1. *a) Bizonyítsuk be, hogy ha egy K test fölötti legfőljebb 3-adfokú polinomnak nincs gyöke K-ban, akkor az irreducibilis.*
b) Adjunk meg olyan $\mathbb{Z}[x]$-beli 3-adfokú polinomot, amelynek nincs gyöke $\mathbb{Z}$-ben, de nem irreducibilis.
c) Adjunk meg olyan $\mathbb{R}[x]$-beli 4-edfokú polinomot, amelynek nincs gyöke $\mathbb{R}$-ben, de nem irreducibilis.

Megoldás: a) Test fölötti polinom nem triviális felbontása csak olyan lehet, ahol a tényezők legalább elsőfokúak, így egy reducibilis legföljebb harmadfokúnak van K fölötti elsőfokú tényezője, annak pedig van K-ban gyöke. Tehát ha nincs K-beli gyöke, akkor szükségképpen irreducibilis.
b) Pl. $(2x+1)(x^2+1)$ vagy $2(x^3+2)$. Az első ellenpélda azon múlik, hogy $\mathbb{Z}$ nem test, és így nem minden elsőfokú polinomnak van gyöke, a második pedig azon, hogy $\mathbb{Z}$ fölött egy valódi felbontásnak lehet konstans faktora is.
c) Pl. $(x^2+1)^2$-nek nincs valós gyöke ($\pm i$ az összes gyöke), de láthatóan reducibilis.

2. *Melyek irreducibilisek $\mathbb{Q}[x]$-ben az alábbi polinomok közül?*
a) x^2+x+1 *b)* $3x^5-6x^3+2x-2$ *c)* x^4+4 *d)* x^5+4

Megoldás: a) Nincs racionális gyöke (sőt valós sem), és csak másodfokú, tehát a $\mathbb{Q}$ test fölött irreducibilis.
b) Irreducibilis, mert teljesül rá a Schönemann–Eisenstein-kritérium $p=2$-vel.
c) $x^4+4=x^4+4x^2+4-4x^2=(x^2+2)^2-(2x)^2=(x^2-2x+2)(x^2+2x+2)$, tehát a polinom reducibilis $\mathbb{Q}[x]$-ben.
d) Ha egy $f(x)\in R[x]$ polinom (ahol R kommutatív, nullosztómentes gyűrű) nemtriviálisan felbomlik: $f(x)=g(x)h(x)$, akkor tetszőleges $c\in R$-re $f(x+c)=g(x+c)h(x+c)$ is felbomlik, és fordítva, ha $f(x+c)=k(x)\ell(x)$ valódi felbontás, akkor $f(x)=k(x-c)\ell(x-c)$ is az, tehát az eredeti polinom irreducibilitása helyett elég belátni, hogy valamely "eltoltja" irreduciblis (test fölött tetszőleges elsőfokú kifejezést is behelyettesíthetünk). x^5+4-be $x+1$-et behelyettesítve a Schönemann–Eisensteines $x^5+5x^4+10x^3+10x^2+5x+5$ polinomot kapjuk, tehát $(x+1)^5+4$, és így x^5+4 is irredubilis $\mathbb{Q}[x]$-ben.

3. *Keressük meg a $2x^6+x^5-5x^4-2x^3-4x^2-3x+3$ polinom összes gyökét. Bontsuk föl a polinomot irreducibilis polinomok szorzatára $\mathbb{C}[x]$-ben, $\mathbb{R}[x]$-ben, illetve $\mathbb{Q}[x]$-ben.*

Megoldás:
A racionális gyökteszt miatt az $f(x)=2x^6+x^5-5x^4-2x^3-4x^2-3x+3$ polinom racionális gyökeit azon $\frac{p}{q}$ számok között kell keresni, amelyekre p osztója 3-nak, és q osztója 2-nek. Tehát $\frac{p}{q}$ lehetséges értékei $\pm 3, \pm 1, \pm\frac{1}{2}, \pm\frac{3}{2}$. Ezeket Horner-módszerrel behelyettesítjük, és ott, ahol 0 maradékot kapunk, rögtön kijön a hányados is, és akkor azzal számolunk tovább.

