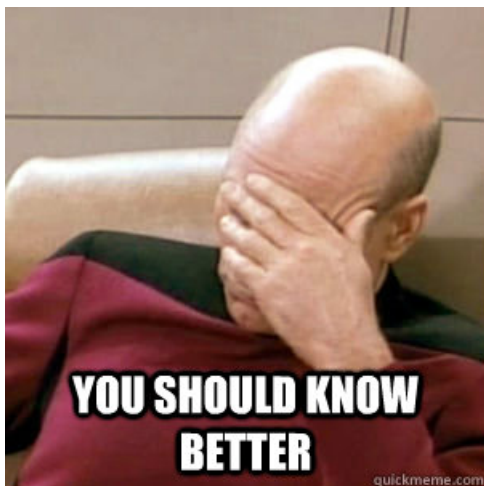


Algebra és számelmélet előadás

Waldhauser Tamás
2016. szeptember 8.

Tematika

Komplex számok, kanonikus és trigonometrikus alak. Moivre-képlet, gyökvonás, egységgyökök, egységgyök rendje, primitív egységgyökök. Harmad- és negyedfokú egyenletek, az algebra alaptétele (ismertetés). Teljes és redukált maradékrendszerek, az Euler-féle ϕ függvény, Euler–Fermat-tétel, rend modulo m , primitív gyökök, index. Négyzetes maradékok, Legendre-szimbólum. Titkosírások, nevezetes számelméleti problémák (ismertetés). A gyűrű, az integritástartomány és a test fogalma, nevezetes példák (számgyűrűk és számtestek, maradékosztály-gyűrűk és maradékosztálytestek, mátrixgyűrűk). A polinom fogalma, test feletti polinomgyűrű. Oszthatóság, maradékosztás, lko és lkkt, euklideszi algoritmus, kétismeretlenes lineáris diofantoszi egyenlet, kongruencia, maradékosztályok, maradékosztály-gyűrű, lineáris kongruencia, multiplikatív inverz mod f . Polinom és polinomfüggvény, Lagrange-interpoláció, polinomok (többszörös) gyökei, Bézout tétele, (iterált) Horner-módszer. Irreducibilis polinomok, egyértelmű irreducibilis faktorizáció. Viète-formulák, irreducibilis faktorizáció a komplex, valós és racionális számtest fölött, Schönemann–Eisenstein-tétel, Rolle-tétel. Polinomgyűrű faktorteste mint „egyszerű algebrai bővítés”, véges testek konstrukciója. Derivált, polinomok közös, ill. többszörös gyökei. Véges halmaz permutációi, a szimmetrikus csoport. Ciklusfelbontás, hatványozás, rend. Előállítás transzpozíciók szorzataként, páros és páratlan permutációk, az alternáló csoport. Permutációs játékok (ismertetés). A csoport, mint absztrakt struktúra, művelettáblázat, izomorfia, izomorfizmus. Nevezetes példák: számok, (redukált) maradékosztályok, permutációk, mátrixok, transzformációk csoportjai, lineáris csoportok, diédercsoport, kvaterniócsoport. Hatványozás, elem rendje, ciklikus csoport és részcsoporthat. Részcsoport, generálás. Mellékosztályok, Lagrange tétele. Alkalmazás összeszámlálási feladatokra (ismertetés).





1. nevezetes szögek szögfüggvényei oda-vissza
2. csoport, gyűrű és test fogalma, nevezetes példák
3. legnagyobb közös osztó fogalma, kiszámítása euklideszi algoritmussal
4. kétismeretlenes lineáris diofantoszi egyenlet megoldása euklideszi algoritmussal
5. a modulo m kongruenciareláció fogalma és tulajdonságai
6. lineáris kongruencia megoldása euklideszi algoritmussal
7. számolás \mathbb{Z}_m -ben, különös tekintettel a multiplikatív inverzre
8. polinomok maradékos osztása
9. permutációkkal való számolás, idegen ciklusokra való felbontás
10. gondolkozni, kérdezni, kételkedni

Követelmények

1. Házi feladatok gyakorlatra

háromfokozatú értékelés:

●		★
---	--	---

2. Elektronikus tesztek

háromfokozatú értékelés:

●		★
---	--	---

3. Házi feladatok előadásra

háromfokozatú értékelés:

