5. Műveletek GF(p^m) felett és Reed–Solomon kódok GF(p^m) felett

Kódolástechnika

Műveletek GF(p^m) felett

q lehet prímszám vagy prímhatvány (p^m, ahol p prím és $m \geq 2$).
Most a $q = p^m$ esettel foglalkozunk.

$$GF(q) = \{0, 1, \ldots, q-1\}$$

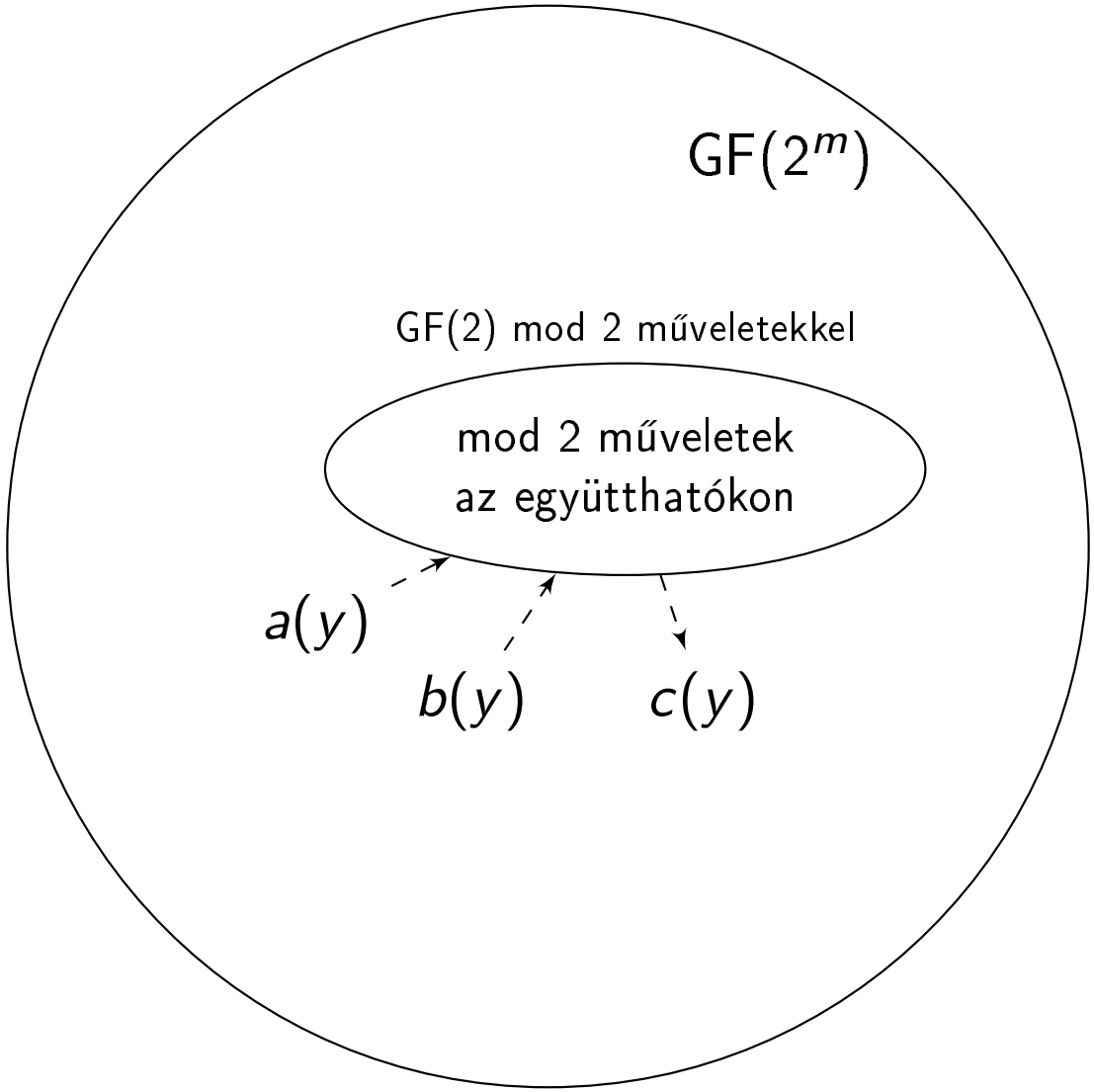
GF(p^m) minden elemének 3 reprezentációja van:

elem	p-áris	polinom
0	$(0 \ldots 00)$	0
1	$(0 \ldots 01)$	1
$\vdots$	$\vdots$	$\vdots$
α	$(\alpha_{m-1}, \ldots \alpha_1, \alpha_0)$	$a(y) = \alpha_{m-1} y^{m-1} + \cdots + \alpha_1 y + \alpha_0$
$\vdots$	$\vdots$	$\vdots$