	2	1	−5	−2	−4	−3	3
1	2	3	−2	−4	−8	−11	−8
−1	2	−1	−4	2	−6	3	0
−1	2	−3	−1	3	−9	12	
3	2	5	11	35	99	300	
−3	2	−7	17	−49	141	−420	
$\frac{1}{2}$	2	0	−4	0	−6	0	

Eddig $f(x)=(x+1)(x-\frac{1}{2})(2x^4-4x^2-6)=(x+1)(2x-1)(x^4-2x^2-3)$, és a negyedfokú tényezőt már x^2 két polinomjának szorzatára tudjuk bontani:

$f(x) = (x+1)(2x-1)(x^2-3)(x^2+1)$. Ezek a faktorok $\mathbb{Q}[x]$ fölött irreducibilisek, mert a másodfokúaknak nincs racionális gyöke. Valós fölött az egyik másodfokút tovább lehet bontani:
$f(x) = (x+1)(2x-1)(x-\sqrt{3})(x+\sqrt{3})(x^2+1)$, a $\mathbb{C}$ fölötti felbontás pedig
$f(x) = (x+1)(2x-1)(x-\sqrt{3})(x+\sqrt{3})(x-i)(x+i)$. A gyökök $-1, \frac{1}{2}, \pm\sqrt{3}, \pm i$.

4. *Számítsuk ki euklideszi algoritmussal a*
a) 348 *és* 493 *számok legnagyobb közös osztóját;*
b) az x^6-1 *és* $x^5-x^4+2x^3+1$ *polinomok legnagyobb közös osztóját!*

Megoldás: a) A $493 = 1\cdot 348+145$, $348 = 2\cdot 145+58$, $145 = 2\cdot 58+29$, $58 = 2\cdot 29+0$ maradékos osztások alapján a legnagyobb közös osztó 29 (az utolsó nem nulla maradék).

b) Az egymás utáni maradékos osztásoknál megtehetjük, hogy az osztónak egy konstanszorosát használjuk (így a maradék, és végső sorban az utolsó nem nulla maradék is konstansszoros lesz, de ez a test fölötti polinomok számelméletében nem számít.
$x^6-1 = (x^5-x^4+2x^3+1)(x+1)+(-x^4-2x^3-x-2)$
$x^5-x^4+2x^3+1 = (x^4+2x^3+x+2)+(8x^3-x^2+x+7)$
$x^4+2x^3+x+2 = (8x^3-x^2+x+7)(\frac{1}{8}x+\frac{17}{64})+(\frac{9}{64}x^2-\frac{9}{64}x+\frac{9}{64})$
$8x^3-x^2+x+7 = (x^2-x+1)(8x+7)+0$
Tehát a legnagyobb közös osztó x^2-x+1.

5. *Keressük meg az összes másodfokú irreducibilis polinomot* $\mathbb{Z}_2$*-ben és* $\mathbb{Z}_3$*-ban!*

Megoldás: Azokat a másodfokúakat kell megkeresni, amelyeknek nincs gyökük az adott testben. Feltehetjük, hogy a főegyüttható 1 (mert minden polinomnak van ilyen skalárszorosa, és az pontosan akkor irreducibilis, ha az eredeti polinom az), és a konstans tag nem lehet 0, mert különben a 0 gyök lenne. $\mathbb{Z}_2$ fölött ezek után csak az x^2+1 és x^2+x+1 jön szóba, de az első nem irreducibilis, mert gyöke az 1, tehát az egyetlen másodfokú irreducibilis polinom $\mathbb{Z}_2[x]$-ben x^2+x+1. A $\mathbb{Z}_3$ fölöttieknél hat választásunk van az együtthatókra, és azt kell ellenőrizni, hogy 1 és $2=-1$ ne legyen gyöke. Az 1 főegyütthatósak között három ilyen van: x^2+x-1, x^2-x-1 és x^2+1, és vehetjük még ezeknek a -1-szeresét.

6. *Bizonyítsuk be, hogy az alábbi polinomok irreducibilisek* $\mathbb{Q}[x]$*-ben a* $\mathbb{Z}_2$ *és/vagy* $\mathbb{Z}_3$ *fölötti felbonthatóságának vizsgálatával!*
a) x^4-5x^3+2x+1*; b)* x^4-2x^3+2x+1*; c)* $3x^5+x^2-2x+3$*; d)* x^4+x^3+x+2.