●		★
---	--	---

4. Szorgalmi feladatok gyakorlatra

négyfokozatú értékelés:

●		★	★★
---	--	---	----

5. Dolgozatok a gyakorlaton

négyfokozatú értékelés:

●		★	★★
---	--	---	----

6. Dolgozat az előadáson

négyfokozatú értékelés:

●		★	★★
---	--	---	----

7. Szóbeli vizsga

háromfokozatú értékelés:

●		★
---	--	---

Követelmények

1. Házi feladatok gyakorlatra

- ▶ rutinfeladatok
- ▶ ellenőrizni, olvashatóan, szabatosan, igényesen leírni!
- ▶ hetente 3 feladatot kell beadni (legalább 10 alkalom lesz)
- ▶ feladatonként 2 pont, összesen 60 pont
- ▶ értékelés:

0 – 39	→	●
40 – 49	→	
50 – 60	→	*

2. Elektronikus tesztek

- ▶ rutinfeladatok
- ▶ <http://www.math.u-szeged.hu/~hartm/practmath/mpract.html>
- ▶ 12 feladat, (majdnem) korlátlan számú próbálkozási lehetőség
- ▶ feladatonként 1 pont, mindegyiket 5-ször kell jól megoldani, összesen 60 pont
- ▶ értékelés:

0 – 39	→	●
40 – 49	→	
50 – 60	→	*

3. Házi feladatok előadásra

- ▶ bizonyítások, számítógépes kísérletek, ???
- ▶ ellenőrizni, olvashatóan, szabatosan, igényesen leírni!
- ▶ emailben kell beadni (lehet szkenn is): `twaldha@math.u-szeged.hu`
- ▶ 8 feladat (legalább)
- ▶ feladatonként 2 pont, összesen 16 pont
- ▶ értékelés:

0 – 7	→	●
8 – 11	→	
12 – 16	→	★

4. Szorgalmi feladatok gyakorlatra

- ▶ érdekesebb, szebb, nehezebb feladatok
- ▶ ellenőrizni, olvashatóan, szabatosan, igényesen leírni!
- ▶ hetente 1 feladatot lehet írásban beadni (legalább 10 alkalom lesz)
- ▶ feladatonként 2 pont, összesen 20 pont
- ▶ értékelés:

0 – 0	→	●
1 – 5	→	
6 – 14	→	★
15 – 20	→	★★

Követelmények

5. Dolgozatok a gyakorlaton

- ▶ rutin- és nehezebb feladatok is
- ▶ három dolgozat: október 10, november 3, december 5
- ▶ egyiket lehet pótolni/javítani
- ▶ dolgozatonként 20 pont, összesen 60 pont
- ▶ értékelés:

0 – 23	→	●
24 – 35	→	
36 – 47	→	★
48 – 60	→	★★

6. Dolgozat az előadáson

- ▶ elméleti(bb) feladatok, egyszerűbb bizonyítások, ???
- ▶ egy dolgozat: december 8
- ▶ két javítási lehetőség a vizsgaidőszakban
- ▶ összesen 60 pont
- ▶ értékelés:

0 – 23	→	●
24 – 35	→	
36 – 47	→	★
48 – 60	→	★★

7. Szóbeli vizsga

- ▶ bizonyítani kell!
- ▶ érteni kell!
- ▶ értékelés:

: -(→ ●

: -| →

: -) → ★



A végső osztályzatot a csillagok számának fele adja (felfelé kerekítve)

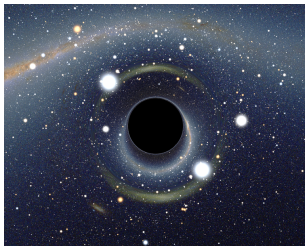
7. Szóbeli vizsga

- ▶ bizonyítani kell!
- ▶ érteni kell!
- ▶ értékelés:

: -(→ ●

: -| →

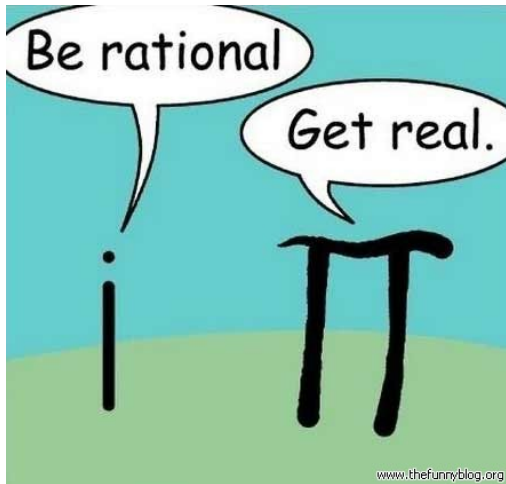
: -) → ★



A végső osztályzatot a csillagok számának fele adja (felfelé kerekítve), de a fekete lyuk mindent elnyel.