Az összeadás p-áris mod p történik, ami ekvivalens a polinom összeadással mod p.

A szorzáshoz rögzítünk egy m-edfokú irreducibilis $p(y)$ polinomot.
A szorzás polinomszorzás modulo $p(y)$.

“Nagy test” és “kis test”



Műveletek GF(4) felett

GF(4)-ben az irreducibilis polinom: $p(y) = y^2 + y + 1$ (ez az egyetlen mod 2 együtthatós másodfokú irreducibilis polinom).

GF(4) elemei:

elem	bináris	polinom
0	(00)	$0 \cdot y^1 + 0 \cdot y^0 = 0$
1	(01)	$0 \cdot y^1 + 1 \cdot y^0 = 1$
2	(10)	$1 \cdot y^1 + 0 \cdot y^0 = y$
3	(11)	$1 \cdot y^1 + 1 \cdot y^0 = y + 1$

Példák összeadásra:

$$y + (y + 1) = 2y + 1 = 0 \cdot y + 1 = 1,$$
$$1 + (y + 1) = y + 2 = y.$$

Műveletek GF(4) felett

Irreducibilis polinom: $p(y) = y^2 + y + 1$.

GF(4) elemei:

elem	bináris	polinom
0	(00)	$0 \cdot y^1 + 0 \cdot y^0 = 0$
1	(01)	$0 \cdot y^1 + 1 \cdot y^0 = 1$
2	(10)	$1 \cdot y^1 + 0 \cdot y^0 = y$
3	(11)	$1 \cdot y^1 + 1 \cdot y^0 = y + 1$

Példák szorzásra:

$$y * y = y^2 = 1(y^2 + y + 1) + y + 1 = y + 1,$$
$$y * (y + 1) = y^2 + y = 1(y^2 + y + 1) + 1 = 1.$$

Műveletek GF(4) felett

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

+	0	1	y	y+1
0	0	1	y	y+1
1	1	0	y+1	y
y	y	y+1	0	1
y+1	y+1	y	1	0

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

*	0	1	y	y+1
0	0	0	0	0
1	0	1	y	y+1
y	0	y	y+1	1
y+1	0	y+1	1	y

GF(4) primitív elem és hatványtábla

GF(4) elemei: $\{0, 1, y, y+1\}$.

y a primitív elem. Hatványtábla:

y^0	1
y^1	y
y^2	$y+1$

(Szokás továbbá $0 = y^{-\infty}$-t is írni.)

Ezen kívül teljesül, hogy

$$y^{q-1} = y^3 = 1.$$

Példák:

$$y^2 = 1(y^2 + y + 1) + y + 1 = y + 1,$$
$$y^3 = y^2 \cdot y = (y+1)y = y^2 + y = 1 \cdot (y^2 + y + 1) + 1 = 1.$$

GF(8) reprezentációi

Irreducibilis polinom: $p(y) = y^3 + y + 1$.

GF(8) elemei:

elem	bináris	polinom
0	(000)	0
1	(001)	1
2	(010)	y
3	(011)	$y + 1$
4	(100)	y^2
5	(101)	$y^2 + 1$
6	(110)	$y^2 + y$
7	(111)	$y^2 + y + 1$

GF(8) hatványtábla

Irreducibilis polinom: $p(y) = y^3 + y + 1$.

y a primitív elem. Hatványtábla:

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Példák:

$$y^3 = 1(y^3 + y + 1) + y + 1 = y + 1,$$
$$y^4 = y \cdot y^3 = y(y^3 + y + 1) + y^2 + y = y^2 + y.$$

Szorzás a hatványtábla segítségével

Irreducibilis polinom: $p(y) = y^3 + y + 1$.

y a primitív elem. Hatványtábla:

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Példák:

$$2 * 6 = y * y^4 = y^5 = 7 (= y^2 + y + 1),$$
$$3 * 3 = y^3 * y^3 = y^6 = 5,$$
$$4 * 5 = y^2 \cdot y^6 = y^8 = y = 2.$$

Szorzás GF(8) felett eltolás (shift) regiszterekkel

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Példa. Meg akarjuk szorozni
$\alpha(y) = a_0 + a_1 y + a_2 y^2$-t y-nal.

