Homework 13

1. Imagine you get the following trace

   0,2,4,6,8,10,12
   from your program (which simply doubles the previous value.)

   Write out the constraints for this trace, in terms of i, j

2. Polynomial practice

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

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

   Note we are doing this over the real numbers, for zkps we would use a finite field

3. Taking the trace from question 1
   If the prover presented the polynomial
   $p(x) = -\frac{1}{30}x^5 + \frac{13}{24}x^4 - \frac{13}{4}x^3 + \frac{215}{24}x^2 - \frac{553}{60}x + 5$
   as representing that trace, should the verifier accept it ?

   If you get really stuck you can use WolframAlpha to help