Feladat 1. Adjon meg egy izomorfizmust a $\mathbb{Z}_2[x]/(x^4+x+1)$ és a $\mathbb{Z}_2[x]/(x^4+x^3+1)$ testek között.

Megoldás: Legyen $a := x/(x^4+x+1)$, $b := x/(x^4+x^3+1)$. Az a képének olyan elemet kell választani, aminek $\mathbb{Z}_2$ feletti minimálpolinomja x^4+x+1. A $\mathbb{Z}_2[x]/(x^4+x^3+1)$ testnek b primitív elelme, hiszen nyilván $b^3 \neq 1$ és $b^5 = b^4+b = b^3+b+1 \neq 1$, így b multiplikatív rendje csak 15 lehet. Mivel 2 karakterisztikájú testben vagyunk, minden (nemnulla) elemnek és négyzetének $\mathbb{Z}_2$ feletti minimápolinomja megegyezik. Így a b, b^2, b^4, b^8 nem lesznek jó választások a képének. A b^3 minimálpolinomja $x^4+x^3+x^2+x+1 = \frac{x^5+1}{x+1}$, hiszen $\frac{(b^3)^5+1}{b^3+1} = \frac{0}{b^3+1} = 0$. Ez sem lesz jó a képének, ahogy az ugyanezzel a mininálpolinommal rendelkező b^6, b^{12}, és $b^{24} = b^9$ sem. Maradtak: b^5, b^7, b^{10}, b^{11}, b^{13}, b^{14}. A b^5 és a b^{10} nem jók, mert harmadrendűek, a pedig nem az. A másik négy jó választás. Ezt onnan lehet tudni, hogy mivel a 16 elemű testnek négy automorfizmusa van, négy izomorfizmus lesz, viszont a képe az izomorfizmust egyértelműen meghatározza.

A lista:

0	0	0	0	0
1	1	1	1	1
a	$b^7 = b^2+b+1$	b^{11}	b^{13}	b^{14}
$a+1 = a^4$	$b^{13} = b^2+b$	b^{14}	b^7	b^{11}
a^2	$b^{14} = b^3+b^2$	b^{13}	b^{11}	b^7
$a^2+1 = a^8$	$b^{11} = b^3+b^2+1$	b^7	b^{14}	b^{13}
$a^2+a = a^5$	$b^5 = b^3+b+1$	b^{10}	b^5	b^{10}
$a^2+a+1 = a^{10}$	$b^{10} = b^3+b$	b^5	b^{10}	b^5
a^3	$b^6 = b^3+b^2+b+1$	b^3	b^9	b^{12}
$a^3+1 = a^{14}$	$b^8 = b^3+b^2+b$	b^4	b^2	b
$a^3+a = a^9$	b^3	b^9	b^{12}	b^6
$a^3+a+1 = a^7$	$b^4 = b^3+1$	b^2	b	b^8
$a^3+a^2 = a^6$	$b^{12} = b+1$	b^6	b^3	b^9
$a^3+a^2+1 = a^{13}$	b	b^8	b^4	b^2
$a^3+a^2+a = a^{11}$	b^2	b	b^8	b^4
$a^3+a^2+a+1 = a^{12}$	$b^9 = b^2+1$	b^{12}	b^6	b^3

.

Feladat 2. Hány tizedfokú irreducibilis polinom van $\mathbb{Z}_2$ felett?

Megoldás: Elsőfokű 2 van, másodfokú egy (x^2+x+1), harmadfokú kettő (x^3+x+1 és x^3+x^2+1).

Negyedfokú polinomból 16 van, ebből 8-nak gyöke a 0, a többi felének gyöke az 1. Emellett van még egy polinom, ami az irreducibilis másodfokú négyzete. A maradék három polinom irreducibilis.

A 8 ötödfokúból, aminek nincs gyöke, három olyan van, ami nem irreducibilis (a másodfokú, és valamelyik harmadfokú irreducibilis szorzata). Hat irreducibilis polinom maradt.