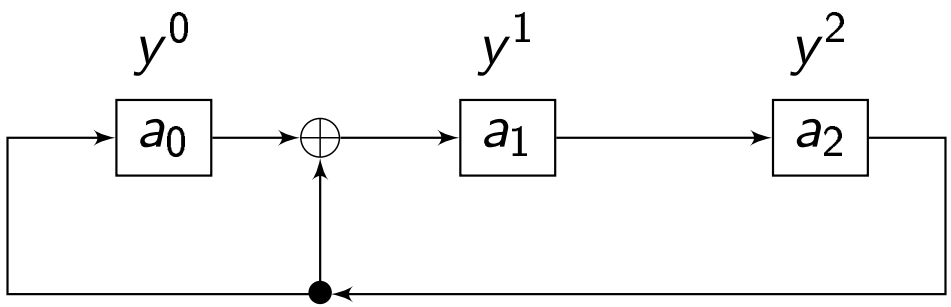
$$y(a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 =$$
$$a_0 y + a_1 y^2 + a_2(y+1) = a_2 + (a_0 + a_2)y + a_1 y^2.$$

Szorzás GF(8) felett eltolás (shift) regiszterekkel

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Példa. Meg akarjuk szorozni
$\alpha(y) = a_0 + a_1 y + a_2 y^2$-t y-nal.

$$y(a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 =$$
$$a_0 y + a_1 y^2 + a_2(y+1) = a_2 + (a_0 + a_2)y + a_1 y^2.$$



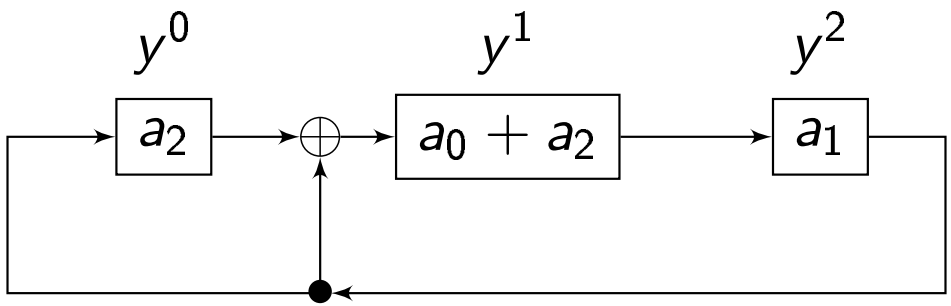
Szorzás GF(8) felett eltolás (shift) regiszterekkel

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Példa. Meg akarjuk szorozni
$\alpha(y) = a_0 + a_1 y + a_2 y^2$-t y-nal.

$$y(a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 =$$
$$a_0 y + a_1 y^2 + a_2(y+1) = a_2 + (a_0 + a_2)y + a_1 y^2.$$

Az órajel következő ütemére:



Szorzás GF(8) felett eltolás (shift) regiszterekkel

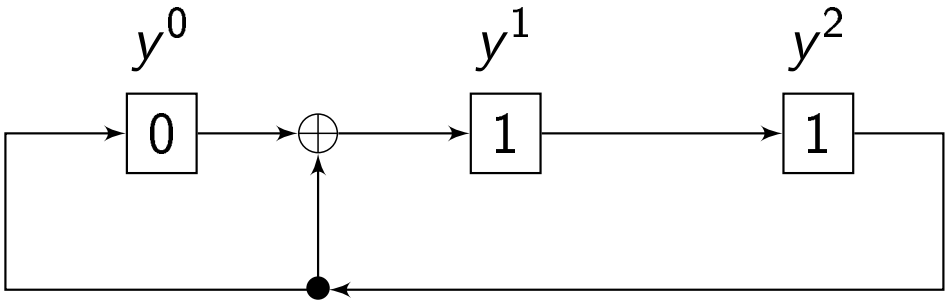
Példa. Ki akarjuk számítani $6 * 2$-t.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

