11.1. *a)* 3, *b)* 2, *c)* 1, *d)* 1, ui. $2^4 \bmod 5 = 1$, és $2^{1001} = 2(2^4)^{250} \bmod 5 = 2$ *e)* 4, ui. 2 hatványai modulo 6: $2, 4, 2, 4, 2, 4, \ldots$.

11.2. Azt mondjuk, hogy a kongruens b-vel modulo m, ha $a \bmod m = b \bmod m$, azaz ha a és b azonos maradékot ad m-mel osztva, azaz ha $a - b$ maradéka 0, vagyis $m \mid a - b$. E reláció reflexív, hisz $a - a$ maradéka 0. Szimmetrikus is, hisz ha $a - b$ maradéka 0, akkor $b - a$ maradéka is. Végül a reláció tranzitív is, hisz ha $a - b$ és $b - c$ maradéka 0, akkor $a - c = a - b + b - c$ maradéka is.

11.3. Az előző feladatban beláttuk, hogy az $m \mid a - b$, azaz $a \equiv b \pmod m$ az a és b között egy ekvivalenciareláció, tehát megad $\mathbb{Z}$ elemein egy osztályozást. Egy osztályba tartoznak az m-mel osztva azonos maradékot adó egészek. Legyen $a, b \in \mathbb{Z}$ két tetszőleges egész, és legyen $a = mq_a + r_a$, $b = mq_b + r_b$, $a \pm b = mq_{a\pm b} + r_{a\pm b}$, $ab = mq_{ab} + r_{ab}$, ahol $0 \leqslant r_a, r_b, r_{a\pm b}, r_{ab} < m$. Másként fogalmazva $m \mid a - r_a$, $m \mid b - r_b$, $m \mid a \pm b - r_{a\pm b}$, $m \mid ab - r_{ab}$. Ekkor

$$m \mid (a - r_a) \pm (b - r_b) - (a \pm b - r_{a\pm b}),$$

ezért $m \mid r_{a\pm b} - (r_a \pm r_b)$, azaz $r_a \pm r_b \equiv r_{a\pm b} \pmod m$, tehát

$$(a \bmod m \pm b \bmod m) \bmod m = (a \pm b) \bmod m.$$

Hasonlóképp be kell látnunk, hogy $m \mid r_a r_b - r_{ab}$.

$$\begin{aligned} r_a r_b - r_{ab} &= (a - mq_a)(b - mq_b) - (ab - mq_{ab}) \\ &= -mq_a - mq_b + mq_{ab} \equiv 0 \pmod m, \end{aligned}$$

amivel igazoltuk a második állítást is.

11.4. A tétel $p = 2$ esetén azt mondja, hogy $a^2 \equiv a \pmod 2$, azaz bármely egész szám négyzetének paritása azonos a szám paritásával, vagyis páros szám négyzete páros, páratlan szám négyzete páratlan. Nyilván az is igaz, hogy $0^p \equiv 0 \pmod p$. Ezután feltehetjük, hogy p páratlan prím, akkor viszont elég csak pozitív a egészekre igazolni a tételt, hisz ha $a^p \equiv a \pmod m$, akkor $(-a)^p \equiv (-a) \pmod m$ is fennáll.

Teljes indukcióval bizonyítunk. $a = 1$-re az állítás igaz, hisz $1^p \equiv 1 \pmod p$ bármely p-re igaz. Tegyük fel, hogy a tétel állítása igaz valamely $a \in \mathbb{N}$ számra. A binomiális tétellel bizonyítjuk, hogy igaz $a + 1$-re is:

$$\begin{aligned} (a+1)^p &= a^p + \binom{p}{1} a^{p-1} + \ldots + \binom{p}{p-1} a + 1 \\ &\equiv a^p + 1, \end{aligned}$$

ugyanis $0 < k < p$ esetén

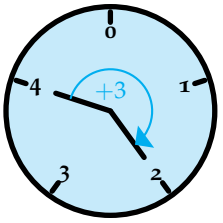
$$\binom{p}{k} = \frac{p!}{k!(n-k)!},$$

és a p prím csak a számlálóban szerepel, tehát $\binom{p}{k}$ osztható p-vel, azaz $\binom{p}{k} a^k \equiv 0 \pmod p$.

11.5. Ha $\mathbb{Z}_m$ műveletáblái rendelkezésre állnak, használhatjuk, egyébként úgy számolhatunk, hogy egészeknek tekintjük a számokat, és vesszük az eredmények maradékát modulo m, azaz egyszerűen úgy számolunk, mint maradékokkal:

$$\begin{aligned} 40 + 45 \bmod 60 &= 85 \bmod 60 = 25, \\ 4 + 3 \bmod 5 &= 7 \bmod 5 = 2, \\ 3 \cdot 7 + 10 \bmod 11 &= 31 \bmod 11 = 9. \end{aligned}$$

$\mathbb{Z}_m$ műveletábláival, vagy pl. $\mathbb{Z}_{12}$ és $\mathbb{Z}_{60}$ esetén egy óra mutatójával is számolhatunk, de más m-re is használhatunk „órát”, például $\mathbb{F}_5$-höz így:



Összefoglalva: $\mathbb{Z}_{60}$-ban: $40 + 45 = 25$, $\mathbb{F}_5$-ben: $4 + 3 = 2$ és $\mathbb{F}_{11}$-ben: $3 \cdot 7 + 10 = 10 + 10 = 9$.