Megoldás: a) Az $f(x) = x^4-5x^3+2x+1$ polinom $\mathbb{Z}_2$ fölötti megfelelője x^4+x^3+1. Ennek nincs gyöke $\mathbb{Z}_2$-ben, tehát ha felbomlana, csak két másodfokú irreducibilis polinomnak lehetne a szorzata, azaz $(x^2+x+1)^2$-nel lenne egyenlő, de az utóbbi (a páros együtthatós tagok kiesése után) x^4+x^2+1 nem egyenlő a megadott polinommal. Ha az $f(x)$ reducibilis lenne $\mathbb{Q}$ fölött, akkor $\mathbb{Z}$ fölött is lenne valódi (legalább elsőfokúakra való) felbontása, és az $\mathbb{Z}_2$ fölött is valódi felbontást adna, mert a főegyütthatók nem válnak 0-vá. Így $f(x)$ irreducibilis $\mathbb{Q}[x]$-ben.

b) Legyen $f(x) = x^4-2x^3+2x+1$. Ennek $\mathbb{Z}_2$ fölött gyöke az 1, tehát $\mathbb{Z}_3$-mal próbálkozunk. Itt az $f(x)$-nek megfelelő polinom x^4+x^3+2x+1. Ennek nincs gyöke $\mathbb{Z}_3$-ban, és ha felbomlana két irreducibilis másodfokú szorzatára, az azt jelentené, hogy az előző feladatban felsorolt másodfokúak valamelyike osztój ennek a polinomnak. Maradékos osztással azt kapjuk, hogy az x^2+x-1-gyel vett maradéka $x+2$, az x^2-x-1-gyel vett maradéka $x+1$, és az x^2+1-gyel vett maradéka $x-1$. Tehát a polinom irreducibilis $\mathbb{Z}_3[x]$-ben, és így $\mathbb{Q}[x]$-ben is.

c) Az $f(x) = 3x^5+x^2-2x+3$ valódi felbontása $\mathbb{Z}[x]$ fölött nem feltétlenül lesz valódi felbontás $\mathbb{Z}_3$ fölött, mert a főegyüttható osztható 3-mal, így egy pozitív fokú faktora akár nulladfokúvá is válhat, ha $\mathbb{Z}_3$ fölött nézzük. Ezért a két test közül csak $\mathbb{Z}_2$-vel próbálkozhatunk. $\mathbb{Z}_2$ fölött a polinom x^5+x^2+1. Ennek nincs gyöke $\mathbb{Z}_2$-ben, tehát ha felbontható, akkor van másodfokú irreducibilis faktora, azaz x^2+x+1 osztója a

polinomnak. Maradékos osztással ellenőrizhetjük, hogy az x^2+x+1-gyel osztva a $f(x)$ $\mathbb{Z}_2$ fölött 1 maradékot ad. Így $f(x)$ irredubilis $\mathbb{Z}_2[x]$-ben, és így $\mathbb{Q}[x]$-ben is.

d) $\mathbb{Z}_2$ fölött az $f(x)=x^4+x^3+x+2$ irreducibilisekre bontása $x^4+x^3+x=x(x^3+x^2+1)$, $\mathbb{Z}_3$ fölött pedig $x^4+x^3+x-1=(x^2+x-1)(x^2+1)$. Ha $f(x)$ felbontható lenne $\mathbb{Q}[x]$-ben, és így $\mathbb{Z}[x]$-ben is, akkor azt a felbontást bonthatnánk tovább $\mathbb{Z}_2$ és $\mathbb{Z}_3$ fölött is, de egy valódi felbontásnak nem lehet egy $1+3$ fokú és egy $2+2$ fokú finomítása is. Tehát $f(x)$ irreducibilis $\mathbb{Q}[x]$-ben.

7. *Legyen $f(x)=x^4-x^2+1$.*

a) Bontsuk fel $f(x)$-et irreducibilis polinomok szorzatára $\mathbb{R}$, illetve $\mathbb{C}$ fölött!

b) Bizonyítsuk be, hogy $f(x)$ irreducibilis $\mathbb{Q}$ fölött!

c) Bizonyítsuk be, hogy $f(x)$ reducibilis $GF(2)$, $GF(3)$ és $GF(5)$ fölött!