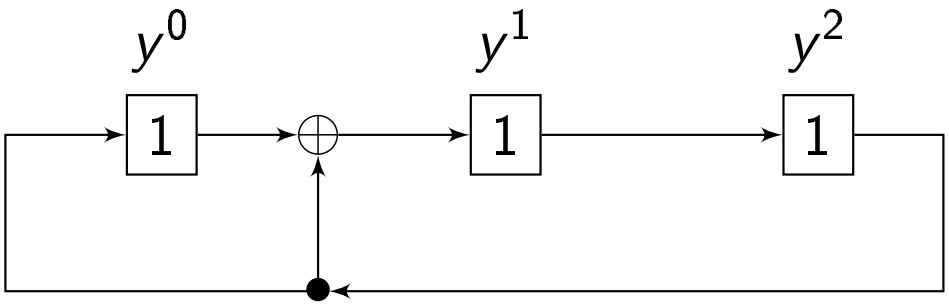
Szorzás GF(8) felett eltolás (shift) regiszterekkel

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Példa. Ki akarjuk számítani $6 * 2$-t.



Az órajel következő ütemére:



Tehát $(y^2+y) * y = y^2+y+1$.

Szorzás GF(8) felett eltolás (shift) regiszterekkel

Példa. Szorzás 4-gyel ($4 = y^2$).

$y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 y^3 + a_2 y^4 =$
$a_0 y^2 + a_1(y + 1) + a_2(y^2 + y) =$
$a_1 + (a_1 + a_2)y + (a_0 + a_2)y^2.$

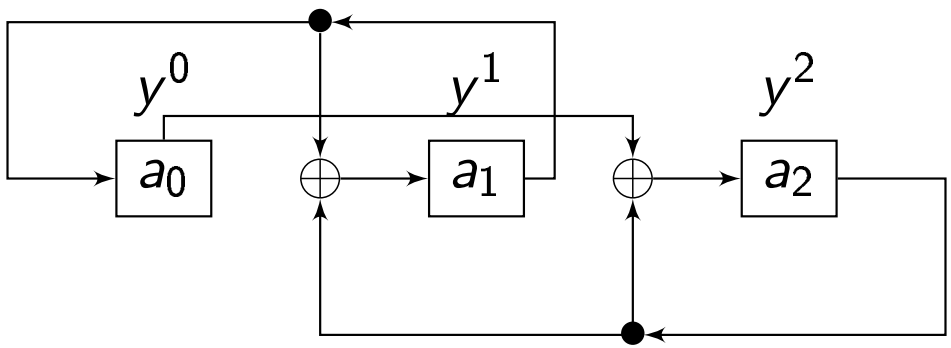
1	1	y^0
2	y	y^1
3	$y + 1$	y^3
4	y^2	y^2
5	$y^2 + 1$	y^6
6	$y^2 + y$	y^4
7	$y^2 + y + 1$	y^5

Szorzás GF(8) felett eltolás (shift) regiszterekkel

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Példa. Szorzás 4-gyel ($4 = y^2$).

$$y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 y^3 + a_2 y^4 =$$
$$a_0 y^2 + a_1(y+1) + a_2(y^2+y) =$$
$$a_1 + (a_1 + a_2)y + (a_0 + a_2)y^2.$$



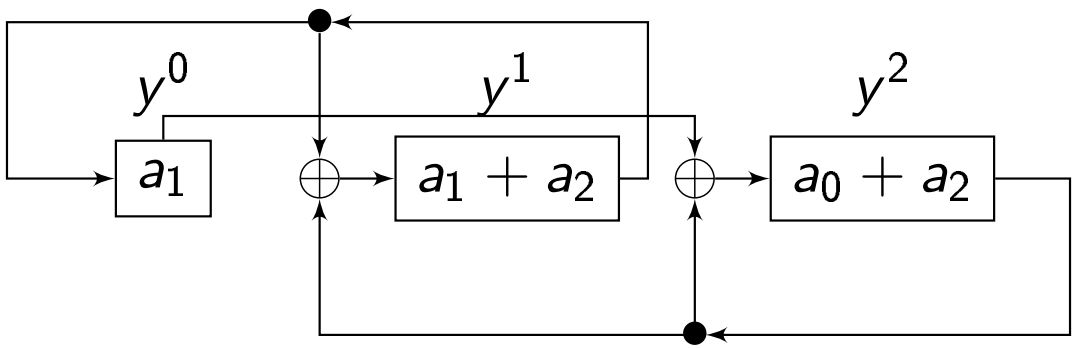
Szorzás GF(8) felett eltolás (shift) regiszterekkel