11.6. *1)* Mivel $\mathbb{Z}_5$-ben $3 \cdot 4 = 2$, és $3 \cdot 2 = 1$, ezért az egyenlet megoldása $x = 4$, és 3 reciproka 2, azaz $1/3 = 2$. *2)* $\mathbb{Z}_6$-ban az egyenletnek nincs megoldása, és 3-nak nincs reciproka, ami leolvasható a 11.5. műveletábláról is. *3)* Bár a 14 nem prím, $\mathbb{Z}$-ben $3 \cdot 5 = 15$, ezért $\mathbb{Z}_{14}$-ben $3 \cdot 5 = 1$, tehát $1/3 = 5$. 5-tel beszorozva a $3 \cdot x = 2$ egyenletet kapjuk, hogy $1 \cdot x = 10$, azaz $x = 10$ a megoldás.

11.7. Nem lenne egyszerűbb modulo 10 számolni az ellenőrző jegyet, mert a 10 összetett szám, így ha páros indexű helyen 5-tel nagyobb vagy kisebb számot írunk, vagy 5-tel osztható indexű helyen páros számmal nagyobbat vagy kisebbet, az összeg 10 többszörösével változik, azaz a maradéka azonos marad. $\mathbb{Z}_{11}$ e hibákat kimutatja, mert 11 prím.

11.8. *1)* Az 101?1?? szóban a b_4, b_6, b_7 bit ismeretlen. A három egyenletet átrendezve, és a megfelelő értékeket behelyettesítve

$$\begin{aligned} b_7 &= b_1 + b_3 + b_5 = 1 + 1 + 1 = 1, \\ b_6 + b_7 &= b_2 + b_3 = 0 + 1 = 1, \\ b_4 + b_6 + b_7 &= b_5 = 1, \end{aligned}$$

ahonnan egyszerű visszahelyettesítéssel

$$\begin{aligned} b_4 &= 0, \\ b_6 &= 0, \\ b_7 &= 1 \end{aligned}$$

az egyetlen megoldás.

2) A ?0110?? szóban a b_1, b_6, b_7 bit ismeretlen. A három egyenletet átrendezve, és a megfelelő értéke-

ket behelyettesítve

$$b_1 + b_7 = b_3 + b_5 = 1 + 0 = 1,$$
$$b_6 + b_7 = b_2 + b_3 = 0 + 1 = 1,$$
$$b_6 + b_7 = b_4 + b_5 = 1 + 0 = 1,$$

ahol a második és harmadik egyenlőség azonos, így két egyenletünk van a három ismeretlenre. A megoldások a $b_7 = t$ paraméterválasztással

$$\begin{bmatrix} b_1 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1+t \\ 1+t \\ t \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} t, \quad t = 0, 1,$$

így a két lehetséges megoldás $(1,1,0)$ és $(0,0,1)$.

3) A ???0010 szóban a b_1, b_2, b_3 bit ismeretlen. A három egyenletet átrendezve, és a megfelelő értékeket behelyettesítve

$$b_1 + b_3 = b_5 + b_7 = 0 + 0 = 0,$$
$$b_2 + b_3 = b_6 + b_7 = 1 + 0 = 1,$$
$$0 = b_4 + b_5 + b_6 + b_7 = 0 + 0 + 1 + 0 = 1,$$

ahol az utolsó egyenlőség miatt az egyenletrendszer inkonzisztens.

4) E kód 1-hibajavító, tehát bármely két kódszó Hamming-távolsága legalább három. Így ha a megadott öt bit mellé a két ismeretlen bitet tetszőlegesen kiegészítjük mind a négy módon (00, 01, 10, 11), akkor e szavak mind legföljebb 2 távolságra vannak egymástól, így nem lehet köztük két kódszó, legfeljebb egy. Viszont bármelyiket kiválasztva közülük, az vagy kódszó, vagy egyetlen bit megváltoztatásával kódszóvá alakítható, és az a bit nem lehet a megadott öt bit egyike sem, hisz azok biztosan jók (legalább is a feladat szerint ezt tudjuk), tehát e négy szó egyike biztosan kódszó. A két hiányzó bitet pótolni tudtuk.

11.9. Először igazoljuk, hogy az $m(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$ polinom irreducibilis. Mivel másodfokú, ezért elég ellenőrizni, hogy nincs gyöke. Valóban

$$m(0) = 0^2 + 2 \cdot 0 + 2 = 2 \neq 0,$$
$$m(1) = 1^2 + 2 \cdot 1 + 2 = 2 \neq 0,$$
$$m(2) = 2^2 + 2 \cdot 2 + 2 = 1 \neq 0.$$

Ezután tekintsük x hatványait modulo $m(x)$, azaz mindig végezzük el az $x^2 = -2x - 2 = x + 1$ helyettesítést:

$$x^0 = 1, \qquad x^1 = x,$$
$$x^2 = x + 1, \qquad x^3 = x(x+1) = 2x + 1,$$
$$x^4 = x(2x+1) = 2x, \qquad x^5 = 2x^2 = 2x + 2,$$
$$x^6 = x(2x+2) = x + 2, \quad x^7 = x(x+2) = 1.$$

Mivel x hatványai kiadják az összes legfeljebb elsőfokú $\mathbb{F}_2[x]$-beli polinomot, az $m(x)$ primitív polinom.

