| galois |

Lab: Cryptol commands and built-in functions

Exercise 1:
Let `x = 42:[6]`. Let `y = 24:[6]`. What is the value of `x+y`? **Note:** at the `Cryptol>` prompt write `let x = 42:[6]` and `let y = 24:[6]`.

Exercise 2:
What is the decimal value of 0b11000110111000010000010010001?

Exercise 3:
Let `x = 42:[6]` and let `y = 24:[_]`. What is the signature of `x` and what is the signature of `y`? What is the signature of `x+y`? Remember, use `:t` to find signatures.

Exercise 4:
What does the safe command do and how is it used?

Exercise 5:
What is the number obtained by negating all the bits of the number 1276439805?

Exercise 6:
Consider the following expression:
`(ratio 1 2)/(ratio 2 3)/(ratio 3 4)/(ratio 4 5)`
This should be computed as follows: `(ratio 1 2)/(ratio 2 3)` is `(ratio 3 4)`, then `(ratio 3 4)/(ratio 3 4)` is `(ratio 1 1)`, then `(ratio 1 1)/(ratio 4 5)` is `(ratio 5 4)`.
But an error message shows up. Fix the above to get the desired result. You can only use the ratios as stated (e.g. do not use `(ratio 5 4)` instead of `(ratio 4 5)`) and you cannot use multiplication!!

Exercise 7:
Use `foldl` to get the same result with input `[(ratio 2 3),(ratio 3 4),(ratio 4 5)]`

Exercise 8:
The operator `(*)` is applied to two numbers and results in the product of the two like this: `((*) 3 4)` is `12`. Verify that `((*) 2)` may be applied to a single number with the result of doubling it.

Exercise 9:
Use `map` to double all the numbers in an input sequence, for example `[3,67,22,43,12,16]`

Exercise 10:
`split [1,2,3,4,5,6,7,8]:[2][4][16]` results in `[[1,2,3,4],[5,6,7,8]]`
`write split on [1,2,3,4,5,6,7,8] to result in [[1,2],[3,4],[5,6],[7,8]]`