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Példa. Szorzás 4-gyel ($4 = y^2$).

$$y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 y^3 + a_2 y^4 =$$
$$a_0 y^2 + a_1(y+1) + a_2(y^2+y) =$$
$$a_1 + (a_1 + a_2)y + (a_0 + a_2)y^2.$$

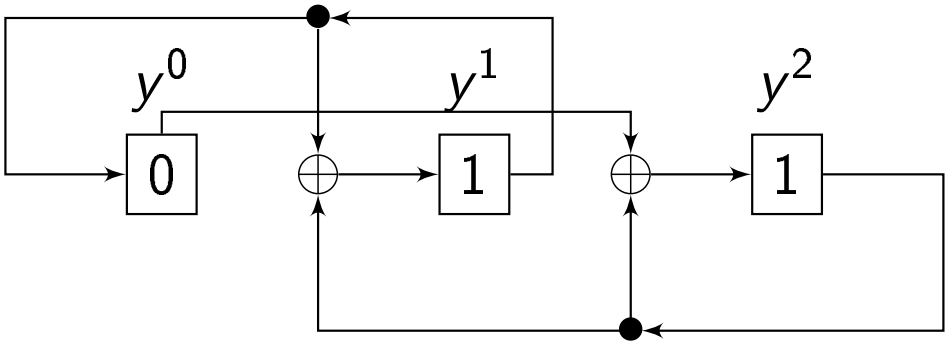
Az órajel következő ütemére:



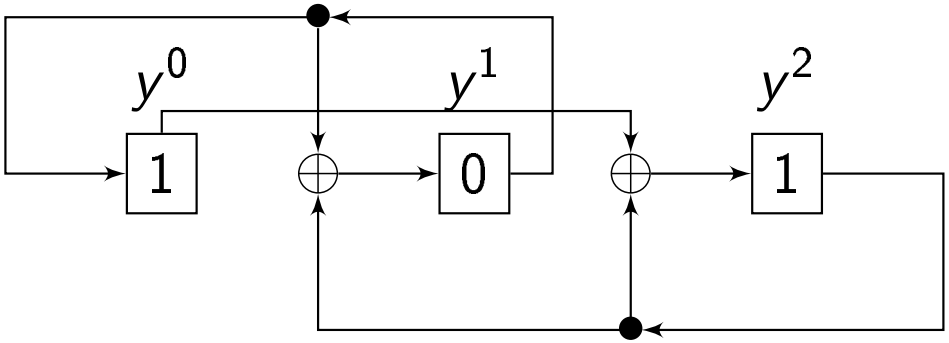
Szorzás GF(8) felett eltolás (shift) regiszterekkel

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Példa. Megszorozzuk y^2+y-t y^2-tel.



Az órajel következő ütemére:



Tehát $(y^2+y)*y^2 = y^2+1$.

1. feladat

(a) Számítsuk ki $3 * 4$-et GF(8)-ban.

(b) Ábrázoljuk a megfelelő eltolás regiszter architektúrát.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

1. feladat

(a) Számítsuk ki $3 * 4$-et GF(8)-ban.

(b) Ábrázoljuk a megfelelő eltolás regiszter architektúrát.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Megoldás.

(a) A hatványtábla alapján:

$$3 * 4 \to y^3 * y^2 = y^5 = y^2 + y + 1$$

1. feladat

(a) Számítsuk ki $3 * 4$-et GF(8)-ban.

(b) Ábrázoljuk a megfelelő eltolás regiszter architektúrát.