11.10. A táblázat elemei az x hatványaival is, és az $m(x)$-szel való maradékokkal is számolhatók.

$\times$	1	x	$x+1$	$2x+1$	$2x$	$2x+2$	$x+2$
1	1	x	$x+1$	$2x+1$	$2x$	$2x+2$	$x+2$
x	x	$x+1$	$2x+1$	$2x$	$2x+2$	$x+2$	1
$x+1 = x^2$	$x+1$	$2x+1$	$2x$	$2x+2$	$x+2$	1	x
$2x+1 = x^3$	$2x+1$	$2x$	$2x+2$	$x+2$	1	x	$x+1$
$2x = x^4$	$2x$	$2x+2$	$x+2$	1	x	$x+1$	$2x+1$
$2x+2 = x^5$	$2x+2$	$x+2$	1	x	$x+1$	$2x+1$	$2x$
$x+2 = x^6$	$x+2$	1	x	$x+1$	$2x+1$	$2x$	$2x+2$

11.11. Mindegyik állítás az algebrai kifejezésekkel való műveleti tulajdonságokból következik. Példaként két azonosságot igazolunk, a többit az Olvasóra hagyjuk.

a) $$\begin{aligned} z + w &= z_1 + z_2\mathrm{i} + w_1 + w_2\mathrm{i} \\ &= w_1 + w_2\mathrm{i} + z_1 + z_2\mathrm{i} = w + z \end{aligned}$$

e) $$\begin{aligned} (z+v)w &= (z_1 + z_2\mathrm{i} + v_1 + v_2\mathrm{i})(w_1 + w_2\mathrm{i}) \\ &= z_1w_1 + z_2w_1\mathrm{i} + v_1w_1 + v_2w_1\mathrm{i} \\ &\quad + z_1w_2\mathrm{i} + z_2w_2\mathrm{i}^2 + v_1w_2\mathrm{i} + v_2w_2\mathrm{i}^2 \\ &= (z_1w_1 + z_2w_1\mathrm{i} + z_1w_2\mathrm{i} + z_2w_2\mathrm{i}^2) \\ &\quad + (v_1w_1 + v_2w_1\mathrm{i} + v_1w_2\mathrm{i} + v_2w_2\mathrm{i}^2) \\ &= zw + vw \end{aligned}$$

11.12. *a)* Legyen $z = a + b\mathrm{i}$, $w = c + d\mathrm{i}$. Ekkor

$$\begin{aligned} \overline{z \pm w} &= \overline{a \pm c + (b \pm d)\mathrm{i}} \\ &= a \pm c - (b \pm d)\mathrm{i} \\ &= a - b\mathrm{i} \pm (c - d\mathrm{i}) \\ &= \bar{z} \pm \bar{w}. \end{aligned}$$

Ezzel igazoltuk az 1. állítást. A többi hasonlóan egyszerűen behelyettesítéssel ellenőrizhető.

b) Indukcióval adódik az előzőkből.

11.13. *a)* $5 + \mathrm{i}$, *b)* $8 + 4\mathrm{i}$, *c)* $1 - 3\mathrm{i}$, *d)* $\frac{1}{2} - \mathrm{i}$, *e)* $8 - 6\mathrm{i}$, *f)* $18 - 26\mathrm{i}$.

11.14. *a)* $2 + \mathrm{i}$, $1 - 4\mathrm{i}$; *b)* $-\mathrm{i}$, $2023\mathrm{i}$; *c)* $3 \pm 5\mathrm{i}$.

11.15. *a)* $\cos 0 + \mathrm{i}\sin 0$, *b)* $\cos\pi + \mathrm{i}\sin\pi$, *c)* $\cos\frac{3\pi}{2} + \mathrm{i}\sin\frac{3\pi}{2}$, *d)* $2(\cos\frac{\pi}{3} + \mathrm{i}\sin\frac{\pi}{3})$, *e)* $2(\cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3})$, *f)* $4\sqrt{2}(\cos\frac{7\pi}{4} + \mathrm{i}\sin\frac{7\pi}{4})$,
g) A szám abszolút értéke 1, így

$$\cos\alpha = \frac{1}{4}(\sqrt{6} + \sqrt{2}) \text{ és } \sin\alpha = \frac{1}{4}(\sqrt{6} - \sqrt{2}).$$

Mivel $\cos^2\alpha - \sin^2\alpha = \cos 2\alpha = \sqrt{3}/2$, ezért $\alpha = \frac{\pi}{12}$, a keresett alak $\cos\frac{\pi}{12} + \mathrm{i}\sin\frac{\pi}{12}$.
h) $(\sqrt{6} + \sqrt{2})(\cos\frac{\pi}{12} + \mathrm{i}\sin\frac{\pi}{12})$.

11.16.
a) $2\sqrt{2}\left(\cos(-\frac{\pi}{12}) + \mathrm{i}\sin(-\frac{\pi}{12})\right)$,
b) $2\sqrt{2}\left(\cos(-\frac{7}{\pi}12) + \mathrm{i}\sin(-\frac{7\pi}{12})\right)$,
c) $2\sqrt{2}\left(\cos(\alpha - \frac{\pi}{12}) + \mathrm{i}\sin(\alpha - \frac{\pi}{12})\right)$.

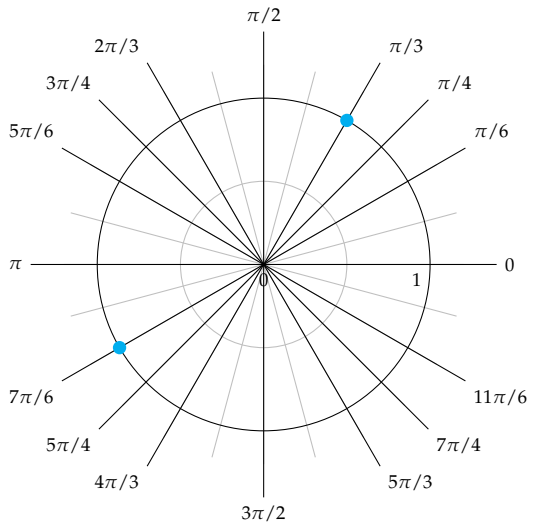
11.17. *a)* $\sqrt{3}+\mathrm{i}$ hossza $\sqrt{\sqrt{3}^2+1^2}=2$, trigonometriai alakja: $2(\cos\frac{\pi}{6}+\mathrm{i}\sin\frac{\pi}{6})$. Így

$$\begin{aligned}[2(\cos\frac{\pi}{6}+\mathrm{i}\sin\frac{\pi}{6})]^6 &= 2^6(\cos\frac{6\pi}{6}+\mathrm{i}\sin\frac{6\pi}{6})\\ &= 64(\cos\pi+\mathrm{i}\sin\pi)\\ &= -64.\end{aligned}$$

b) $\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$, mivel $2023\equiv 1 \pmod 6$.

c) $-\frac{\sqrt{3}}{2}-\frac{1}{2}\mathrm{i}$, mivel $2023\equiv 7 \pmod{12}$.