1. Komplex számok

Kanonikus alak, konjugált, abszolút érték, komplex számsík



A komplex számok definíciója

1.1. Definíció.

A valós számokból álló számpárokat *komplex számoknak* nevezzük.

A komplex számok halmazát \mathbb{C} jelöli, tehát $\mathbb{C} = \mathbb{R} \times \mathbb{R}$.

Az (a, b) és (c, d) komplex számok *összegét* és *szorzatát* a következőképpen értelmezzük:

$$(a, b) + (c, d) = (a + c, b + d);$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

A komplex számok teste

1.2. Tétel.

A komplex számok testet alkotnak.

Bizonyítás.

A következőket kell(ene) ellenőrizni:

0. a műveletek értelmezettek a $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ halmazon;
1. az összeadás asszociatív;
2. az összeadás kommutatív;
3. létezik additív egységelem: $(0, 0)$;
4. minden elemnek létezik additív inverze: (a, b) additív inverze $(-a, -b)$;
5. a szorzás asszociatív: egyszerű de hosszadalmas számolás;
6. a szorzás kommutatív;
7. létezik multiplikatív egységelem: $(1, 0)$;
8. minden nemzéró elemnek létezik multiplikatív inverze: HF;
9. a szorzás disztributív az összeadásra:

$$(a, b) \cdot ((c, d) + (e, f)) = \dots = (ac + ae - bd - bf, ad + af + bc + be)$$

$$(a, b) \cdot (c, d) + (a, b) \cdot (e, f) = \dots = (ac - bd + ae - bf, ad + bc + af + be) \quad \square$$

Első házi feladat az előadásra

Bizonyítsa be, hogy ha $u = (a, b) \in \mathbb{C}$ és $u \neq (0, 0)$, akkor létezik egy olyan egyértelműen meghatározott $u^* = (x, y)$ komplex szám, amelyre $u \cdot u^* = (1, 0)$.

- ▶ szabatosan, igényesen, értelmes magyar mondatokban leírni
- ▶ beküldendő emailben: `twaldha@math.u-szeged.hu`
- ▶ pdf fájl legyen (lehet szkennelt is)
- ▶ fájlnev: `EHA-eahf1.pdf` (például `WATHAAS-eahf1.pdf`)
- ▶ határidő: szeptember 21, reggel 8 óra

A valós számok beágyazása

1.3. Állítás.

Minden $a, b \in \mathbb{R}$ esetén

$$(a, 0) + (b, 0) = (a + b, 0) \quad \text{és} \quad (a, 0) \cdot (b, 0) = (ab, 0).$$

Jelölés.

Tetszőleges $a \in \mathbb{R}$ esetén az $(a, 0)$ komplex szám helyett egyszerűen a -t írunk, és nem is különböztetjük meg az a valós számtól. (Úgy tekintjük, hogy $\mathbb{R} \subseteq \mathbb{C}$.)





$i = (0,1)$

Kanonikus alak

1.3. Állítás.

Minden $a, b \in \mathbb{R}$ esetén

$$(a, 0) + (b, 0) = (a + b, 0) \quad \text{és} \quad (a, 0) \cdot (b, 0) = (ab, 0).$$

Jelölés.

Tetszőleges $a \in \mathbb{R}$ esetén az $(a, 0)$ komplex szám helyett egyszerűen a -t írunk, és nem is különböztetjük meg az a valós számtól. (Úgy tekintjük, hogy $\mathbb{R} \subseteq \mathbb{C}$.)
A $(0, 1)$ komplex számot pedig i jelöli a továbbiakban.