A 16 hatodfokúból, aminek nincs gyöke, 3 olyan van, ami a másodfokú és valamelyik negyedfokú irreducibilis szorzata, 1 olyan, ami a másodfokú irreducibilis köbe, és 3 olyan, ami két harmadfokú irreducibilis szorzata. Az irreducibilisek száma 9.

Hetedfok esetén a releváns particiók: $7 = 5+2 = 4+3 = 3+2+2$. Ezekhez a partíciókhoz rendre $6 \cdot 1 = 6$, $3 \cdot 2 = 6$, és 2 polinom tartozik. Így $2^5 - 14 = 18$ irreducibilis polinom van.

Nyolcadfokra: $8 = 6+2 = 5+3 = 4+4 = 4+2+2 = 3+3+2 = 2+2+2+2$. Az ezekhez tartozó polinomok száma: 7, $6 \cdot 2 = 12$, $3+\binom{3}{2} = 6$, 3, 3, 1, az irreducibilisek száma $2^6 - 9 - 6 \cdot 2 - (3 + \binom{3}{2}) - 3 - 3 - 1 = 30$.

Kilencedfokra: $9 = 7 + 2 = 6 + 3 = 5 + 4 = 5 + 2 + 2 = 4 + 3 + 2 = 3 + 3 + 3 = 3 + 2 + 2 + 2$, az irreducibilisek száma $2^7 - 18 - 9 \cdot 2 - 6 \cdot 3 - 6 - 3 \cdot 2 - 4 - 2 = 56$.

Végül tizedfokra: $10 = 8 + 2 = 7 + 3 = 6 + 4 = 6 + 2 + 2 = 5 + 5 = 5 + 3 + 2 = 4+4+2 = 4+3+3 = 4+2+2+2 = 3+3+2+2 = 2+2+2+2+2$, az irreducibilisek száma: $2^8 - 30 - 18 \cdot 2 - 9 \cdot 3 - 9 - (6 + \binom{6}{2}) - 6 \cdot 2 - (3 + \binom{3}{2}) - 3 \cdot 3 - 3 - 3 - 1 = 99$.

Feladat 3. Legyenek p és q prímszámok. Mutassa meg, hogy a $\mathbb{Z}_p$ fölötti q-ad fokú irreducibilis polinomok száma $\frac{p^q-p}{q}$.

Megoldás: Legyen $\mathbf{K}$ egy p^q elemű test. Minden $k \in K$ elemre a $\mathbb{Z}_p(k)$ test közbülső teste a q fokú $\mathbf{K} \,|\, \mathbb{Z}_p$ testbővítésnek. Így $\deg_{\mathbb{Z}_p}(k) = [\mathbb{Z}_p(k) : \mathbb{Z}_p] \in \{1, q\}$. A k nyilván akkor elsőfokú, ha benne van a prímtestben. A többi $p^q - p$ elemnek így q-ad fokú a $\mathbb{Z}_p$ feletti minimálpolinomja. Ezek a minimálpolinomok irreducibilisek $\mathbb{Z}_p$ delett, és egy polinom legfeljebb q elemnek lehet minimálpolinomja. Így van $\mathbb{Z}_p$ felett legalább $\frac{p^q-p}{q}$ irreducibilis polinom.

Ahhoz, hogy megmutassuk, hogy ennél nincs is több, belátjuk, hogy minden $\mathbb{Z}_p$ feletti irreducibilis f polinom pontosan q darab $\mathbf{K}$-beli elemnek minimálpolinomja. Ez ekvivalens azzal, hogy $\mathbf{K}$ felbontási testje f-nek.

