Čtyřprvkové těleso (označované GF[4] podle anglického „Galois field“) obsahuje kromě povinné 0 a 1 další dva prvky, které nelze získat sčítáním jedničky, protože je to těleso charakteristiky 2, tj. platí $1 + 1 = 0$. Tyto zbývající prvky budeme značit a, b.

Sčítání a násobení v GF[4] je komutativní a je snadné si ho zapamatovat.

- Pokud jde o násobení, je zřejmé, jak se násobí jedničkou i nulou. Zbývá si tedy pamatovat, že a a b jsou vzájemně inverzní, tedy $a \cdot b = 1$. (Mohli bychom tedy ušetřit písmeno b a psát GF[4] $= \{0, 1, a, a^{-1}\}$.) Dále platí $a^2 = b$ a $b^2 = a$.
- V případě sčítání umíme přičítat nulu. Protože je těleso charakteristiky 2, počítá se v něm modulo 2, a je tedy $a + a = b + b = 1 + 1 = 0$. Zbývá si uvědomit, že pokud sečteme dva různé nenulové prvky, dostaneme ten třetí. Tedy $a + 1 = b$, $b + 1 = a$ a konečně $a + b = 1$.

Řešte nad GF[4]**:**

(1)
$$\left(\begin{array}{ccc|c} b & b & b & a \\ 1 & b & b & b \\ 0 & b & b & 0 \end{array}\right)$$

(2)
$$\left(\begin{array}{ccc|c} 1 & a & a & 0 \\ 0 & b & b & 0 \\ a & 1 & 0 & a \end{array}\right)$$

(3)
$$\left(\begin{array}{ccc|c} 1 & b & a & b \\ 1 & 0 & b & b \\ a & a & a & 1 \end{array}\right)$$

(4)
$$\left(\begin{array}{ccc|c} a & 1 & b & 1 \\ 0 & a & 1 & 1 \\ 1 & b & 0 & 0 \end{array}\right)$$

(5)
$$\left(\begin{array}{ccc|c} b & b & a & a \\ b & 1 & 0 & 1 \\ 0 & 1 & a & 0 \end{array}\right)$$

(6)
$$\left(\begin{array}{ccc|c} 0 & b & a & a \\ 0 & b & 0 & b \\ b & b & a & 0 \end{array}\right)$$

(7)
$$\left(\begin{array}{ccc|c} b & a & 0 & a \\ a & 0 & b & b \\ a & a & a & 0 \end{array}\right)$$

(8)
$$\left(\begin{array}{ccc|c} a & 0 & b & a \\ a & a & 0 & 0 \\ b & 1 & 0 & 1 \end{array}\right)$$

(9)
$$\left(\begin{array}{ccc|c} 1 & a & b & b \\ b & 0 & a & 0 \\ a & a & a & a \end{array}\right)$$

(10)
$$\left(\begin{array}{ccc|c} 1 & a & 1 & b \\ b & 1 & 0 & a \\ 1 & b & a & 0 \end{array}\right)$$

(11)
$$\left(\begin{array}{ccc|c} a & a & a & a \\ a & a & b & b \\ b & a & a & 0 \end{array}\right)$$

(12)
$$\left(\begin{array}{ccc|c} b & 0 & a & a \\ 0 & b & 0 & 1 \\ b & a & a & 1 \end{array}\right)$$

(13)
$$\left(\begin{array}{ccc|c} a & a & b & b \\ 0 & b & 1 & a \\ 0 & a & a & 0 \end{array}\right)$$

(14)
$$\left(\begin{array}{ccc|c} b & a & 1 & a \\ 1 & a & 1 & b \\ a & b & a & 1 \end{array}\right)$$

(15)
$$\left(\begin{array}{ccc|c} b & 0 & b & 1 \\ 0 & a & a & 1 \\ b & 0 & a & b \end{array}\right)$$

(16)
$$\left(\begin{array}{cccc|c} b & 1 & 1 & a & b \\ b & 0 & b & 1 & 0 \\ b & a & a & b & 0 \end{array}\right)$$

(17)
$$\left(\begin{array}{cccc|c} 1 & 1 & a & b & b \\ 1 & a & b & b & b \\ 1 & a & a & a & a \end{array}\right)$$