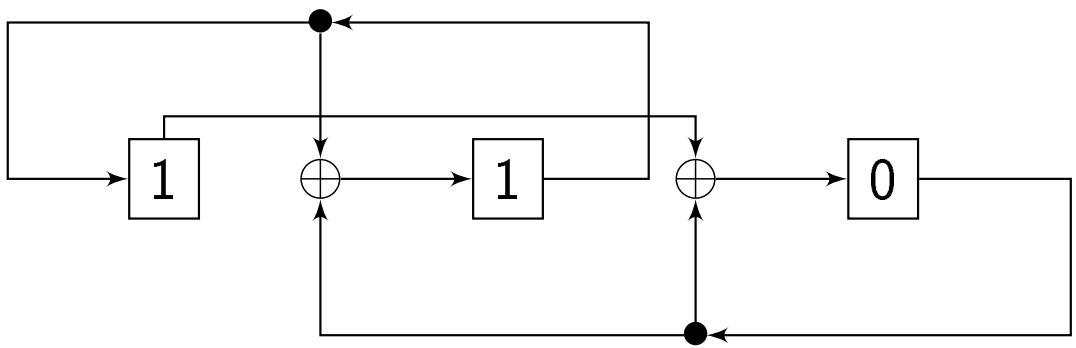
1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Megoldás.

(a) A hatványtábla alapján:

$$3 * 4 \to y^3 * y^2 = y^5 = y^2 + y + 1$$

(b)



1. feladat

(a) Számítsuk ki $3 * 4$-et GF(8)-ban.

(b) Ábrázoljuk a megfelelő eltolás regiszter architektúrát.

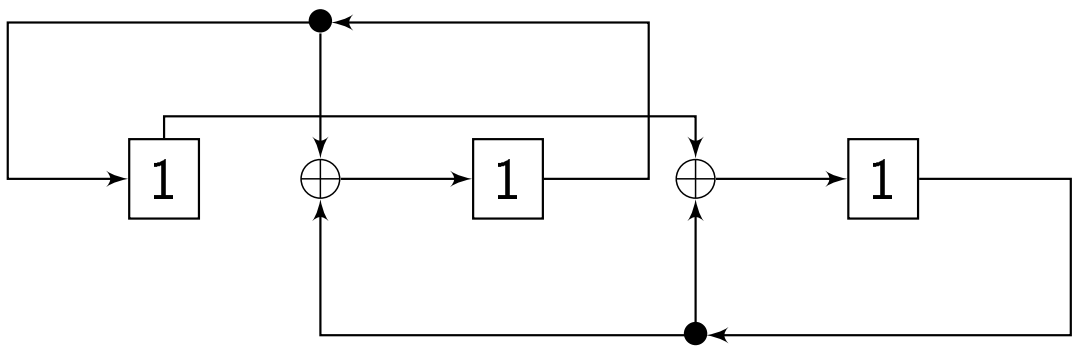
1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Megoldás.

(a) A hatványtábla alapján:

$$3 * 4 \rightarrow y^3 * y^2 = y^5 = y^2 + y + 1$$

(b) A következő időegységkor:



Reed–Solomon kódok GF(p^m) felett

A Reed–Solomon kódok GF(p^m) felett lényegében ugyanúgy működnek, mint GF(q) felett, ha q prím. Ugyanúgy $n = q - 1$, és a primitív elem mindig az y, így a GF(p^m) feletti C(n, k) Reed-Solomon kód generátorpolinomja és paritás ellenőrző polinomja

$$g(x) = \prod_{i=1}^{n-k}(x - y^i), \qquad h(x) = \prod_{i=n-k+1}^{n}(x - y^i).$$

Reed–Solomon kódok GF(p^m) felett

A Reed–Solomon kódok GF(p^m) felett lényegében ugyanúgy működnek, mint GF(q) felett, ha q prím. Ugyanúgy $n = q - 1$, és a primitív elem mindig az y, így a GF(p^m) feletti C(n, k) Reed-Solomon kód generátorpolinomja és paritás ellenőrző polinomja

$$g(x) = \prod_{i=1}^{n-k} (x - y^i), \qquad h(x) = \prod_{i=n-k+1}^{n} (x - y^i).$$

A kód képes

- $n - k$ hibát detektálni, és
- $\left\lfloor \frac{n-k}{2} \right\rfloor$ hibát javítani.