Tudjuk, hogy f-nek van egy $\mathbf{L}$ felbontási testje $\mathbb{Z}_p$ felett. Ezt generálják f gyökei, legyenek ezek $x_1, \ldots, x_q$. Mivel $\mathbf{L} = \mathbb{Z}_p(x_1, \ldots, x_q)$, és az összes x_i algebrai $\mathbb{Z}_p$ felett, $\mathbf{L}$ véges test. Mivel minden x_i minimálpolinomja a q-ad fokú f, $[\mathbb{Z}_p(x_i) : \mathbb{Z}_p] = \deg_{\mathbb{Z}_p}(x_i) = q$, így $|\mathbb{Z}_p(x_i)| = p^q$. Tehát minden x_i benne van az $\mathbf{L}$ egy p^q elemű résztestjében. De egy véges testnek maximum egy p^q elemű részteste van, tehát az összes x_i ugyanabban a p^q elemű résztestben van benne, és mivel az x_i-k generáljál $\mathbf{L}$-t, ez a résztest maga $\mathbf{L}$. Tehát $\mathbf{L}$ egy p^q elemű test, vagyis izomorf $\mathbf{K}$-val. Mivel egy $\mathbf{L} \to \mathbf{K}$ izomorfizmus megőrzi $\mathbf{L}$ prímtestét (és így f-et), ez azt jelenti, hogy $\mathbf{K}$ is felbontási teste f-nek.

Feladat 4. Tekintük a következő kódolást:

$$\mathbb{Z}_2^{10} \to \mathbb{Z}_2^{19},\ (x_1, \ldots, x_{10}) \mapsto (x_1, x_1 + x_2, x_2, x_2 + x_3, \ldots, x_9, x_9 + x_{10}, x_{10}).$$

Mennyi ennek a kódolásnak a minimális távolsága? (Vagyis legkevesebb hány bitben tér el két különböző bemenet képe?)

Megoldás: Lineáris kódolásról van szó, ilyenkor a minimális távolság meghatározásához azt kell nézni, hogy nemnulla vektor képe legalább hány nemnulla komponenset tartalmaz.

Jól látható, hogy ez ebben az esetben 2: például a 0000000001 vektor képe csak két 1 bitet tartalmaz, míg ha egy bemenetben $x_i = 1$, akkor x_i bit a képben 1, és vagy az x_{i-1} és az $x_{i-1} + x_i$ bitek léteznek, és egyikük 1, vagy az x_{i+1} és az $x_{i+1} + x_i$ bitek léteznek, és egyikük 1.

Feladat 5. Mennyi az $f = x^4 + x + 1$ polinom által meghatározott $\mathbb{Z}_2^6 \to \mathbb{Z}_2^{10}$ kódolás minimális távolsága? (Vagyis legkevesebb hány bitben tér el két különböző bemenet képe?)

Megoldás: Nem lehet több 3-nál, hiszen például az 1 polinomnak (vagyis a 000001 bitsorozatnak) a képe f, ami csak három monomot tartalmaz.

Lehet ennél kevesebb a minimális távolság? Ha igen, akkor van olyan g polinom, ami legfeljebb ötödfokú, és fg legfeljebb két monomot tartalmaz, vagyis x^n vagy $x^m + x^n$ alakú. Előbbi alakú polinom nyilván nem lehet f-fel osztható. Utóbbi akkor és csak akkor osztható f-fel, ha $1 + x^{n-m}$ osztható vele, így feltehetjük, hogy $m = 1$.

Van olyan $n \leq 9$, amire $x^n + 1$ osztható f-fel? Ezt végig lehet számolni, de a következőképpen is lehet érvelni: $f \mid x^n + 1$ ekvivalens azzal, hogy a $\mathbb{Z}_2[x]/(f)$ testben az $a := x/(f)$ elemre $a^n + 1 = 0$, vagyis $a^n = 1$, vagyis a multiplikatív rendje osztja n-net. Akkor van ezt teljesítő $n \leq 9$, ha a multiplikatív rendje legfeljebb 9. A test 16 elemű, így a multiplikatív rendje a 15 osztója, így elég azt leellenőrizni, hogy a^3, illetve a^5 a testben egyenlő-e 1-gyel. Egyik sem az (lásd az 1. feladatot).

Tehát a minimális távolsága a kódnak 3.