A *b)* és *c)* feladatokhoz szemléltetés: $\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}=\cos\frac{\pi}{3}+\mathrm{i}\sin\frac{\pi}{3}$, $(\frac{\sqrt{3}}{2}+\frac{1}{2}\mathrm{i})^7=(\cos\frac{\pi}{6}+\mathrm{i}\sin\frac{\pi}{6})^7=\cos\frac{7\pi}{6}+\mathrm{i}\sin\frac{7\pi}{6}$.



11.18. *a)* A trigonometrikus alakot használva

$$\begin{aligned}(1+\mathrm{i})^n &= \left(\sqrt{2}\left(\cos\frac{\pi}{4}+\mathrm{i}\sin\frac{\pi}{4}\right)\right)^n\\ &= 2^{\frac{n}{2}}\left(\cos\frac{n\pi}{4}+\mathrm{i}\sin\frac{n\pi}{4}\right).\end{aligned}$$

b) Hasonlóan az előző ponthoz

$$\begin{aligned}(\sqrt{3}-\mathrm{i})^n &= \left(2\left(\cos\frac{\pi}{6}+\mathrm{i}\sin\frac{\pi}{6}\right)\right)^n\\ &= 2^n\left(\cos\frac{n\pi}{6}+\mathrm{i}\sin\frac{n\pi}{6}\right).\end{aligned}$$

c), d) Az *a)* pontbeli egyenlőség bal oldalát bontsuk fel a binomiális tétel szerint (az 1 hatványait nem jelöljük):

$$\begin{aligned}&(1+\mathrm{i})^n\\ &=\binom{n}{0}+\binom{n}{1}\mathrm{i}+\binom{n}{2}\mathrm{i}^2+\binom{n}{3}\mathrm{i}^3+\ldots+\binom{n}{n}\mathrm{i}^n\\ &=\left(1-\binom{n}{2}+\binom{n}{4}-\ldots\right)+\mathrm{i}\left(\binom{n}{1}-\binom{n}{3}+\ldots\right),\end{aligned}$$

így a valós és az imaginárius rész összehasonlítása az *a)*-beli eredménnyel adja a megoldást.

11.19. *a)* $|\mathrm{i}|=1$, $\arg(\mathrm{i})=\frac{\pi}{2}$, így

b) $|z|=|-16+16\mathrm{i}|=\sqrt{512}=\sqrt{2^9}$, $\arg(z)=\frac{3\pi}{4}$, így

$$z=\sqrt{2^9}\left(\cos\frac{3\pi}{4}+\mathrm{i}\sin\frac{3\pi}{4}\right).$$

a köbgyökei trigonometriai alakban

$$\sqrt[3]{z}=2\sqrt{2}\left(\cos\frac{3\pi+8k\pi}{12}+\mathrm{i}\sin\frac{3\pi}{12}\right),\quad k=0,1,2,$$

ugyanis

$$\frac{\frac{3\pi}{4}+2k\pi}{3}=\frac{3\pi+8k\pi}{12}.$$

A három argumentum $\frac{\pi}{4}$, $\frac{11\pi}{12}$, $\frac{19\pi}{12}$. Csak az elsőt tudjuk könnyen algebrai alakba írni:

$$z_1=2\sqrt{2}\left(\cos\frac{\pi}{4}+\mathrm{i}\sin\frac{\pi}{4}\right)=2\sqrt{2}\left(\frac{1}{\sqrt{2}}+\mathrm{i}\frac{1}{\sqrt{2}}\right)=2+2\mathrm{i}.$$

Egyik lehetőség, hogy szögek összegének trigonometriai függvényeivel kifejezzük a másik két szög, nevezetesen a $\frac{\pi}{4}+\frac{2\pi}{3}$ és $\frac{\pi}{4}+\frac{4\pi}{3}$ szögek függvényeit, de a komplex számok egyszerűbb módszert kínálnak. A három köbgyök egy szabályos háromszöget alkot, ezért ha a $2+2\mathrm{i}$ számot megszorozzuk a harmadik egységgyökökkel, megkapjuk a három keresett gyököt algebrai alakban is:

$$z_1=2+2\mathrm{i},$$

$$z_2=(2+2\mathrm{i})\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}\right)=-\sqrt{3}-1+\mathrm{i}(\sqrt{3}-1),$$

$$z_3=(2+2\mathrm{i})\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}\right)=\sqrt{3}-1+\mathrm{i}(-\sqrt{3}-1).$$

c) A négy gyök: $1+\mathrm{i}$, $1-\mathrm{i}$, $-1+\mathrm{i}$, $-1-\mathrm{i}$.

d) A hat gyök: $\frac{3}{2}+\frac{\sqrt{3}}{2}$, $\sqrt{3}\mathrm{i}$, $-\frac{3}{2}+\frac{\sqrt{3}}{2}$, $-\frac{3}{2}-\frac{\sqrt{3}}{2}$, $-\sqrt{3}\mathrm{i}$, $\frac{3}{2}-\frac{\sqrt{3}}{2}$.