d) Bizonyítsuk be, hogy $f(x)$ reducibilis $GF(p)$ fölött minden p prímre.*

Megoldás: a) $x^4-x^2+1=(x^2+1)^2-3x^2=(x^2-\sqrt{3}x+1)(x^2+\sqrt{3}x+1)$ az $\mathbb{R}[x]$-beli irreducibilisekre bontás (a két másodfokú faktornak nincsenek valós gyökei), $\mathbb{C}$ fölött ez tovább bomlik: $f(x)=(x-(\frac{\sqrt{3}}{2}+\frac{1}{2}i))(x-(\frac{\sqrt{3}}{2}-\frac{1}{2}i))(x-(-\frac{\sqrt{3}}{2}+\frac{1}{2}i))(x-(-\frac{\sqrt{3}}{2}-\frac{1}{2}i))$ (a gyökei éppen a 12. primitív egységgyökök).

b) Ha $\mathbb{Q}$ fölött felbontható lenne, az a felbontás tovább finomítható lenne valós fölötti irreducibilisekre bontássá. De a valós fölötti felbontás is csak két tényezőből áll, tehát akkor konstans szorzó erejéig ez lenne a $\mathbb{Q}$ fölötti felbontás. Viszont az $x^2-\sqrt{3}x+1$ polinomnak semelyik nemnulla skalárszorosa nem lehet racionális együtthatós (két együtthatójának a hányadosa irracionális).

c) $\mathbb{Z}_2[x]$-ben $x^4-x^2+1=x^4+x^2+1=(x^2+x+1)^2$, $\mathbb{Z}_3$-ban $x^4-x^2+1=x^4+2x^2+1=(x^2+1)^2$, és $\mathbb{Z}_5$-ben $x^4-x^2+1=x^4-2x^2+1-4x^2=(x^2-1)^2-(2x)^2=(x^2-2x-1)(x^2+2x-1)$.

8. *Van-e olyan polinom $\mathbb{Q}[x]$-ben, amelynek nem minden együtthatója egész, mégis egész értéket vesz föl minden egész helyen?*

Megoldás: Ilyen például az $\frac{1}{2}x^2+\frac{1}{2}x$.

9. *Bizonyítsuk be, hogy ha $f(x)\in\mathbb{Z}[x]$, és $a,b\in\mathbb{Z}$, akkor $a-b \mid f(a)-f(b)$.*

Megoldás: Legyen $f(x)=c_nx^n+c_{n-1}x^{n-1}+\ldots+c_1x+c_0$. Ekkor $f(a)-f(b)=c_n(a^n-b^n)+c_{n-1}(a^{n-1}-b^{n-1})+\ldots+c_1(a-b)$, és minden k-ra $a^k-b^k=(a-b)(a^{k-1}+a^{k-2}b+a^{k-3}b^2+\ldots+ab^{k-2}+b^{k-1})$, tehát $f(a)-f(b)$ minden tagja osztható $(a-b)$-vel, így $f(a)-f(b)$ is osztható vele.

10. *Van-e olyan egész együtthatós f polinom, amely az $1,2,-1$ helyeken az alábbi értékeket veszi föl?*

a) $f(1)=3$, $f(2)=10$, és $f(-1)=7$;

b) $f(1)=3$, $f(2)=10$, és $f(-1)=2$.

Megoldás: a) Newton-interpolációval: $f_0(x)\equiv 3$ jó az 1-ben, $f_1(x)=f_0(x)+a(x-1)=3+a(x-1)$ jó az 1-ben és a 2-ben, ha $10=3+a(2-1)$, azaz $a=7$, és így $f_1(x)=7x-4$. Végül $f_2(x)=f_1(x)+b(x-1)(x-2)=7x-4+b(x-1)(x-2)$ jó mindhárom helyen, ha $7=-11+b(-2)(-3)$, tehát $b=3$, és $f_2(x)=7x-4+3(x^2-3x+2)=3x^2-2x+2$.

b) Nincs ilyen egész együtthatós polinom a 9. feladat állítása szerint, ugyanis $f(1)-f(-1)=1$ nem osztható 2-vel.