1.4. Tétel.

Minden komplex szám előáll, mégpedig egyértelmű módon, $x + yi$ ($x, y \in \mathbb{R}$) alakban. Az (a, b) komplex szám ilyen felírásánál $x = a$ és $y = b$, azaz

$$(a, b) = a + bi.$$

1.5. Definíció.

A $z = (a, b)$ komplex szám $a + bi$ alakban való felírását z *kanonikus alakjának*, az a valós számot z *valós részének* (jelölése: $\operatorname{Re} z$), a b valós számot z *képzetes részének* (jelölése: $\operatorname{Im} z$) nevezzük. Az i komplex szám neve *képzetes egység*.

Számolás kanonikus alakban

1.6. Állítás.

A képzetes egység négyzete: $i^2 = -1$.

Megjegyzés.

Ezután a komplex számokat nem valós számokból álló számpárokként, hanem $a + bi$ alakú formális kifejezéseként kezeljük. Ezekkel ugyanúgy lehet számolni, ahogyan betűs kifejezésekkel szoktunk, de i^2 helyett szabad (sőt, többnyire kell is!) -1 -et írni. Az összeadás és a kivonás elég természetes ebben az alakban, a szorzás és a reciprokképzés pedig a következő módon végezhető el:

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i;$$

$$\frac{1}{a + bi} = \frac{1}{a + bi} \cdot \frac{a - bi}{a - bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i \quad (\text{ha } a + bi \neq 0).$$

Példa.

$$\frac{2 + 3i}{1 + 4i} = \frac{2 + 3i}{1 + 4i} \cdot \frac{1 - 4i}{1 - 4i} = \frac{2 - 12i^2 - 8i + 3i}{17} = \frac{14 - 5i}{17} = \frac{14}{17} - \frac{5}{17}i$$

Konjugált

1.7. Definíció.

A $z = a + bi$ komplex szám *konjugáltján* a $\bar{z} = a - bi$ komplex számot értjük.

1.8. Tétel.

Bármely u, v komplex számokra érvényesek az alábbiak:

$$(1) \quad \overline{u + v} = \bar{u} + \bar{v};$$

$$(5) \quad \overline{\bar{u}} = u;$$

$$(2) \quad \overline{u - v} = \bar{u} - \bar{v};$$

$$(6) \quad \bar{u} = u \iff u \in \mathbb{R};$$

$$(3) \quad \overline{u \cdot v} = \bar{u} \cdot \bar{v};$$

$$(7) \quad u + \bar{u} = 2 \operatorname{Re} u;$$

$$(4) \quad \overline{u/v} = \bar{u}/\bar{v}, \text{ ha } v \neq 0;$$

$$(8) \quad u \cdot \bar{u} = (\operatorname{Re} u)^2 + (\operatorname{Im} u)^2.$$

Bizonyítás.

Egyszerű számolás, egyedül (4)-nél érdemes trükközni: könnyebben kijön, ha visszavezetjük (3)-ra.



A komplex számsík

1.9. Definíció.

Legyen adott a síkban egy Descartes-féle derékszögű koordinátarendszer, és feleltessük meg az $a + bi$ komplex számnak az (a, b) koordinátájú pontot.

Így kapjuk a *komplex számsíkot*, más néven *Gauss-féle számsíkot*.

Az első tengelyt (abszcissza) *valós tengelynek*, a második tengelyt (ordináta) pedig *képzetes tengelynek* hívjuk. A valós tengelyen találhatóak a valós számok, a képzetes tengelyen pedig az úgynevezett *tiszta képzetes számok*.

1.10. Definíció.

A $z = a + bi$ komplex szám *abszolút értékén* a $|z| = \sqrt{a^2 + b^2}$ nemnegatív valós számot értjük.

1.11. Megjegyzés.

A komplex számsíkon az abszolút érték az origótól (nullától) való távolságot jelenti, a konjugálás nem más, mint a valós tengelyre való tükrözés, az összeadás pedig (hely)vektorok összeadásával írható le geometriailag.

Az abszolút érték tulajdonságai

1.12. Tétel.

Bármely u, v komplex számokra érvényesek az alábbiak:

$$(1) |u| = \sqrt{u\bar{u}};$$

$$(2) 1/u = \bar{u}/|u|^2 \text{ ha } u \neq 0;$$

$$(3) |u \cdot v| = |u| \cdot |v|;$$

$$(4) |u/v| = |u|/|v| \text{ ha } v \neq 0;$$

$$(5) |\bar{u}| = |u|;$$

$$(6) |u + v| \leq |u| + |v|.$$

Bizonyítás.

