

# Lecture 10 - Polynomials in $GF(2)$ and CRCs

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

$\oplus$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

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

	0	1
0	0	1
1	1	2

No. With this definition of addition this is NOT a field: doesn't have closure

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

$$0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0$$

$$= x^3 + x^2 + 1$$

**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  $GF(2)$ ?

regular rules

$$\begin{array}{r} x^2 + 1 \\ \times x^3 + x \\ \hline x^5 + x^3 \\ \hline x^5 + 2x^3 + x \end{array}$$

$GF(2)$  rules

$$\begin{array}{r} x^2 + 1 \\ \times x^3 + x \\ \hline x^5 + x^3 \\ \hline x^5 + 0x^3 + x \\ \hline x^5 + x \end{array}$$

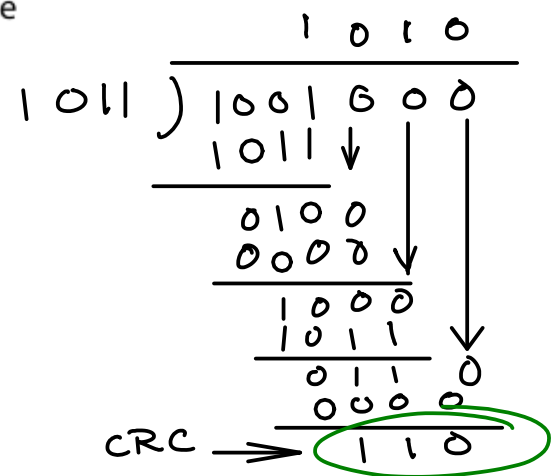
**Exercise 5:** How do we "subtract" a polynomial in  $GF(2)$ ?

add it (same operation)

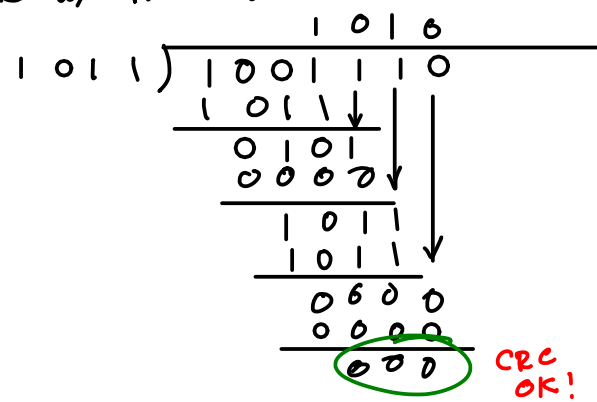
**Exercise 6:** If the generator polynomial is  $G(x) = x^3 + x + 1$  and the message is 1001, what are  $n - k$ ,  $M(x)$  and the CRC? Check your result. Invert the last bit of the CRC and compute the remainder again.

— 1011

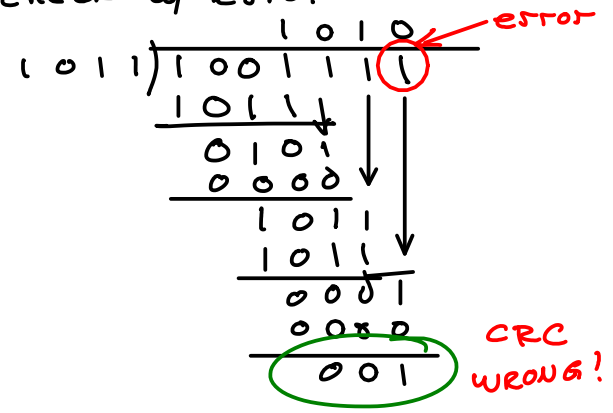
$n - k = 3$   
 number of parity bits  
 = 1 less than bits in  $G(x)$   
 = order of  $G(x)$



check w/ no error:



check w/ error:



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

have  $2^{n-k}$  possible CRCs.

probability of the right CRC =  $\frac{1}{2^{n-k}}$

for 16-bit CRC UEP =  $\frac{1}{65536}$

32 bit CRC UEP =  $\frac{1}{2^{32}} = \frac{1}{4} 10^{-9}$