galois

Solution to the exercises

```
Exercise 1:
 In file solutions.cry:
   type Circle = { radius : Rational, left : [64], top : [64] }
   a = \{ radius=(ratio 5 2), left=20, top=16 \}
 Running in Cryptol:
   Cryptol> : l solutions.cry
   Loading module Cryptol
   Loading module Main
   Main> :s base=10
   Main> aCircle
   \{ \text{radius} = (\text{ratio 5 2}), \text{ left} = 20, \text{ top} = 16 \}
Exercise 2:
 Add this to solutions.cry:
   areaCircle : Circle -> Rational
   areaCircle b = (b.radius * b.radius * (ratio 355 113))
   aCircleArea = areaCircle aCircle
 Running in Cryptol:
   Main> : l solutions.cry
   Loading module Cryptol
   Loading module Main
   Main> aCircleArea
   (ratio 8875 452)
Exercise 3:
 Add the following to solutions.cry:
   type Displacement = { left : [64], top : [64] }
   disp : Displacement
   disp = { left= 12, top=2 }
   nudgeCircle : Circle -> Displacement -> Circle
   nudgeCircle circle d =
      { radius = circle.radius, left = circle.left+d.left, top = circle.top+d.top }
   movedaCircle = nudgeCircle aCircle disp
   newDisp : Displacement
   newDisp = \{ left= -32, top=2 \}
   secondTry = nudgeCircle aCircle newDisp
 Running in Cryptol:
   Main> : l solutions.cry
   Loading module Cryptol
   Loading module Main
   Main> movedaCircle
   \{ \text{radius} = (\text{ratio 5 2}), \text{ left} = 32, \text{ top} = 18 \}
   Main> secondTry
   \{\text{radius} = (\text{ratio } 5 \ 2), \text{ left} = 18446744073709551604, \text{ top} = 18\}
```

Exercise 4:

```
Add the following to solutions.cry (recall import Float is at the top of the file):
 type BMI = { weight : Float16, height : Float16 }
type BMIimp = { weight : Float16, feet : Float16, inches : Float16 }
 calcBMI : BMI -> Float16
 calcBMI bmi = bmi.weight /. bmi.height /. bmi.height * 10000
 calcBMIimp : BMIimp -> Float16
 calcBMIimp bmi = bmi.weight /. (bmi.feet*12+bmi.inches) /.
                    (bmi.feet*12+bmi.inches) * 703
                                                       // for testing
 t1 = { weight=80, height=174 }
 t2 = { weight=180.0, feet=5.0, inches=8.5 } // for testing
Running in Cryptol:
 Main> : l solutions.cry
 Loading module Cryptol
 Loading module Float
 Loading module Main
 Main> calcBMI t1
 0x1a.6c
 Main> calcBMIimp t2
 0x1a.f8
```