e) $(-27\mathrm{i})^{\frac{1}{6}}=\sqrt{3}\left(\cos(-\frac{\pi}{12}+\frac{k\pi}{3})+\mathrm{i}\sin(-\frac{\pi}{12}+\frac{k\pi}{3})\right)$, ahol $k=0,1,\ldots,5$. A hat argumentum $\pm\frac{\pi}{12}$, $\pm\frac{\pi}{4}$, $\pm\frac{7\pi}{12}$, ezért a $\frac{\pi}{4}$-hez tartozó algebrai alakot megszorozva a hatodik egységgyökökkel, megkaphatjuk a hat algebrai alakot is:

$$\pm\left(\sqrt{\frac{3}{2}}+\sqrt{\frac{3}{2}}\mathrm{i}\right),$$

$$\pm\left(\sqrt{\frac{3}{2}}+\sqrt{\frac{3}{2}}\mathrm{i}\right)\left(\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}\right)=\pm\left(\frac{\sqrt{3}-3}{2\sqrt{2}}+\frac{\sqrt{3}+3}{2\sqrt{2}}\right),$$

$$\pm\left(\sqrt{\frac{3}{2}}+\sqrt{\frac{3}{2}}\mathrm{i}\right)\left(\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}\right)=\pm\left(\frac{\sqrt{3}+3}{2\sqrt{2}}+\frac{\sqrt{3}-3}{2\sqrt{2}}\right).$$

f) Mivel $z=1+\mathrm{i}\sqrt{3}$ esetén $|z|=2$ és $\arg(z)=\frac{\pi}{3}$, így $z=2\left(\cos\frac{\pi}{3}+\mathrm{i}\sin\frac{\pi}{3}\right)$. Másrészt $(\frac{\pi}{3}+2k\pi)/5=\frac{\pi}{15}+\frac{2k\pi}{5}$, így a gyökök:

$$\sqrt[5]{2}\left(\cos(\frac{\pi}{15}+\frac{2k\pi}{5})+\mathrm{i}\sin(\frac{\pi}{15}+\frac{2k\pi}{5})\right),\ k=0,\ldots,4.$$

g) $2\left(\cos(\frac{\pi}{4}+\frac{2k\pi}{5})+\mathrm{i}\sin(\frac{\pi}{4}+\frac{2k\pi}{5})\right),\ k=0,\ldots,4.$

11.20. Legyen $\varepsilon = \cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n}$. A keresett összeg

$$1 + \varepsilon^k + \varepsilon^{2k} + \ldots + \varepsilon^{(n-1)k}.$$

Ha $n = 1$, akkor az összeg 1. Ha $n > 1$ és n osztója k-nak, akkor az összeg n darab 1-es összege, azaz n. Ha n nem osztója k-nak, akkor a mértani sorozat összegképlete szerint

$$1 + \varepsilon^k + \ldots + \varepsilon^{(n-1)k} = \frac{1-\varepsilon^{nk}}{1-\varepsilon^k} = 0,$$

mivel $\varepsilon^{nk} = (\varepsilon^n)^k = 1$.

11.21. Mivel az előző 11.20. feladat eredményét is felhasználva $\varepsilon \neq 1$ esetén

$$(1 + 2\varepsilon + 3\varepsilon^2 + \ldots + n\varepsilon^{n-1})(1-\varepsilon) = -n,$$

ezért az összeg $-\frac{n}{1-\varepsilon}$, ha $\varepsilon \neq 1$, és $\frac{n(n+1)}{2}$, ha $\varepsilon = 1$.

11.22. A feladat a

$$z = (a + b\mathrm{i})(c + d\mathrm{i}) = (ac - bd) + (bc + ad)\mathrm{i}$$

művelet elvégzése 4 helyett 3 szorzással.

$$\begin{aligned} k_1 &= c(a+b) \\ k_2 &= a(d-c) \\ k_3 &= b(c+d) \\ \mathrm{Re}(z) &= k_1 - k_3 \\ \mathrm{Im}(z) &= k_1 + k_2. \end{aligned}$$

Ha a szorzás időigénye legalább háromszorosa az összeadásénak, ami pl. kézi számolásnál megeshet, akkor megéri e módszert használni – a modern kompute reknél nincs lényeges különbség az összeadás és a szorzás időigénye között, ott nincs értelme ezzel próbálkozni.

11.23. *a)* Egyszerű behelyettesítéssel

$$\begin{aligned} &(a + u_1\mathrm{i} + u_2\mathrm{j} + u_3\mathrm{k})(b + v_1\mathrm{i} + v_2\mathrm{j} + v_3\mathrm{k}) \\ &= ab + a\mathbf{v} + b\mathbf{u} - u_1v_1 - u_2v_2 - u_3v_3 \\ &\quad + u_1\mathrm{i}v_2\mathrm{j} + u_1\mathrm{i}v_3\mathrm{k} + u_2\mathrm{j}v_1\mathrm{i} + u_2\mathrm{j}v_3\mathrm{k} + u_3\mathrm{k}v_1\mathrm{i} + u_3\mathrm{k}v_2\mathrm{j} \\ &= ab + a\mathbf{v} + b\mathbf{u} - \mathbf{u}\cdot\mathbf{v} \\ &\quad + u_1v_2\mathrm{k} - u_1v_3\mathrm{j} - u_2v_1\mathrm{k} + u_2v_3\mathrm{i} + u_3v_1\mathrm{j} - u_3v_2\mathrm{i} \\ &= ab + a\mathbf{v} + b\mathbf{u} - \mathbf{u}\cdot\mathbf{v} + \mathbf{u}\times\mathbf{v}. \end{aligned}$$

11.24. Ha $0 = 1$, akkor a gyűrű bármely a elemére $a = 1a = 0a = 0$, azaz a gyűrűnek egyetlen eleme van, a zéruselem.

11.25. Mivel $\mathbb{Q}(\sqrt{2})$ elemei egyúttal valós számok is, így a definíció 2-4. azonosságai fennállnak, elég csak az 1.-et igazolni. Ehhez be kell látni, hogy két $\mathbb{Q}(\sqrt{2})$-beli szám összege és szorzata is $\mathbb{Q}(\sqrt{2})$-beli. Ezt az

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$

és az

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2},$$

összefüggések igazolják.

