-y=3$ adódik, és innen is könnyebben *fejezhető ki* bármelyik ismeretlen. Az így *származtatott* egyenlet az eredeti egyenletek bármelyikével társítva gyorsabban megoldható az eredeti egyenletrendszer.

e) A determinánsok módszere. Ezt az algoritmikus jellegű módszert a tanulók a XI. osztályban tanulják, és a lényege az, hogy a számolások csak az együtthatókkal történnek, így nem szükségesek az előbbiekben leírt *kifejezési* és *behelyettesítési* műveletek. A módszert a továbbiakban részletesen ismertetjük, és ugyanakkor előre kihangsúlyozzuk, hogy ez a módszer (és ennek keretén belül az ú.n. **Cramer-szabály**) éppen a kiküszöbölés módszerén alapszik.

Az előző rövid bemutatást legalább a következő két okból láttuk szükségesnek:
1) A Z_n halmazon történő megoldási módszereket megpróbáljuk az előző módszerekhez igazítani és megvizsgáljuk, hogy ezek mikor alkalmazhatók Z_n halmazon is, ugyanis az R-en való alkalmazásukkal ellentétben, a Z_n–n nem mindig alkalmazhatók eredményesen!
2) Az előző leírásban szereplő néhány dűlt betűs szó, mint például: *kifejezzük, átvisszük, beszorozzuk, mindkét oldalt végigosztjuk*, *kiküszöböljük* stb. teljesen másképpen kell értenünk és tárgyalnunk a Z_n halmazon, mint az R-en. Hamarosan meglátjuk, hogy miért, és ekkor jobban átlátható, hogy a tárgyalt témakör jóval komplexebb mint ahogyan első látásra tűnhet.

Mindezek jobb megértése és elmélyítése végett, szükségünk van Z_n halmazon alaposabban áttanulmányozni az egyenlőségek *végigosztásának* (egyszerűsítésének) és *beszorzásának* a részleteit. Ezáltal pedig fényt derítünk arra, hogy az egyenletek megoldása során mikor *veszíthetünk el gyököket*, illetve mikor *adódnak idegen gyökök*, és ilyen esetekben mit kell tennünk.

2. Egyszerűsítési és beszorzási szabályok a (Z_n, +, ·) struktúrában

Tekintsük a Z_{15} halmazon a $\hat{20}=\hat{80}$ igaz egyenlőséget, és figyeljük meg a következőket:

1) A $\hat{20}=\hat{80}\Leftrightarrow\hat{5}\cdot\hat{4}=\hat{20}\cdot\hat{4}$ és ha az egyenlőség mindkét oldalát végigosztjuk a $\hat{4}$-pal, akkor az $\hat{5}=\hat{20}$ egyenlőséget kapjuk, ami a Z_{15}-ben valóban igaz állítás.

2) A $\hat{20}=\hat{80}\Leftrightarrow\hat{4}\cdot\hat{5}=\hat{16}\cdot\hat{5}$ és ha az egyenlőség mindkét oldalát végigosztjuk az $\hat{5}$-pal, akkor a $\hat{4}=\hat{16}$ egyenlőséget kapjuk, ami a Z_{15}-ben egy hamis állítás.

És most végezzük el a fordított irányú műveletet is, vagyis:

3) Az $\hat{5}=\hat{20}$ nyilvánvalóan igaz állítás a Z_{15}-ben. Ha most az egyenlőség mindkét oldalát megszorozzuk $\hat{4}$-pal, akkor a $\hat{20}=\hat{80}$ állítást kapjuk, ami Z_{15}-ben nyilvánvalóan igaz állítás.

4) A $\hat{4}=\hat{16}$ egyenlőség a Z_{15}-ben nyilvánvalóan hamis állítás, ellenben ha az egyenlőség mindkét oldalát megszorozzuk $\hat{5}$-pal, akkor a $\hat{20}=\hat{80}$ állítást kapjuk, ami Z_{15}-ben nyilvánvalóan igaz állítás, ellenben ez ellentmond azon logikai alaptörvénynek, miszerint hamis állításból helyes logikai következtetésekkel nem kaphatunk igaz állítást.

Nos, vajon miért történt mindez így, és mi ennek az oka?