2. feladat

Határozzuk meg annak a GF(8) feletti RS kódnak a paritás ellenőrző polinomját, amely 2 hibát képes kijavítani.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

2. feladat

Határozzuk meg annak a GF(8) feletti RS kódnak a paritás ellenőrző polinomját, amely 2 hibát képes kijavítani.

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Megoldás. A kód paraméterei:

$$n = 8-1 = 7, \qquad t = 2 = \left\lfloor \frac{n-k}{2} \right\rfloor \quad \rightarrow \quad k = 3.$$

$$h(x) = \prod_{i=n-k+1}^{n} (x - y^i) = (x-y^5)(x-y^6)(x-y^7) =$$

$$(x+y^5)(x+y^6)(x+y^7) = (x^2+yx+y^4)(x+1) =$$

$$x^3 + yx^2 + y^4x + x^2 + yx + y^4 = x^3 + y^3x^2 + y^2x + y^4.$$

3. feladat

Egy GF(8) feletti kód generátor polinomja

$$g(x) = x^3 + y^6x^2 + yx + y^6.$$

(a) Mik a kód paraméterei?

(b) Mi a bináris alakban csupa 1-esből álló u üzenethez tartozó kódszó?

(c) Ez egy RS kód?

3. feladat

Egy GF(8) feletti kód generátor polinomja

$$g(x) = x^3 + y^6x^2 + yx + y^6.$$

(a) Mik a kód paraméterei?

(b) Mi a bináris alakban csupa 1-esből álló u üzenethez tartozó kódszó?

(c) Ez egy RS kód?

Megoldás. Az (a) részhez n és k értéke kell. Ha tudnánk, hogy ez egy RS kód, akkor tudnánk, hogy $n = q - 1 = 7$. Kezdjük ezért inkább a (c) résszel!

(c) A RS kódok generátorpolinomja $g(x) = \prod_{i=1}^{n-k}(x - y^i)$ alakú; a kérdés az, hogy a feladatban adott polinom előáll-e ilyen alakban.

3. feladat

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

(c) A megadott polinom harmadfokú (x kitevőjét kell nézni, az y-os tagok az együtthatók részei, úgymond 'számok' GF(8)-ból).

$$g(x) = (x-y)(x-y^2)(x-y^3) =$$
$$= (x^2 - \underbrace{(y+y^2)}_{y^4} x + y^3)(x-y^3) =$$
$$= x^3 + x^2 \underbrace{(-y^3-y^4)}_{(y+1)+(y^2+y)} + x\underbrace{(-y^7+y^3)}_{1+(y+1)=y} + y^6 =$$
$$x^3 + y^6 x^2 + yx + y^6$$

ami megegyezik a megadott polinommal, azaz igen, ez egy RS kód.

3. feladat

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

(c) A megadott polinom harmadfokú (x kitevőjét kell nézni, az y-os tagok az együtthatók részei, úgymond 'számok' GF(8)-ból).

$$g(x) = (x-y)(x-y^2)(x-y^3) =$$
$$= (x^2 - \underbrace{(y+y^2)}_{y^4} x + y^3)(x-y^3) =$$
$$= x^3 + x^2 \underbrace{(-y^3-y^4)}_{(y+1)+(y^2+y)} + x\underbrace{(-y^7+y^3)}_{1+(y+1)=y} + y^6 =$$
$$x^3 + y^6x^2 + yx + y^6$$

ami megegyezik a megadott polinommal, azaz igen, ez egy RS kód.

(a) Mivel RS kód, így $n = q-1 = 7$. Továbbá $\deg(g(x)) = 3 = n-k \rightarrow$ ez egy C(7,4) kód.

3. feladat

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Megoldás.

(b) Az u üzenetvektor $(111, 111, 111, 111)$, mivel $n = 4$. $(111) = y^5$, tehát u polinom alakja

$$u(x) = y^5 + y^5x + y^5x^2 + y^5x^3.$$

Innen

$$\begin{aligned} c(x) &= g(x)u(x) = \\ &= (y^6 + yx + y^6x^2 + x^3)(y^5 + y^5x + y^5x^2 + y^5x^3) = \\ &= \cdots = y^4 + y^3x + y^6x^2 + yx^3 + y^2x^4 + x^5 + y^5x^6 \end{aligned}$$

A kódszó kiolvasható az együtthatókból: $c = (6\,3\,5\,2\,4\,1\,7)$.