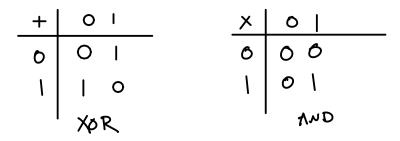
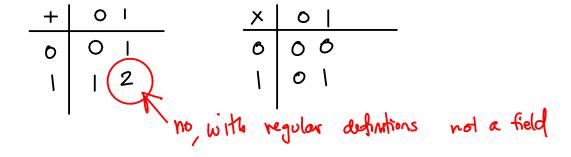
## Lecture 11 - Fields in GF(2) and CRCs

**Exercise 1**: Write the addition and multiplication tables for GF(2). What logic function can be used to implement modulo-2 addition? Modulo-2 multiplication?



**Exercise 2**: What are the possible values of the results if we used values 0 and 1 but the regular definitions of addition and multiplication? Would this be a field?



**Exercise 3**: What is the polynomial representation of the codeword 01101?

$$0x^{4} + [x^{3} + |x^{2} + 0x^{1} + |x^{0}]$$

**Exercise 4**: What is the result of multiplying  $x^2 + 1$  by  $x^3 + x$  if the coefficients are regular integers? If the coefficients are values in GF(2)? Which result can be represented as a bit sequence?

$$(x^{2}+1)(x^{3}+x) = x^{5}+x^{3}+x^{3}+x$$

$$\frac{x^{5}+2x^{3}+x}{x^{5}+0x^{2}+x} \leq \text{Veso Itw/ regular arith}$$

$$\frac{x^{5}+0x^{2}+x}{x^{5}+0x^{2}+1x+0} = \frac{123}{123}$$

$$\frac{0x^{3}+1x^{2}+0x+1}{|x^{2}-0x^{2}-1x|} = \frac{123}{615}$$

$$\frac{0x^{5}-0}{|x^{5}-0x|} = 0$$

$$0x^{5}-0x^{5}-0x^{5} = 0$$

$$0x^{5}+1x^{5$$

**Exercise 5**: If the generator polynomial is  $G(x) = x^3 + x + 1$  and the data to be protected is 1001, what are n - k, M(x) and the CRC? Check your result. Invert the last bit of the CRC and compute the remainder again.

$$x^{3} + 6x^{2} + 0x + |x^{0}|$$

$$\times x^{2}$$

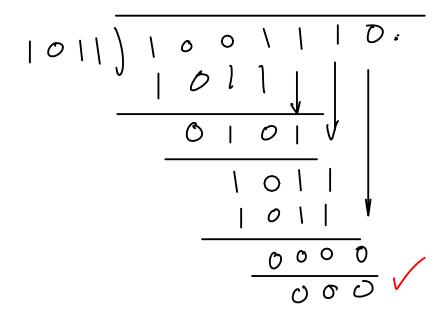
$$= |x^{6} + 0x^{5} + 0x^{4} + |x^{3}|$$

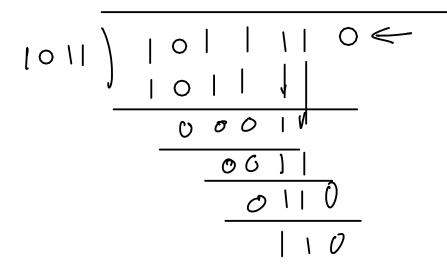
$$+ 8x^{2} + 8x^{4} + 0x^{5}$$

$$M(x) = |\infty \circ / \overline{0 \circ 0}$$

$$\frac{1001000}{1011} = 1010$$
 remainder 110

$$\frac{1}{2}$$
  $\frac{3}{7}$  =  $\chi^3$ 





**Exercise 6**: Is a 32-bit CRC guaranteed to detect 30 consecutive errors? How about 30 errors evenly distributed within the message?

**Exercise 7**: What is the probability that a CRC of length n-k bits will be the correct CRC for a randomly-chosen codeword? Assuming random data, what is the undetected error probability for a 16-bit CRC? For a 32-bit CRC?

$$\frac{1}{Z^{16}} \sim \frac{1}{65 \, \text{k}} \sim 10^{-5}$$

$$\frac{1}{Z^{32}} \sim \frac{1}{4 \, \text{k}^{10}} \sim 10^{-9}$$