Emlékezzünk csak vissza, hogy az 1. részben írtunk a zérusosztókról! Nos, éppen ebben rejlik a dolgok lényege. Az 1) és 3) esetben (4, 15)=1 ezért az 1. részben leírt eredmények alapján $\hat{4}$ nem zérusosztó a Z_{15}-ben. Ellenben, a 2) és 4) esetben (5, 15)= 5, vagyis $\hat{5}$ éppen zérusosztó a Z_{15}-ben (tehát igaz pl., hogy $\hat{5}\cdot\hat{3}=\hat{0}$ anélkül, hogy $\hat{5}$ vagy $\hat{3}$ valamelyike is $\hat{0}$ lenne a Z_{15}-ben). Tehát máris körvonalazódik az a fontos megállapítás miszerint: a Z_n-ben csak akkor oszthatjuk végig illetve szorozhatjuk be egy egyenlőség mindkét oldalát egy $\hat{a}\in Z_n$, $\hat{0}$-tól különböző számmal, ha $\hat{a}$ nem zérusosztó a Z_n-ben. Ezen fontos megállapításunkat a következő tételben részletesebben pontosítjuk:

4. tétel. Legyen a, b∈ N és k, m, n∈ N^*.

a) A Z_n-ben ha $\hat{a}\cdot\hat{k}=\hat{b}\cdot\hat{k}$, akkor $\hat{a}=\hat{b}$ igaz a Z_r-ben, ahol $r=\dfrac{n}{(k,n)}$

b) A Z_n-ben ha $\hat{a}\cdot\hat{k}=\hat{b}\cdot\hat{k}$ és (k, n)= 1, akkor $\hat{a}=\hat{b}$ igaz a Z_n-ben

c) A Z_n-ben ha $\hat{a}=\hat{b}$, akkor $\hat{a}\cdot\hat{k}=\hat{b}\cdot\hat{k}$ is igaz a Z_n-ben

d) Ha $\hat{a}\cdot\hat{m}=\hat{b}\cdot\hat{m}$ igaz a $Z_{m\cdot n}$-ben, akkor $\hat{a}=\hat{b}$ igaz a Z_n-ben

e) Ha $\hat{a}=\hat{b}$ igaz a Z_n-ben, akkor $\hat{a}\cdot\hat{m}=\hat{b}\cdot\hat{m}$ is igaz a $Z_{m\cdot n}$-ben

Bizonyítás: **a)** Legyen d= (k, n), így k=d·k_1 és n=d·n_1 ahol (k_1, n_1)=1. Az $\hat{a}\cdot\hat{k}=\hat{b}\cdot\hat{k}$ egyenlőség alapján a·k= b·k+ p·n vagyis n | (a·k-b·k) ⇔ d·n_1 | k·(a-b) ⇔ d·n_1 | d·k_1·(a-b) ezért n_1 | k_1·(a-b), és mivel (k_1, n_1)=1, így n_1 |(a-b) vagyis $\hat{a}=\hat{b}$ igaz a Z_r-ben, ahol d= (k, n), n=d·n_1 és $n_1=r=\dfrac{n}{(k,n)}$.

b) Azonnal következik az **a)**-ból, hiszen ekkor a (k, n)= 1 alapján $n_1=r=\dfrac{n}{(k,n)}=n$.

c) Az $\hat{a}=\hat{b}$ egyenlőség alapján n | (a-b) ⇔ n | k·(a-b) ⇔ n | (a·k-b·k) vagyis az $\hat{a}\cdot\hat{k}=\hat{b}\cdot\hat{k}$ egyenlőség is igaz a Z_n-ben.

d) Az $\hat{a}\cdot\hat{m}=\hat{b}\cdot\hat{m}$ egyenlőség igaz a $Z_{m\cdot n}$-ben , ezért a·m=b·m+q·m·n, ahonnan a= b+ q·n tehát az $\hat{a}=\hat{b}$ egyenlőség igaz a Z_n-ben.

e) Az $\hat{a}=\hat{b}$ egyenlőség igaz a Z_n-ben, ezért a= b+ q·n így a·m=b·m+q·m·n, tehát az $\hat{a}=\hat{b}$ egyenlőség igaz a $Z_{m\cdot n}$-ben.

Természetesen, még sok más tulajdonság megfogalmazható és bizonyítható, de a továbbiakban csupán ezekre van szükségünk. Az elsőfokú egyismeretlenes egyenletek megoldására vonatkozóan figyeljük meg a következőket:

A $\hat{2}\cdot x=\hat{4}$ egyenletnek a Z_6-ban 2 megoldása van, éspedig x=$\hat{2}$ és x= $\hat{4}$. Ellenben, ha az egyenlet mindkét oldalát végigosztjuk $\hat{2}$-pal, akkor az x= $\hat{2}$ egyenletnek sem a Z_6-ban sem a $Z_r=Z_3$-ban nincs 2 megoldása, egyetlen megoldás az x=$\hat{1}$. Ellenben a $\hat{2}\cdot x=\hat{4}$ egyenletnek a Z_7-ben x= $\hat{2}$ az egyetlen megoldása , és a $\hat{2}$-pal végigosztott egyenletnek is x= $\hat{2}$ a Z_7-ben megmarad egyetlen megoldásnak. Mindezekre magyarázatot a következő tételek adnak:

5. tétel. Legyen k, a, b ∈ N, A= k·a≠ 0, B= k· b és (A, n)= 1. Akkor mint az $\hat{A}\cdot x=\hat{B}$ egyenletnek, mint a $\hat{k}$-pal végigosztott $\hat{a}\cdot x=\hat{b}$ „egyszerűsített” egyenletnek egy- egy megoldása van a Z_n-ben.

