

# Modulo 2 Arithmetic

Modulo 2 arithmetic is performed digit by digit on binary numbers. Each digit is considered independently from its neighbours. Numbers are not carried or borrowed.

## Addition/Subtraction

Modulo 2 addition/subtraction is performed using an exclusive OR (xor) operation on the corresponding binary digits of each operand.

$$0 \pm 0 = 0; \quad 0 \pm 1 = 1; \quad 1 \pm 0 = 1; \quad 1 \pm 1 = 0$$

## Multiplication

$$\begin{array}{r} 1011 \\ \times 0101 \\ \hline 1011 \\ 0000 \\ 1011 \\ 0000 \\ \hline 0100111 \end{array}$$

## Division

Modulo 2 division can be performed in a manner similar to arithmetic long division. Subtract the denominator (the bottom number) from the leading parts of the numerator (the top number). Proceed along the numerator until its end is reached. Remember that we are using modulo 2 subtraction. For example, we can divide 100100110 by 10011 as follows:

$$\begin{array}{r} \phantom{10011} \overline{10001} \text{ remainder } 101 \\ 10011 \overline{)100100110} \\ \phantom{10011} \underline{10011} \\ \phantom{10011} 10110 \\ \phantom{10011} \underline{10011} \\ \phantom{10011} 101 \end{array}$$

This has the effect that  $X/Y = Y/X$ . For example:

$$\begin{array}{r} \phantom{10011} \overline{1} \text{ remainder } 1010 \\ 11001 \overline{)10011} \\ \phantom{10011} \underline{11001} \\ \phantom{10011} 1010 \end{array}$$

$$\begin{array}{r} \phantom{10011} \overline{1} \text{ remainder } 1010 \\ 10011 \overline{)11001} \end{array}$$

10011  
1010