3-bit 2's complement

$z_2 z_1 z_0$	Z	$2'c$
000	0	0
001	1	1
010	2	2
011	3	3
100	4	-4
101	5	-3
110	6	-2
111	7	-1

Z_{2^k}

$Z_8 = Z \pmod 8 = \{0, \ldots\ldots, 7\}$

$(-1) \pmod 8 = (8-1) \bmod 8 = 7$

Polynomial Functions

$f: Z_4 \to Z_4$

	X: x_2 x_1	Y: y_2 y_1	
0	0 0	0 0	0
1	0 1	0 1	1
2	1 0	0 0	0
3	1 1	0 1	1

$f_1: Y = x^2 \pmod 4$

$x=2 \quad Y=0$

$x=3 \quad Y=3^2 \pmod 4 = 1$

$f_1 \in \mathbb{Z}_4[x]$

x →	Y
0 0	0 0
0 1	0 0
1 0	0 1
1 1	0 1

$Y[1:0] = X[1:0] \gg 1$

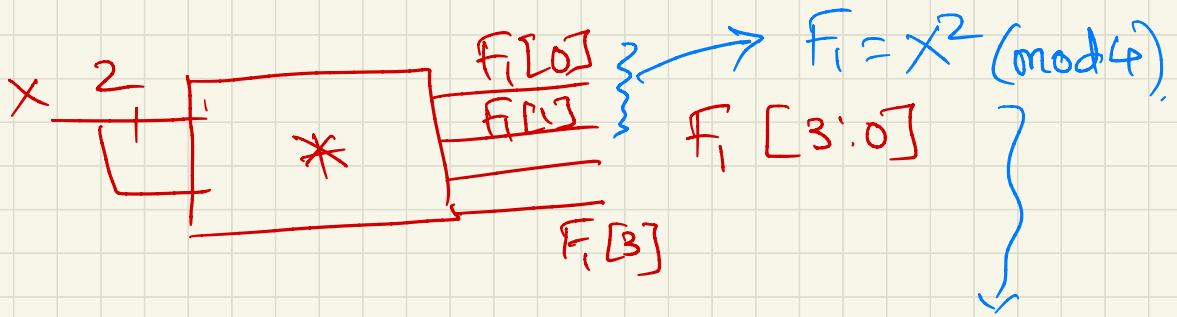
1-bit right shift

$Y = f(x) \pmod 4$

No such $f(x)$ exists.

$\mathbb{Z}_{2^k}$ ⇒ Not a helpful model.

Z.D., non-UFD, cannot apply Euclidean algorithms



$F_1[1:0] = F_1 << 1$

$= 2x^2 \pmod 4$

$2x^2 = 2x \pmod 4$

0 0

1 1

$x=2 \quad 8 = 4 = 0 \bmod 4$

$3 \quad 18 = 6 = 2 \bmod 4$

$2x^2 = 2x \quad \in \mathbb{Z}_4$

$\Rightarrow 2x^2 - 2x = 0 \pmod 4$.

↳ vanishes everywhere in $\mathbb{Z}_4$.

Over $\mathbb{Z}_p[x]$

$f_1, f_2 \in \mathbb{Z}_p[x]$

$f_1 \equiv f_2 \iff$

$f_1 - f_2 \pmod{x^p - x} = 0$

$\iff$ $f_1 - f_2$ is a multiple of $x^p - x$.