

Assignment 2

September 29, 2009

1. Give the steps of the naive Euclidean division algorithm for the division of $3+x-x^2+x^3$ by $x-1$.
2. Give the steps of the fast Euclidean division algorithm for the division of $3+x-x^2+x^3$ by $x-1$. You should get the same result as in the previous problem.

For all such computational questions, you are free to do the computations by hand, or to implement the algorithm and run it. If you implement in a language like C or java, you can use `floats` or `ints` as coefficients.

3. Consider a power series

$$F = 1 + f_1x + f_2x^2 + \dots .$$

In this problem, you are to prove that there exists a unique power series

$$G = 1 + g_1x + g_2x^2 + \dots$$

such that $F = G^2$; we will write $G = \sqrt{F}$. To prove it, show that you can compute the coefficients of G one after the other in a unique manner, by extracting coefficients in the equality $F = G^2$. How many operations does it take to compute n terms of G ?

4. Give the first 10 terms of $\sqrt{1+2x}$; your result can be with either floating point or exact coefficients. How did you compute it?

You can use any kind of trick.

5. You are going to write down a specific Newton iteration for computing G as in problem 3. We actually use an indirect computation, by computing $H = 1/G$ first.

(a) Prove that H satisfies $F - 1/H^2 = 0$.

(b) Show that the Newton iteration for the previous equation is $H_0 = 1$ and

$$H_{(i+1)} = \frac{H_{(i)}(3 - FH_{(i)}^2)}{2} \text{ rem } x^{2^{i+1}}$$

- (c) (bonus difficult question, not needed to get 100%) Prove correctness: if $H_{(i)}$ is such that $H_{(i)} = H \bmod x^{2^i}$, prove that $H_{(i+1)}$ is such that $H_{(i+1)} = H \bmod x^{2^{i+1}}$.
- (d) Taking correctness for granted, prove that the first n terms of H can be computed in $O(M(n))$ operations. You don't have to redo the proofs given on the slides.
- (e) Use the result on inverse computation to prove that the first n terms of G can be computed in $O(M(n))$ operations.

6. How much time did you spend on the assignment?