4) (15b) Napište tabulku operace násobení (druhá skupina měla sčítání) v $GF(4)$. Jako ireducibilní polynom použijte $x^2 + x + 1$ a prvky tělesa $GF(4)$ vyjádřete v tabulce jako vektory se souřadnicemi v bázi $\{1, \alpha\}$, kde α je primitivní prvek. (druhá skupina měla jako mocniny primitivního prvku). *Mám něco špatně? Otevři PR na Githubu!*

Postup řešení:

Výpočet primitivních prvků α

Nejdříve je nutno odvodit počet prvků, neboli to v jaké zbytkové třídě se nacházíme. GF(2^2) nám značí zbytkovou třídu $\mathbb{Z}_4$, tedy čtyři prvky celkem. Prvky GF jsou polynomy. Máme zadán generující polynom, pomocí kterého lze odvodit prvky tohoto pole. Řád generujícího polynomu vždy bude shodný s číslem n, na které je umocněna 2 v značení GF(2^n). Číslo n také značí počet bitů, na které se budou kódovat prvky pole.

Prvek	**Notace polynomem**	**Binární kódování**
0	0	00
α^0	1	01
α^1	$x \cdot \alpha^0 = x$	10
α^2	$x \cdot \alpha^1 = x^2 = x + 1$	11

Binární kódování polynomu znamená pouze to, že pro i-tou mocninu x napíšeme 1 pokud tam je a 0 pokud tam není (např. $x^2 + x + 1 \rightarrow 111$, nebo $x^3 + 1 \rightarrow 1001$). Při vytváření prvků pole se vždy začíná nulou, a $\alpha^0 = 1$. Každá další α^i se dá vypočítat jako $x \cdot \alpha^{i-1}$. V tabulce lze vidět takto vypočítanou α^1, kterou lze pohodlně zakódovat na 2 bity. Problém nastává až s $\alpha^2 = x^2$, což se na dva bity zakódovat nedá, na tři ale ano ($x^2 \rightarrow 100$). Nyní je jen potřeba prvek dostat do pole, tedy ho XORovat s generujícím polynomem a oříznout na dva bity:

$$100 \oplus 111 = 011$$

Což je po oříznutí 11. Tabulka je tedy hotová, pokud bychom se pokusili o výpočet α^3, dostali bychom opět α^0.

2a) Tvorba tabulky pro operaci sčítání s mocninami α

Operace sčítání není v GF nic jiného než obyčejný XOR binární reprezentace. Pro tvorbu tabulky je jen pak potřeba najít odpovídající alfu. Pozor, v GF(2^n) je operace sčítání stejná jako odčítání.

$+$	0	α^0	α^1	α^2
0	0	α^0	α^1	α^2
α^0	α^0	0	α^2	α^1
α^1	α^1	α^2	0	α^0
α^2	α^2	α^1	α^0	0

2b) Tvorba tabulky pro operaci násobení s vektory v bázi $\{1, \alpha\}$

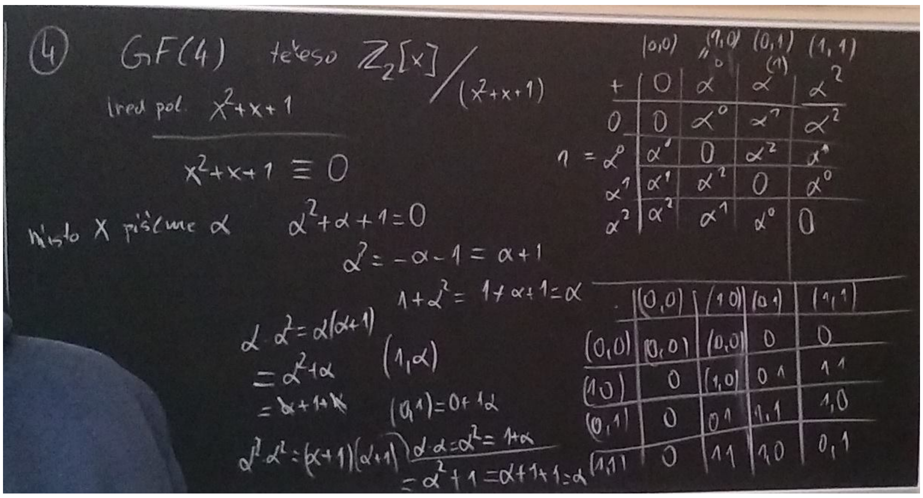
Abych se přiznal, tak netuším, co znamenají ty vektory báze, ale podle vzorového řešení je to jen binární reprezentace s MSB vpravo, tedy opačně než jsem si zapsal nahoře do tabulky.

Násobení v GF(q) funguje tak, že $\alpha^i \cdot \alpha^j = \alpha^{(i+j) mod (q-1)}$. V našem případě, tedy GF(4) např. $\alpha^1 \cdot \alpha^2 = \alpha^{3 mod 3} = \alpha^0 \rightarrow 01$ binárně $\rightarrow (1,0)$ ve vektoru.

$\cdot$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,1)$	$(0,0)$	$(0,1)$	$(1,1)$	$(1,0)$
$(1,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$

Zdrojové materiály:

Slidy k BMS (14,15)



Obrázek 1: Vzorové řešení z konzultací