11.26. Láttuk, hogy a mátrixok összeadása és szorzása nem vezet ki az $n \times n$-es mátrixok halmazából, és az összeadás kommutatív, asszociatív, a zérusmátrix nullelemként viselkedik, és minden mátrixnak van ellentettje. Hasonlóan láttuk, hogy a szorzás asszociatív, és van egységelem (az egységmátrix). Végül az összeadás a szorzásra nézve disztributív. Tehát az $n \times n$-es mátrixok egységelemes gyűrűt alkotnak. Az $n = 1$ esetben magát $\mathbb{F}$-t kapjuk meg, ami test. Ahhoz, hogy $n > 1$ esetén a struktúra nem test, sőt, nem is kommutatív azt kell belátni, hogy mindig találunk egy zérusmátrixtól különböző szinguláris mátrixot és találunk két nem felcserélhető mátrixot.

A csupa 1-esből álló mátrix mindig szinguláris, ui. van legalább két sora, és bármely sora megegyezik az elsővel, tehát az elemi sorműveletek során biztosan keletkezik legalább egy nullasor, tehát e mátrixnak nincs multiplikatív inverze.

Az alább összeszorzott két mátrix, melyeknek csak a bal felső 2×2-es részében van 0-tól különböző elem, sosem felcserélhető, ui.

$$\begin{bmatrix} 1 & 1 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix} = \begin{bmatrix} 1+1 & 1 & \ldots & 0 \\ 1 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix},$$

másrészt

$$\begin{bmatrix} 1 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & \ldots & 0 \\ 1 & 1+1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix}.$$

Hozzá kell még tenni, hogy $1 + 1 = 1$ semelyik testben sem áll fenn, ui. 1-et kivonva $1 = 0$-t kapnánk. (Tudjuk, hogy $\mathbb{F}_2$-ben $1 + 1 = 0$, ahol pedig nem nulla, ott jelölhetjük 2-vel.)

11.27. Először belátjuk, hogy $[x^4 + x + 1 \in \mathbb{F}_2[x]$ irreducibilis. Az látszik, hogy 0 és 1 nem gyök, tehát nincs $\mathbb{F}_2$-beli gyöke, de ez kevés, másodfokúak szorzata meg elvben lehet. Tegyük fel, hogy

$$\begin{aligned} x^4 + x + 1 &= (x^2 + ax + b)(x^2 + cx + d), \\ &= x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd, \end{aligned}$$

ahol $a, b, c, d \in \mathbb{F}_2$. Az együtthatók összehasonlításából az alábbi egyenleteket kapjuk:

$$\begin{aligned} a + c &= 0, & b + ac + d &= 0, \\ ad + bc &= 1, & bd &= 1. \end{aligned}$$

Az utolsó egyenletből $b = d = 1$, így az $ad + bc = 1$ egyenlet szerint $a \neq c$, ugyanakkor az első egyenlet szerint $a = c$, így ez az ellentmondás igazolja, hogy a polinom irreducibilis. Ezután be kell látnunk, hogy x hatványai $\mathbb{F}_2[x]/(x^4 + x + 1)$-ben számolva kiadnak

15 különböző elemet, melyek az $\mathbb{F}_{16}$ nemnulla elemei lesznek. Az alábbi táblázat bal oszlopa mutatja, hogy ez igaz, tehát az $x^4+x+1 \in \mathbb{F}_2[x]$ polinom primitív. A primitív elemet jelölje α. Az α hatványai alapján a 4 elemű résztest csak az $\{0, 1, \alpha^5, \alpha^{10}\}$ elemekből állhat, hisz e halmaz zárt a szorzásra nézve. Könnyű ellenőrizni, hogy az összeadásra, hisz a hatványok legföljebb harmadfokú kifejezéseivel az előző halmaz azonos a $\{0, 1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$ halmazzal. Ha bevezetjük a $\beta = \alpha^2+\alpha$ és a $\bar\beta = \beta+1$ jelölést, melyek mindketten gyökei az $x^2+x+1 \in \mathbb{F}_2[x]$ primitív polinomnak akkor ilyen módon is megkaptuk az $\mathbb{F}_4$ elemeit. (A $\bar\beta$ jelölés analóg ahhoz, ahogy az irreducibilis $x^2+1 \in \mathbb{R}[x]$ gyökei i és $\bar{\mathrm{i}}$ jelöli.) Végül – bár ez nem volt kérdés –, felírhatjuk $\mathbb{F}_{16}$ elemeit az $\mathbb{F}_4$ test bővítésével is. Ehhez az $\mathbb{F}_4[x]/(x^2+x+\beta)$ faktorstruktúrából is eljuthatunk. A táblázatban megadjuk az $\mathbb{F}_{16}$ test elemeit mint $\mathbb{F}_2$ fölötti vektortér elemeit, ahol a koordinátákat a kifejezés együtthatói adják.