Bizonyítás: Először is lássuk be, hogy ha (A, n)=1 ⇔ (k·a, n)= 1, akkor (a, n)= 1 is igaz. Valóban, ha feltételeznénk az ellenkezőjét vagyis, hogy (a, n)= d ≠ 1, akkor a= d·a_1 és n=d·n_1 ahol $(a_1,n_1)=1$, tehát 1=(k·a, n)=(k·d·a_1, d·n_1) = d· (k·a_1, n_1) ellentmondáshoz jutunk, hiszen d ≠ 1. Így hát az 1. részben bizonyított **1. tétel** alapján, mivel 1= (A, n)= (a, n) osztja a szabad tagot, ezért mind a két egyenletnek pontosan 1-1 megoldása van a Z_n-ben.

Ezzel beláttuk, hogy ha a Z_n-ben egy $\hat{p}\cdot x=\hat{q}$ egyenlet mindkét oldalát beszorozzuk, vagy ha elosztjuk ugyanazzal a $\hat{k}$-pal amelyre (k, n)=1, akkor nem hozunk be idegen gyököket, sem gyököket nem veszítünk el.

6. tétel. Legyen k, a, b ∈N, A= k·a ≠0, B= k· b és (A, n)= k≠1. Ekkor az $\hat{A}\cdot x=\hat{B}$ egyenletnek a Z_n-ben pontosan *k* megoldása van, és a $\hat{k}$-pal végigosztott $\hat{a}\cdot x=\hat{b}$ „egyszerűsített” egyenletnek pedig pontosan *egy* megoldása van a $Z_{\frac{n}{k}}$-ban.

Bizonyítás: Ugyancsak az 1. részben bizonyított **1.tétel** alapján az $\hat{A}\cdot x=\hat{B}$ egyenletnek d= (A, n) számú megoldása van Z_n-ben és ezúttal (A, n)= k$\neq$1 adott. Továbbá az A= k·a $\neq 0$ feltétel alapján k | n is igaz, ezért $\frac{n}{k}\in N^*$, és így k= (A, n)= (k· a, k· $\frac{n}{k}$)=k· (a, $\frac{n}{k}$) vagyis (a, $\frac{n}{k}$) =1. Tehát az $\hat{a}\cdot x=\hat{b}$ egyenletnek az 1. rész **2. tétele** szerint a $Z_{\frac{n}{k}}$-ban valóban *egy* megoldása van. A k= 1 esetben visszakapjuk az **5. tételt**.

Az elsőfokú kétismeretlenes egyenletek esetén, a 2. részben bizonyított **2.** és **3.tétel** figyeljük meg a következőket:

A $\hat{4}x+\hat{4}y=\hat{2}$ egyenletnek a Z_5-ben a (4, 4, 5)= 1 alapján 1·5= 5 megoldása van, a $\hat{2}$-pal „végigosztott" $\hat{2}x+\hat{2}y=\hat{1}$ egyenletnek a Z_5-ben a (2, 2, 5)= 1 alapján ugyancsak 1·5=5 megoldása van. Ugyancsak a $\hat{4}x+\hat{4}y=\hat{2}$ egyenletnek a Z_6-ban a (4, 4, 6)= 2 alapján 2·6= 12 megoldása van továbbá a $\hat{2}$-pal „végigosztott" $\hat{2}x+\hat{2}y=\hat{1}$ egyenletnek a (2, 2, 6)=2 | 1 hamis állítás alapján nincs megoldása a Z_6-ban, ellenben a (2, 2, 1)= 1 | 1 igaz állítás alapján 1·3=3 megoldása van a Z_3-ban. Mindezekre magyarázatot a következő tételek adnak:

7. tétel. Legyen k, a, b $\in$N* , A= k·a, B= k·b, C=k·c és (A, B, n)= 1. Akkor mint az $\hat{A}x+\hat{B}y=\hat{C}$ egyenletnek, mint a $\hat{k}$-pal végigosztott $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ „egyszerűsített" egyenletek mindegyikének *n* számú megoldása van a Z_n-ben.