Egyszerű számolás, felhasználva a konjugált tulajdonságait, kivéve (6)-ot, amit geometriailag sokkal könnyebb belátni. □

Házi feladat a gyakorlatra

1. feladat. Számítsa ki az alábbi komplex számokat kanonikus alakban.

(a) $\frac{2+3i}{1+4i} = ?$ eredmény: $\frac{14}{17} - \frac{5}{17}i$

(b) $u\bar{v} + \bar{u}v = ?$, $\frac{\bar{u}}{v} + \frac{u}{\bar{v}} = ?$, $|uv| = ?$, $\left|\frac{u}{v}\right| = ?$, ahol $u = 2 - 3i$ és $v = 1 + i$
eredmény: $u\bar{v} + \bar{u}v = -2$, $\frac{\bar{u}}{v} + \frac{u}{\bar{v}} = 5$, $|uv| = \sqrt{26}$, $\left|\frac{u}{v}\right| = \frac{1}{2}\sqrt{26}$

(c) $\left(\frac{-1+i}{2+i}\right)^2 - \left(\frac{-1-i}{2-i}\right)^2 = ?$

(d) $(\overline{2+5i})^2 + \overline{(2+5i)^2} = ?$

(e) $(\overline{-6+9i} + 4 - 8i) \cdot i = ?$

Házi feladat a gyakorlatra

2. feladat. Ábrázolja a Gauss-féle számsíkon az alábbi számhalmazokat.

(a) $\{z \in \mathbf{C}: \operatorname{Im}(\bar{z} - i) > 1\}$, $\{z \in \mathbf{C}: |iz - i| = 1\}$

(b) $\{z \in \mathbf{C}: |\bar{z} + 2 - i| \leq 2\}$

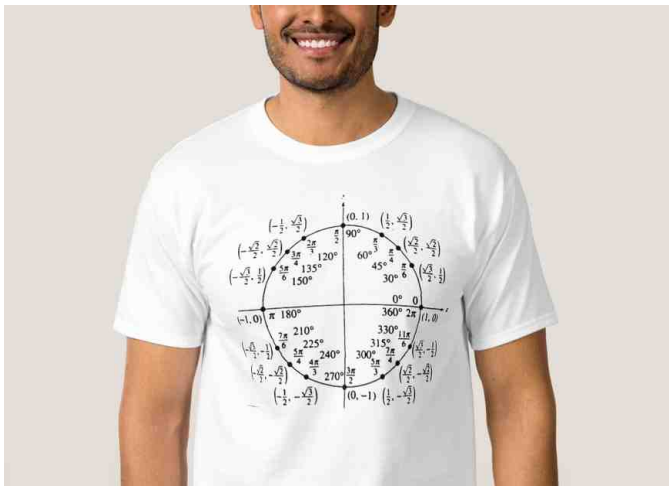
eredmény: $-2 - i$ középpontú, 2 sugarú zárt körlemez

(c) $\{z \in \mathbf{C}: |\bar{z} - i| = 1\}$

(d) $\{z \in \mathbf{C}: 0 \leq \operatorname{Re}(z + 3) < 1\}$

(e) $\{z \in \mathbf{C}: |iz - 1 - i| > 1\}$

Trigonometrikus alak, hatványozás, gyökvonás, egységgyökök



Trigonometrikus alak

1.13. Definíció.

Egy nemnulla z komplex szám *argumentumán* olyan $\arg z$ irányított szöget értünk, amellyel a valós tengely pozitív felét az origó körül elforgatva átmegy a z -nek megfelelő ponton.

1.14. Megjegyzés.

A nullának nincs argumentuma, a nullától különböző komplex számok argumentuma pedig csak „modulo 2π ”, azaz 2π egész számú többszöröseitől eltekintve meghatározott.

1.15. Állítás.

Bármely $0 \neq z \in \mathbb{C}$ esetén az $r = |z|$ és $\varphi = \arg z$ jelöléssel

$$z = r (\cos \varphi + i \sin \varphi) = r \operatorname{cis} \varphi.$$

1.16. Definíció.

A nemnulla komplex számok fenti (azaz $|z| \cdot (\cos \arg z + i \sin \arg z)$ alakú) felírását *trigonometrikus alaknak* nevezzük.

