

Midterm

November 5, 2008

1. Give the steps of Karatsuba's multiplication with inputs $A = 3 + x$ and $B = 1 - x$.
2. Define $\varphi = 1 + \sqrt{7}$.
 - Find a polynomial P of degree 2 with rational coefficients such that $P(\varphi) = 0$.
 - Use Euclidean division and XGCD computation to express $\varphi/(2\varphi + 1)$ in the form

$$a_0 + a_1\varphi,$$

with a_0, a_1 rational numbers.

- More generally, consider a ψ for which you are given an irreducible polynomial Q of degree d , with rational coefficients, and with $Q(\psi) = 0$. How could you rewrite an expression such as

$$\frac{e_0 + e_1\psi + \cdots + e_{d-1}\psi^{d-1}}{f_0 + f_1\psi + \cdots + f_{d-1}\psi^{d-1}},$$

where all e_i and f_i are rationals? Using the results given for the complexity of Euclidean division and XGCD computation, give the complexity of finding the simplified form (in terms of d).

3. Consider a power series

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

In this problem, we compute the unique power series

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

such that $F = G^2$. We 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

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

I do not ask you to prove correctness of the iteration.

- (c) Using the results seen in class about the complexity of Newton iteration, prove that $H \bmod x^n$ and then $G \bmod x^n$ can be computed in $O(M(n))$ operations.

4. We continue with

$$F = 1 + f_1x + f_2x^2 + \cdots,$$

and we now choose an integer ℓ . In this problem, we compute the unique power series

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

such that $F = G^\ell$. As before, we use an indirect computation, by computing $H = 1/G$ first.

- (a) Warmup question (independent of the Newton iteration context): given a series

$$S = 1 + s_1x + s_2x^2 + \cdots + s_{n-1}x^{n-1},$$

show that $S^\ell \bmod x^n$ can be computed in $O(M(n) \log(\ell))$ operations.

Hint: use the idea of binary powering.

- (b) Prove that H satisfies $F - 1/H^\ell = 0$.
 (c) Show that the Newton iteration for the previous equation is $H_0 = 1$ and

$$H_{(i+1)} = \frac{H_{(i)}(\ell + 1 - FH_{(i)}^\ell)}{\ell} \bmod x^{2^{i+1}}.$$

I do not ask you to prove correctness of the iteration.

- (d) Using the results seen in class about the complexity of Newton iteration, and the warmup question, give the complexity of computing $H \bmod x^n$ and then $G \bmod x^n$ (your answer should depend on n and ℓ).