Bizonyítás: Először is lássuk be, hogy ha (A, B, n)=1 $\Leftrightarrow$ (k·a, k·b, n)= 1, akkor (a, b, n)= 1 is igaz. Valóban, ha feltételeznénk az ellenkezőjét vagyis, hogy (a, b, n)= d $\neq$ 1, akkor az a= d·a_1, b= d·$b_1$és n=d·n_1 ahol $(a_1,b_1,n_1)=1$ összefüggések alapján felírható, hogy 1=(k· a, k· b, n)= =(k·d·a_1, k·d·b_1, d·n_1) =d· (k·a_1, k·b_1, n_1) ami ellentmondás, hiszen d $\neq$ 1. Így hát a 2. részben bizonyított **2.** és **3.tétel** alapján, mivel 1= (A, B, n)= (a, b, n) osztja a szabad tagot, ezért mind a két egyenletnek *n* számú megoldása van a Z_n-ben.

Ezzel beláttuk, hogy ha a Z_n-ben egy $\hat{p}\cdot x+\hat{q}\cdot y=\hat{r}$ egyenlet mindkét oldalát beszorozzuk, vagy ha elosztjuk ugyanazzal a $\hat{k}$-pal amelyre (k, n)=1, akkor nem hozunk be idegen gyököket, sem gyököket nem veszítünk el.

8. tétel. Legyen k, a, b $\in$N* , A= k·a, B= k·b, C=k·c és (A, B, n)= k$\neq$1. Ekkor az $\hat{A}x+\hat{B}y=\hat{C}$ egyenletnek a Z_n-ben pontosan k·n megoldása van és a $\hat{k}$-pal végigosztott $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ „egyszerűsített" egyenletnek pedig pontosan $\frac{n}{k}$ megoldása van a $Z_{\frac{n}{k}}$-ban.

Bizonyítás: Ugyancsak a 2. részben bizonyított **2.** és **3.tétel** alapján az $\hat{A}x+\hat{B}y=\hat{C}$ egyenletnek a Z_n-ben (A, B, n)= k számú megoldása van. Ugyanakkor a tétel feltételei mellett k | n igaz állítás, így $\frac{n}{k}\in N^*$, így a k= (A, B, n)= (k· a, k· b, k· $\frac{n}{k}$)=k· (a, b, $\frac{n}{k}$) alapján (a, b, $\frac{n}{k}$)=1, és ugyancsak a **2.** és **3.tétel** alapján az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ egyenletnek (a, b, $\frac{n}{k}$)· $\frac{n}{k}=\frac{n}{k}$ számú megoldása van a $Z_{\frac{n}{k}}$-ban. A k=1 esetben visszakapjuk a 7**. tételt**.

Belátható, hogy amennyiben a **6. tételben** az (A, n)=k illetve az ennek megfelelő analóg **8. tételben** az (A, B, n)= k feltételeket az (A, n)= d $\neq$k, illetve (A, B, n)= d $\neq$k kikötésekre cserélnénk ki, úgy jóval komplexebb helyzettel találnánk szembe magunkat, ellenben főleg a terjedelmi okok miatt ezektől eltekintünk, és az ilyen irányú további tanulmányozásokat az érdeklődő Olvasókra bízzuk.

Befejezésül kihangsúlyozzuk, hogy erre a hosszas kitérőre a következők miatt volt szükség: bármilyen módszerrel is oldjuk meg a Z_n halmazon az $\begin{cases} \hat{a}_1 x + \hat{b}_1 y = \hat{c}_1 \\ \hat{a}_2 x + \hat{b}_2 y = \hat{c}_2 \end{cases}$ alakú egyenletrendszert, mindenképpen eljutunk (még a determinánsokkal is) a $\hat{p} \cdot x = \hat{q}$ illetve $\hat{r} \cdot y = \hat{s}$ alakú egyenletekhez ellenben amíg ezekhez eljutunk, azelőtt az adott két $\hat{a} \cdot x + \hat{b} \cdot y = \hat{c}$ alakú egyenletekkel olyan algebrai műveleteket kell végeznünk, amelyek során megoldásokat veszíthetünk el, illetve idegen megoldásokat kaphatunk továbbá a megoldások száma is megváltozhat.

A következő részekben feladatokkal szemléltetve a helyettesítési módszer alkalmazhatóságát, előnyeit, hátrányait, lehetőségeit és hatékonyságát vizsgáljuk és szükség esetén a különféle eljárásokon alapuló megoldási módszereket is „bevetünk”. És miután meggyőződtünk arról, hogy melyek a módszer nehézségei és korlátai, azután a kiküszöbölés módszeréhez, majd az erre alapuló determinánsok módszeréhez folyamodunk amivel az egyenletrendszerek átfogóbb, áttekinthetőbb és rendszerezett megoldási módszerét mutatjuk be.