Trigonometrikus alak

1.17. Megjegyzés.

A nullának nincs trigonometrikus alakja, hiszen argumentuma sincs, de $r = 0$ és bármely $\varphi \in \mathbb{R}$ esetén nyilván $0 = r(\cos \varphi + i \sin \varphi)$.

Példa.

Legyen $z = 1 + i$. Ekkor $r = |z| = \sqrt{2}$, és

$$z = \sqrt{2} \cdot \left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \right) = \sqrt{2}(\cos \varphi + i \sin \varphi) \implies \varphi = \frac{\pi}{4}.$$

Tehát $z = \sqrt{2} \operatorname{cis} \frac{\pi}{4}$.

Példa.

Legyen $z = 1 + \sqrt{3}i$. Ekkor $r = |z| = 2$, és

$$z = 2 \cdot \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i \right) = 2(\cos \varphi + i \sin \varphi) \implies \varphi = \frac{\pi}{3}.$$

Tehát $z = 2 \operatorname{cis} \frac{\pi}{3}$.

Számolás trigonometrikus alakban

1.18. Állítás.

Bármely $r, r' \in \mathbb{R}^+$ és $\varphi, \varphi' \in \mathbb{R}$ esetén

$$r \operatorname{cis} \varphi = r' \operatorname{cis} \varphi' \iff r = r' \text{ és } \exists k \in \mathbb{Z} : \varphi' = \varphi + 2k\pi.$$

1.19. Tétel.

Tetszőleges nullától különböző $u = r \operatorname{cis} \varphi$ és $v = s \operatorname{cis} \psi$ komplex számokra

- (1) $\bar{u} = r \operatorname{cis} (-\varphi)$;
- (2) $uv = rs \operatorname{cis} (\varphi + \psi)$;
- (3) $\frac{1}{v} = \frac{1}{s} \operatorname{cis} (-\psi)$;
- (4) $\frac{u}{v} = \frac{r}{s} \operatorname{cis} (\varphi - \psi)$.

1.20. Megjegyzés.

A szorzat trigonometrikus alakjára vonatkozó képletből látszik, hogy rögzített $v = \operatorname{cis} \psi$ egységnyi abszolút értékű komplex szám esetén a $z \mapsto z \cdot v$ leképezés nem más, mint az origó körüli ψ szögű forgatás a komplex számsíkon.

Számolás trigonometrikus alakban

Példa.

Számítsuk ki ugyanazt a törtet trigonometrikus és kanonikus alakban is.

$$\frac{1 + \sqrt{3}i}{1 + i} = \frac{2 \operatorname{cis} \frac{\pi}{3}}{\sqrt{2} \operatorname{cis} \frac{\pi}{4}} = \frac{2}{\sqrt{2}} \operatorname{cis} \left(\frac{\pi}{3} - \frac{\pi}{4} \right) = \sqrt{2} \operatorname{cis} \frac{\pi}{12}$$

$$\frac{1 + \sqrt{3}i}{1 + i} = \frac{1 + \sqrt{3}i}{1 + i} \cdot \frac{1 - i}{1 - i} = \frac{1 + \sqrt{3} - i + \sqrt{3}i}{2} = \frac{\sqrt{3} + 1}{2} + \frac{\sqrt{3} - 1}{2}i$$

A két alakot összehasonlítva kapjuk, hogy

$$\cos \frac{\pi}{12} = \frac{\sqrt{3} + 1}{2\sqrt{2}} \quad \text{és} \quad \sin \frac{\pi}{12} = \frac{\sqrt{3} - 1}{2\sqrt{2}}.$$

Házi feladat a gyakorlatra

3. feladat. Számítsa ki trigonometrikus és kanonikus alakban is.

(a) $\frac{1 + \sqrt{3}i}{1 + i} = ?$

eredmény: $\sqrt{2} \operatorname{cis} \frac{\pi}{12} = \frac{\sqrt{3} + 1}{2} + \frac{\sqrt{3} - 1}{2}i$

(b) $\frac{(-1 - i)(\sqrt{3} + i)}{(-1 + i)(-\sqrt{3} + i)} = ?$

eredmény: $\operatorname{cis} \frac{11\pi}{6} = \frac{\sqrt{3}}{2} - \frac{1}{2}i$

(c) $(-1 - i)(\sqrt{3} + i) = ?$

(d) $(\sqrt{3} - i)(2 + 2\sqrt{3}i) = ?$

(e) $\frac{1 - i}{1 + i} = ?$