	$\mathbb{F}_2[x]/(x^4+x+1)$		$\mathbb{F}_4[x]/(x^2+x+\beta)$		
α^i	$\mathbb{F}_2(\alpha)$	$\mathbb{F}_2^4$	$\mathbb{F}_2(\beta)$	$\mathbb{F}_4(\alpha)$	$\mathbb{F}_4^2$
0	0	0000	0	0	00
α^0	1	0001	1	1	01
α	α	0010		α	10
α^2	α^2	0100		$\alpha+\beta$	1β
α^3	α^3	1000		$\bar\beta\alpha+\beta$	$\bar\beta\beta$
α^4	$\alpha+1$	0011		$\alpha+1$	11
α^5	$\alpha^2+\alpha$	0110	β	β	0β
α^6	$\alpha^3+\alpha^2$	1100		$\beta\alpha$	$\beta 0$
α^7	$\alpha^3+\alpha+1$	1011		$\beta\alpha+\bar\beta$	$\beta\bar\beta$
α^8	α^2+1	0101		$\alpha+\bar\beta$	$1\bar\beta$
α^9	$\alpha^3+\alpha$	1010		$\beta\alpha+\beta$	$\beta\beta$
α^{10}	$\alpha^2+\alpha+1$	0111	$\beta+1$	$\bar\beta$	$0\bar\beta$
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110		$\bar\beta\alpha$	$\bar\beta 0$
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111		$\bar\beta\alpha+1$	$\bar\beta 1$
α^{13}	$\alpha^3+\alpha^2+1$	1101		$\beta\alpha+1$	$\beta 1$
α^{14}	α^3+1	1001		$\bar\beta\alpha+\bar\beta$	$\bar\beta\bar\beta$

11.28. A szorzástábla tekinthető a test szorzástáblájának. Az elemek összeadástáblája ugyanezen $\mathbb{F}_3[x]$-beli polinomok összegeként számolható.

11.30. A behelyettesítés hosszadalmas lenne, például $5^5 = 3125$. Ehelyett alkalmazzuk a Horner-módszert. Először leírjuk a táblázat első sorának második oszlopától kezdődően a *polinom együtthatóit* az ismeretlen monoton csökkenő kitevőjének sorrendjében. Ne feledkezzünk meg a 0 együtthatókról. Példánkban nincs x^2-es tag, ezért x^2 együtthatója 0.

	1	−3	−6	0	−90	3

Ezután a második sor első oszlopába írjuk azt az értéket, amelyet be akarunk helyettesíteni a p polinomba, esetünkben ez 5. Ezután *bemásoljuk* a p polinom főegyütthatóját a második sor második második helyére:

	1	−3	−6	0	−90	3
5	1					

Ezután minden lépésben egy szorzás és egy összeadás következik a tételbeli $c \cdot b_k + a_k$ képlet szerint.

Minden lépést külön sorba írunk, és mellette megadjuk az elvégzendő műveletet is, amelynek eredménye a következő táblázatban meg is jelenik.

	1	−3	−6	0	−90	3	
5	1						$5\cdot 1-3=2$
5	1	2					$5\cdot 2-6=4$
5	1	2	4				$5\cdot 4+0=20$
5	1	2	4	20			$5\cdot 20-90=10$
5	1	2	4	20	10		$5\cdot 10+3=53$
5	1	2	4	20	10	53	

Tehát $p(5) = 53$. Egyúttal le tudjuk olvasni e táblázatból az $(x-5)$-tel való maradékos osztás minden adatát:

$$x^5 - 3x^4 - 6x^3 - 90x + 3$$
$$= (x-5)(x^4 + 2x^3 + 4x^2 + 20x + 10) + 53.$$

11.31. $\mathbb{Z}_5$-ben számolva

	2	1	0	3	2
3	2	2	1	1	0
4	2	0	1	0	

A gyökök 3 és 4, az $(x-3)(x-4)$-gyel való osztás hányadosa $2x^2+1$, ami viszont irreducibilis, mert $\mathbb{Z}_5$-ben nincs gyöke, azaz a $0, 1, 2, 3, 4$ számok behelyettesítése sosem ad nullát modulo 5. A gyöktényezős alak $(x-3)(x-4)(2x^2+1)$, de megadható $= (x+2)(x+1)(2x^2+1)$. alakban is.

11.32. Osztani kell a polinomot polinomot $(x-x_0)$-lal, a maradék az $x-x_0$-ban felírt polinom konstans tagja lesz. A hányadost ismét osztjuk $(x-x_0)$-lal, a maradék az $(x-x_0)$ együtthatója lesz. Az *a)* feladatban a teljes táblázat:

	1	−2	9	5
−2	1	−4	17	−29
−2	1	−6	29	
−2	1	−8		
−2	1			

A színessel jelzett számok lesznek az együtthatók, a polinom tehát $(x+2)^3 - 8(x+2)^2 + 29(x+2) - 29$. Hasonló számolással oldható meg a *b)* feladat is. De

észrevehetjük, hogy az *a)*-ban kapott polinom a *b)*-belivel azonos, így kitalálható a válasz számolás nélkül is: $(x-2)^3-2(x-2)^2+9(x-2)+5$.

11.33. *a)* Az előző feladathoz hasonlóan fejezzük ki a $p(x+2)$ polinomot $x-2$ polinomjaként:

	1	−2	0	0	0
2	1	0	0	0	0
2	1	2	4	8	
2	1	4	12		
2	1	6			
2	1				

Így a polinom $x^4+6x^3+12x^2+8x$.

b) Hasonlóan az előzőhöz:

	1	−10	31	−26	−28	40
2	1	−8	15	4	−20	0
2	1	−6	3	10	0	
2	1	−4	−5	0		
2	1	−2	−9			
2	1	0				
2	1					

A polinom tehát x^5-9x^3.

11.34. Az $(x-1)^2$-nel való oszthatóság azt jelenti, hogy az $p(x)=ax^n+bx^{n-1}+1$ polinomnak az 1 kétszeres gyöke. Ha gyöke, akkor $a+b+1=0$. Ha kétszeres gyöke, akkora deriváltjának is gyöke, azaz $p'(x)=nax^{n-1}+(n-1)bx^{n-2}$, így $=na+(n-1)b=1$. Ezekből $a=n-1$, $b=-n$.

