| galois |

Lab: Cryptol Types

Exercise 1:
Print the ascii value, in base 10, of the letter '$' using only a sequence?

Exercise 2:
What is `(ratio 34 3)` divided by `(ratio 27 7)`?

Exercise 3:
Write an example of a structure `X` with type `X : [4][3][2][32]`

Exercise 4:
What is the multiplicative inverse of `37 mod 61`?

Exercise 5:
`(ratio -1 2)` shows an error. The type signature for `ratio` is this:

```
ratio : Integer -> Integer -> Rational
```

But

```
-1 : {a} (Ring a, Literal 1 a) => a
```

So how can one create `(ratio -1 2)` from the numbers `-1` and `2`?

Exercise 6:
The attempt to get an infinite sequence of even numbers, beginning with `2`, by using `2*[1...]` fails. Use another approach to produce the intended result.

Exercise 7:
The function split is interesting that it partitions elements of a sequence according to a type signature. Consider

```
Cryptol> split [1,2,3,4,5,6,7,8]

Cannot evaluate polymorphic value.
Type: {n, m, a} (n * m == 8, Literal 8 a, fin m) => [n][m]a
```

From this info, apply split to `[1,2,3,4,5,6,7,8]` to get `[[1,2],[3,4],[5,6],[7,8]]`

Exercise 8:
Show `[True, True, False, True, False, True, False, True]` is the number `213`. That is, do something to the above sequence that causes `213` to be displayed.

Exercise 9:
Let `P` and `Q` be propositions (each takes value `True` or `False`). Show that if `P` implies `Q` and `Q` is `False`, then `P` is False. There are several ways to do this.