Feladat 6. Tegyük fel, hogy a $p = (x^5+x^2+1)(x^5+x^4+x^3+x^2+1)$ polinom által meghatározott 2-hibajavító $\mathbb{Z}_2^{20} \to \mathbb{Z}_2^{30}$ BCH-kódolást alkalmaztuk egy csatornán, amin legfeljebb 2 bit romlik el. A csatornán beérkezett az

$$10100|11011|01101|00110|11111|10010$$

bitsorozat. Mi volt az üzenet?

Megoldás: A feladat: változtassunk meg a beérkezett f bitsorozatban legfeljebb két bitet úgy, hogy a kapott sorozatnak megfelelő (legfeljebb 29 fokú) polinom osztható legyen p-vel.

A modulo p számolást helyettesíti a modulo $x^5 + x^2 + 1$ és a modulo $x^5 + x^4 + x^3 + x^2 + 1$ számolás (vagyis testbeli számolások). Nézzük az x hatványait ezen modulusok szerint:

1	1	1
x^1	x	x
x^2	x^2	x^2
x^3	x^3	x^3
x^4	x^4	x^4
x^5	x^2+1	$x^4+x^3+x^2+1$
x^6	x^3+x	x^2+x+1
x^7	x^4+x^2	x^3+x^2+x
x^8	x^3+x^2+1	$x^4+x^3+x^2$
x^9	x^4+x^3+x	x^2+1
x^{10}	x^4+1	x^3+x
x^{11}	x^2+x+1	x^4+x^2
x^{12}	x^3+x^2+x	x^4+x^2+1
x^{13}	$x^4+x^3+x^2$	x^4+x^2+x+1
x^{14}	$x^4+x^3+x^2+1$	x^4+x+1
x^{15}	$x^4+x^3+x^2+x+1$	x^4+x^3+x+1
x^{16}	x^4+x^3+x+1	x^3+x+1
x^{17}	x^4+x+1	x^4+x^2+x
x^{18}	$x+1$	x^4+1
x^{19}	x^2+x	$x^4+x^3+x^2+x+1$
x^{20}	x^3+x^2	$x+1$
x^{21}	x^4+x^3	x^2+x
x^{22}	x^4+x^2+1	x^3+x^2
x^{23}	x^3+x^2+x+1	x^4+x^3
x^{24}	$x^4+x^3+x^2+x$	x^3+x^2+1
x^{25}	x^4+x^3+1	x^4+x^3+x
x^{26}	x^4+x^2+x+1	x^3+1
x^{27}	x^3+x+1	x^4+x
x^{28}	x^4+x^2+x	x^4+x^3+1
x^{29}	x^3+1	x^3+x^2+x+1
x^{30}	x^4+x	$x^4+x^3+x^2+x$

Az f maradéka x^5+x^2+1 szerint x^2+x, $x^5+x^4+x^3+x^2+1$ szerint x^3+x^2. Nincs olyan x-hatvány, ami ezt a két maradékot adná, tehát két x-hatvány összegeként kell ezeket a maradékokat előállítani.

Az i-j párok, amelyekre $x^i + x^j \equiv x^2 + x \pmod{x^5 + x^2 + 1}$: 0-11, 1-2, 3-12, 4-28, 5-18, 6-20, 7-30, 8-27, 9-13, 10-26, 14-16, 15-25, 17-22, 21-24, 23-29 ($x^2 + x \equiv x^{19}$, így 19-nek nincs párja).

Az i-j párok, amelyekre $x^i + x^j \equiv x^3 + x^2 \pmod{x^5 + x^4 + x^3 + x^2 + 1}$: 0-24, 1-7, 2-3, 4-8, 5-18, 6-16, 9-26, 10-21, 11-23, 12-28, 13-15, 14-19, 17-25, 20-29, 27-30 ($x^3 + x^2 \equiv x^{22}$, így 22-nek nincs párja).

A közös pár 5-18. Így a 6. és a 19. bit romlott el. Az üzenet megkapásához nincs más dolgunk mint hogy elosszuk a 10100|01011|01101|00100|11111|10010 sorozatnak megfelelő polinomot p-vel. Ezt visszaírva sorozatra, az üzenet:

$$10110|01100|10110|00110.$$