(18)
$$\left(\begin{array}{cccc|c} b & 1 & b & b & 0 \\ a & a & 1 & b & a \\ 1 & a & 0 & b & 1 \end{array}\right)$$

(19)
$$\left(\begin{array}{cccc|c} b & a & a & 1 & b \\ b & 0 & 1 & 0 & 1 \\ 1 & a & 0 & a & b \end{array}\right)$$

(20)
$$\left(\begin{array}{cccc|c} 0 & a & a & b & a \\ 1 & b & 0 & a & a \\ b & 0 & 1 & 1 & 0 \end{array}\right)$$

(21)
$$\left(\begin{array}{cccc|c} a & b & 1 & 0 & a \\ a & b & b & b & b \\ b & b & b & b & b \end{array}\right)$$

(22)
$$\left(\begin{array}{cccc|c} b & a & 0 & 1 & a \\ 1 & b & 1 & b & b \\ a & b & b & 0 & 0 \end{array}\right)$$

(23)
$$\left(\begin{array}{cccc|c} 1 & a & b & 0 & a \\ b & a & a & b & b \\ 0 & b & 0 & a & 0 \end{array}\right)$$

(24)
$$\left(\begin{array}{cccc|c} a & a & b & b & 1 \\ 1 & 1 & b & a & a \\ 1 & b & b & 1 & 1 \end{array}\right)$$

(25)
$$\left(\begin{array}{cccc|c} a & a & a & b & a \\ b & b & a & 1 & 1 \\ a & a & b & a & a \end{array}\right)$$

(26)
$$\left(\begin{array}{cccc|c} a & b & b & a & 1 \\ 1 & b & 0 & a & 1 \\ b & b & b & b & b \end{array}\right)$$

(27)
$$\left(\begin{array}{cccc|c} 0 & 0 & a & a & a \\ 0 & a & a & a & 0 \\ b & 0 & b & a & 0 \end{array}\right)$$

(28)
$$\left(\begin{array}{cccc|c} 0 & 1 & 0 & b & 1 \\ a & 1 & 0 & b & 1 \\ b & b & b & b & b \end{array}\right)$$

(29)
$$\left(\begin{array}{cccc|c} 0 & 1 & b & a & b \\ a & b & b & a & a \\ b & b & a & a & a \end{array}\right)$$

(30)
$$\left(\begin{array}{cccc|c} a & b & b & b & 0 \\ a & a & a & 0 & 1 \\ 0 & a & b & a & 0 \end{array}\right)$$

Řešení:

(1) $(b,0,0)+\langle(0,1,1)\rangle$
(2) $(0,a,a)$
(3) $(b,0,0)+\langle(b,a,1)\rangle$
(4) $(1,a,a)$
(5) $(0,1,b)$
(6) $(b,1,b)$
(7) $(a,a,0)+\langle(a,b,1)\rangle$
(8) $(b,b,1)$
(9) $(1,a,a)$
(10) $(a,b,0)$
(11) $(a,a,1)$
(12) $(b,a,0)+\langle(b,0,1)\rangle$
(13) $(1,1,1)$
(14) $(b,0,0)+\langle(0,b,1)\rangle$
(15) $(0,1,a)$
(16) $(b,a,b,0)+\langle(0,0,a,1)\rangle$
(17) $(b,a,1,0)+\langle(b,a,1,1)\rangle$
(18) $(b,1,1,0)+\langle(b,0,a,1)\rangle$
(19) $(b,0,b,0)+\langle(1,a,b,1)\rangle$
(20) $(a,0,1,0)+\langle(0,b,1,1)\rangle$
(21) $(0,a,b,0)+\langle(0,b,a,1)\rangle$
(22) $(1,b,0,0)+\langle(a,0,1,1)\rangle$
(23) $(0,1,0,a)+\langle(b,0,1,0)\rangle$
(24) $(b,a,1,0)+\langle(0,a,0,1)\rangle$
(25) $(0,0,a,a)+\langle(1,1,0,0)\rangle$
(26) $(a,1,a,0)+\langle(1,1,1,1)\rangle$
(27) $(1,1,1,0)+\langle(a,0,1,1)\rangle$
(28) $(0,1,0,0)+\langle(0,b,a,1)\rangle$
(29) $(0,b,0,0)+\langle(1,1,1,1)\rangle$
(30) $(a,b,a,0)+\langle(b,0,b,1)\rangle$