11.35. *a)* Az $x^7-x^6-10x^5+10x^4+31x^3-31x^2-30x+30$ polinom főegyütthatója 1, így minden racionális gyöke egész. A szóba jöhető gyökök $1,2,3,5,6,10,15,30$ és ezek -1-szeresei, de az 1-en kívül egyik sem gyök, ami mutatja e módszer korlátait. A Horner-módszer szerint

	1	−1	−10	10	31	−31	−30	30
1	1	0	−10	0	31	0	−30	0

Egyébként $x^6-10x^4+31x^2-30=(x^2-2)(x^2-3)(x^2-5)$, amit megkaphatnánk az $y=x^2$ helyettesítés után az $y^3-10y^2+31y-30$ polinomból:

	1	−10	31	−30
2	1	−8	15	0
3	1	−5	0	
5	1	0		

b) $30x^3+x^2-6x-1=30(x+\frac{1}{3})(x-\frac{1}{2})(x+\frac{1}{5})=(3x+1)(2x-1)(5x+1)$.

c) $2x^3+15x^2+22x-15=2(x+3)(x-\frac{1}{2})(x+5)=(x+3)(2x-1)(x+5)$.

11.36. Például

$$\begin{aligned}x^3+2x^2+2x+1&=(x-2)(x-4)(x-6)\\&=(x+5)(x+3)(x+1)\\&=(2x-4)(2x-1)(2x-5)\\&=(2x+3)(2x+6)(2x+2).\end{aligned}$$

ui. $\mathbb{F}_7$-ben $2\cdot2\cdot2=1$ és $2(x-2)=2x-4$, $2(x-4)=2x-1$, $2(x-6)=2x-5$, és $-c$ helyett írhatunk $7-c$-t.

11.37.

a) $x^3-3x^2+2=(x-3)(x^2-6)+(6x-16)$,

b) $x^5-3x^3+2x=(x^2-2)(x^3-x)+0$,

c) E feladat polinomosztással is megoldható, de jóval egyszerűbb Horner-módszerrel, az $x=2$ behelyettesítésével. $x^5-3x^3+2x=(x-2)(x^4+2x^3+x^2+2x+6)(x-2)+12$.

11.38. A negatív gyökök száma az $f(-x)$ pozitív gyökeinek számával becsülhető felülről. Kihasználjuk még az alábbi feldatokban, hogy ha egy polinomnak nem minden gyöke valós, akkor a nem valós (komplex) gyökök száma páros.

a) Az előjelek $+\,-\,+-$, a jelváltások száma 3, $f(-x)=-x^3-x^2-x-1$, a negatív gyökök száma 0, tehát vagy 3 pozitív vagy 1 pozitív és két komplex gyöke van ($f(x)=(x^2+1)(x-1)$, így a gyökök 1, $\pm$i).

b) Az előjelszámok azonosak mint az előző pontban, de itt pozitív minden gyök: 1, $\frac{1}{2}(5\pm\sqrt{21})$.

c) $++--+$, a pozitív gyökök száma legfeljebb 2, $f(-x)=-x^5+4x^4-10x^2+x+6$, $-+-+$, a negatívok száma legfeljebb 3, a gyökök $-3,-2,-1,1,1$.

d) $++-+$, 2 előjelváltás, $f(-x)=-x^3+x^2+x+1$, 1 előjelváltás, tehát vagy 2 pozitív és 1 negatív vagy 2 komplex és 1 negatív gyök van (-1.839, 0.42 ± 0.6i).

e) $+--+$, 2 előjelváltás, $f(-x)=-x^3-x^2+x+1$, 1 előjelváltás, így 0 vagy 2 pozitív és 1 negatív gyök van (a gyökök -1, 1, 1).

f) 1 pozitív és 0 vagy 2 negatív gyök (0.54, -0.77 ± 1.12i)

g) 1 pozitív, 2 komplex.

11.39. *a)* Fejezzük ki $p(x)$-et $x-k$ polinomjaként. Mivel k egész, ezért e polinom is egészegyütthatós. Legyen tehát

$$\begin{aligned}p(x)&=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0\\&=a_n(x-k)^n+c_{n-1}(x-k)^{n-1}+\ldots+c_1(x-k)+c_0,\end{aligned}$$

ahol $c_0=f(k)$. Mivel $f(\frac{a}{b})=0$, ezért

$$\begin{aligned}b^nf\left(\frac{a}{b}\right)&=a_n(a-kb)^n+c_{n-1}(a-kb)^{n-1}b+\ldots\\&\quad+c_1(a-kb)b^{n-1}+c_0b^n=0.\end{aligned}$$

Mivel $a-kb$ osztója 0-nak és az utolsót kivéve a bal oldal minden tagjának, ezért az utolsónak is, azaz $a-kb\mid c_nb^n$. De ha a és b relatív prímek, akkor $a-kb$ és b, és így $a-kb$ és b^n is, tehát $f(k)=c_n$ osztható $a-kb$-vel.

b) Alkalmazzuk az előző állítást $k=1$-re, illetve $k=-1$-re.

c) A $p(x) = 8x^5 - 64x^4 + 150x^3 - 168x^2 + 95x - 25$ polinomnak Descartes előjelszabálya szerint minden gyöke lehet pozitív, negatív gyöke nincs. Ha van racionális gyöke, akkor a számláló $1, 5, 25$, míg a nevező $1, 2, 4, 8$ lehet. Mivel $p(1) = -4$, ezért csak az $a = 5$, $b = 1$ jöhet szóba, azaz csak az 5 lehet racionális gyök. A Horner-módszer gyorsan igazolja, hogy valóban az. (A polinom tényezőkre bontása

$$(2x - 1 - \mathrm{i})(2x - 1 + \mathrm{i})(2x - 2 - \mathrm{i})(2x - 2 + \mathrm{i})(x - 5),$$

vagyis valós gyöke sincs több.)