Corpuri finite - $GF(p^m)$ sau F_{p^m}

$p(x) = x^3 + x + 1$

Elemente din $GF(2^3)$

$\{0, 1, \alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1\}$

* mult. suport: mț unui nr. prim $|R| = p^m$
  p - caracteristică

* cum construim un corp finit?
  $\forall p$ prim, $m \geq 1$ $\rightarrow \exists$ corp cu p^m el.
  $\rightarrow$ vectori de coef. între 0 și p-1
  - polinoame (toate de gr. m-1 peste $\mathbb{Z}_p$) $\Rightarrow p^m$ el.
  - un pol. ired. de gr. m, cu coef din $\mathbb{Z}_p$

(mț. suport[1], op. notată aditiv[2], opusul față de adunare[3], 0 - el. neutrul față de adunare[4], op. not. multiplicativ[5] = înmulțirea $\rightarrow$ asoc + comut., e[6] - el. neutru față de înmult, op.[7] de inversare față de înmulțire $\rightarrow$ fără 0)
zero nu e inversabil $1 \cdot x^3 + 1x = (1x^3 + 1x + 1) + (0x^3 + 0x^2 + 0x + 0)$

$GF(2^3)$ coef. din $\mathbb{Z}_p = \mathbb{Z}_2 = \{0, 1\}$ adunare în $\mathbb{Z}_2$: $0+0=0$, $1+0=1$, $0+1=1$, $1+1=0$

* adunare: adun coef. pt aceeași putere x^i
  aliniem vectorii și adunăm componentele pe poziții
  reducem mod p
  0: polin. constant 0 sau vect. format numai din zerouri
  opusul: pe componente; opusul modulo p al compon. vectorului; gradul rămâne același

* înmulțire: ex: 2 pol de gr. m-1 $\Rightarrow$ max gr $2m-2$
  modulo f; înm. obișnuită; f gr exact m
  $\Downarrow$ gr. max m-1 (restul)

$1\cdot x^7 + 0\cdot x^6 + 1\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + 1\cdot x^2 + 0\cdot x^1 + 1\cdot x^0$

$(x^7 + x^5 + x^2 + 1) \cdot (x^2 + x)$ $\quad f: x^8 + x^6 + x^5 + x^4 + 1$

165 $\cdot$ 6

$7\,6\,5\,4\,3\,2\,1\,0$

$165 = 1\,0\,1\,0\,0\,0\,1\,0\,1$

$6 = \quad\quad\quad\quad\quad 1\,1\,0$

$= (x^7 + x^5 + x^2 + 1)x^2 + (x^7 + x^5 + x^2 + 1)x$

$= (x^9 + x^7 + x^4 + x^2 + x^8 + x^6 + x^3 + x) \bmod f$

$77 = 1\,0\,0\,1\,1\,0\,1$

$74 = 1\,0\,0\,1\,0\,1\,0$

$1\,0\,0\,1\,1\,0\,0$

aducăm coef. modulo 2 $\quad 0+0 \equiv_2 0$; $1+0 \equiv_2 1$; $0+1 \equiv_2 1$; $1+1 \equiv_2 0$

$0\cdot x^3 + 0\cdot x^2 = (0+0)x^3$ $\quad (0+1)x^4 = x^4$ $\quad 1\cdot x^5 + 1\cdot x^5 = 0$

$(1+1)x^5 = 0x^5$ (2 mod 2)

$\mathbb{Z}_2 = \{0, 1\}$

$\mathbb{Z}_3 = \{0, 1, 2\}$ $\quad 1+2 \equiv_3 3 \equiv_3 0$

$x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x \quad \bmod \; x^8 + x^6 + x^5 + x^4 + 1$

$(\cdot 1 \bmod x)$ $\quad x^9 + x^7 + x^6 + x^5 + x$

$x^8 + x^5 + x^4 + x^3 + x^2$

$x^8 + x^6 + x^5 + x^4 + 1$

$x^6 + x^3 + x^2 + 1$

$= x^6 + x^3 + x^2 + 1$ $\quad \Rightarrow 1001101 = 77$

pol. ired. al 8-lea din lista

$t = (2.m.\ \mathrm{mod}\ 16)$

$158 \times 27 \bmod f_t = \square$ $\quad GF(2^8)$

$x^m \equiv -1 \bmod p$

$(\alpha^i)^m \equiv \alpha^n \bmod p \quad n = \frac{p-1}{2}$

$\alpha^{in} \equiv \alpha^{\frac{p-1}{2}} \bmod p$

$in \equiv \frac{p-1}{2} \bmod (p-1)$

$ax+by=c$, $\exists$ sol în $\mathbb{Z} \Leftrightarrow (a,b) \mid c$

1) $\exists$ sol? $(m, p-1) \mid \frac{p-1}{2}$

2) # sol? $(m, p-1)$ $\quad ax \equiv b \bmod m$ $\quad$ # sol = $= (a,m)$

3) α gen din $\mathbb{Z}_p^*$

4) $i = \left\{ \frac{p-1}{2 \cdot (n, p-1)} + k \cdot \frac{p-1}{(m, p-1)} \mid 0 \le k < (m, p-1) \right\}$

5) $x = \{ \alpha^i \bmod p \}$

$\mathbb{Z}_p^* \rightarrow \exists \alpha$ gen. $\quad \alpha^{\frac{p-1}{2}} \equiv -1 \bmod p$

(?) $n = \log_\alpha (-1)$

$\forall a \in \mathbb{Z}_m^*, \ a^{\phi(m)} \equiv 1 \bmod m$

$\phi(p) = p-1$;

$\alpha^{p-1} \equiv 1 \bmod p$

$(\alpha^{p-1})^1 \equiv 1 \bmod p$

$(\alpha^{p-1})^{\frac{2}{2}} \equiv 1 \bmod p$

$(\alpha^{\frac{p-1}{2}})^2 \equiv 1 \bmod p$

Def ord: cea m. mică putere $\alpha^{\square} \equiv 1 \bmod p$

$z^2 \equiv 1 \bmod p$

$z = 1$; $\quad z = -1$, $\alpha^{\frac{p-1}{2}} \equiv -1 \bmod p$

$\alpha^{\frac{p-1}{2}} \stackrel{?}{\equiv} 1 \bmod p$

$\text{ord}_p(\alpha) = \phi(p) = p-1$

$\frac{p-1}{2} < p-1$