11. *Tegyük föl, hogy az $f(x)\in\mathbb{R}[x]$ polinom 4-edfokú, 1 főegyütthatós, és $f(1)=10$, $f(2)=20$, $f(3)=30$. Mennyi lehet $f(0)+f(4)$?*

Megoldás: Az $f(1)=10$, $f(2)=20$, $f(3)=30$ feltételt kielégíti a $10x$ polinom, így $f(x)=10x+g(x)(x-1)(x-2)(x-3)$ valamilyen $g(x)$ valós polinommal. Ez az $f(x)$ polinom akkor lesz negyedfokú, ha $g(x)$ elsőfokú, és akkor lesz 1 főegyütthatós, ha $g(x)$ főegyütthatója 1. Tehát $g(x)=x+c$ valamely $c\in\mathbb{R}$-re. Így $f(x)=10x+(x+c)(x-1)(x-2)(x-3)$, és $f(0)+f(4)=-6c+40+6c=40$.

12. *Legyenek a, b és c az $2x^3 - x^2 + 3x + 6$ polinom három gyöke $\mathbb{C}$-ben. Határozzuk meg az abc, $a^3 + b^3 + c^3$ és $a^2b^2 + a^2c^2 + b^2c^2$ kifejezések értékét.*

Megoldás: A polinom gyöktényezős felbontása $2x^3 - x^2 + 3x + 6 = 2(x-a)(x-b)(x-c)$, tehát $x^3 - \frac{1}{2}x^2 + \frac{3}{2}x + 3 = (x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc$, és így $a + b + c = \frac{1}{2}$, $ab + ac + bc = \frac{3}{2}$, és $abc = -3$.

Ebből $a^2b^2 + a^2c^2 + b^2c^2 = (ab+ac+bc)^2 - 2(a^2bc + b^2ac + c^2ab) = (ab+ac+bc)^2 - 2abc(a+b+c) = \frac{9}{4} + 6 \cdot \frac{1}{2} = \frac{21}{4}$, továbbá $a^3 + b^3 + c^3 = (a+b+c)^3 - 3(a^2b + a^2c + b^2a + b^2c + c^2a + c^2b) - 6abc = (a+b+c)^3 - 3((ab+ac+bc)(a+b+c) - 3abc) - 6abc = (a+b+c)^3 - 3(ab+ac+bc)(a+b+c) + 3abc = \frac{1}{8} - 3 \cdot \frac{3}{2}\frac{1}{2} - 9 = -\frac{89}{8}$.

13. *Az $x^3 - 2x^2 + 5x + 1$ polinom gyökei α, β és γ. Adjuk meg azt a harmadfokú, 1 főegyütthatós polinomot, amelynek gyökei $\alpha + \beta$, $\alpha + \gamma$ és $\beta + \gamma$.*

Megoldás: A gyökök és együtthatók közti összefüggésből (mint az előző feladat megoldásának elején) tudjuk, hogy $\alpha + \beta + \gamma = 2$, $\alpha\beta + \alpha\gamma + \beta\gamma = 5$ és $\alpha\beta\gamma = -1$. Az új polinom $x^3 + px^2 + qx + r$, ahol $-p = ((\alpha+\beta) + (\alpha+\gamma) + (\beta+\gamma)) = 2(\alpha+\beta+\gamma) = 4$, $q = (\alpha+\beta)(\alpha+\gamma) + (\alpha+\beta)(\beta+\gamma) + (\alpha+\gamma)(\beta+\gamma)) = \alpha^2 + \beta^2 + \gamma^2 + 3(\alpha\beta + \alpha\gamma + \beta\gamma) = (\alpha+\beta+\gamma)^2 + (\alpha\beta + \alpha\gamma + \beta\gamma) = 9$, és $-r = (\alpha+\beta)(\alpha+\gamma)(\beta+\gamma) = \alpha^2\beta + \alpha^2\gamma + \beta^2\alpha + \beta^2\gamma + \gamma^2\alpha + \gamma^2\beta + 2\alpha\beta\gamma = (\alpha\beta + \alpha\gamma + \beta\gamma)(\alpha+\beta+\gamma) - \alpha\beta\gamma = 10 + 1 = 11$. Tehát a keresett polinom $x^3 - 4x^2 + 9x - 11$.

Hf1. *Bontsuk föl az $x^5 + 6x^3 + 2x^2 - 4x - 2$ polinomot irreducibilisek szorzatára $\mathbb{Q}[x]$-ben.*

Hf2. *Bizonyítsuk be, hogy nincs olyan harmadfokú $f(x) \in \mathbb{Q}[x]$ polinom, amelyre $f(-1) = 4$, $f(0) = 1$, $f(1) = 2$ és $f(2) = 7$.*