Homework 8

1. Polynomial practice

   for
   $p(x) = x^3 - 5x^2 - 4x + 20 = 0$

   a) find an integer root a , i.e. $p(a) = 0$ (clue a < 7)

   b) write this in terms of a lower degree polynomial $q(x)$
   such as $p(x) = (x - a)q(x)$
   What are the degrees of $p(x)$ and $q(x)$?
   $p(x)$ is degree 3 and $q(x)$ is degree 2
   Note we are doing this over the real numbers, for zkps we would use a finite field

2. Listen to the Zero Knowledge podcast about the evolution of SNARKS

a) using Ruffini:

	1	−5	−4	20
−2		−2	14	−20
	1	−7	10	0

1, −1
2, −2
4, −4
5, −5

$x = -2$

$p(-2) = (-2)^3 - 5(-2)^2 - 4(-2) + 20 = 0$

$p(-2) = -8 - 20 + 8 + 20 = 0$ //

b)

$q(x) = x^2 - 7x + 10$

$a = -2$

$p(x) = (x - (-2))(x^2 - 7x + 10)$

$p(x) = (x+2)(x^2 - 7x + 10)$

$= x^3 - 7x^2 + 10x + 2x^2 - 14x + 20$

$= x^3 - 5x^2 - 4x + 20$ //