Math 288X: Algorithms in Algebra and Number Theory

Fall 2021

Problem set #1

Problem 1 (Karatsuba's algorithm)**.** Let R be a commutative ring. Consider the following algorithm:

1: **function** KARATSUBA($f, g \in R[X]$)
2: Let $n = \max(\deg(f), \deg(g))$.
3: Write $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{i=0}^{n} b_i X^i$.
4: **if** $n = 0$ **then**
5: **return** $a_0 \cdot b_0$.
6: **else**
7: Write $f(X) = p(X^2) + X \cdot q(X^2)$ and $g(X) = r(X^2) + X \cdot s(X^2)$ with polynomials $p, q, r, s \in R[X]$.
8: Compute $u =$ KARATSUBA(p, r).
9: Compute $v =$ KARATSUBA(q, s).
10: Compute $w =$ KARATSUBA($p + q, r + s$).
11: **return** $u(X) + X \cdot (w(X) - u(X) - v(X)) + X^2 \cdot v(X)$.
12: **end if**
13: **end function**

a) Show that KARATSUBA(f, g) $= f \cdot g$.

b) Show that for large n, KARATSUBA(f, g) has running time $\theta(n^{\log(3)/\log(2)})$ on an $\mathcal{O}(\log n)$-bit RAM with $\mathcal{O}(1)$ arithmetic in R.

c) What's wrong with the following proof by induction that the running time is $\mathcal{O}(n + 1)$? The claim is clear for $n = 0$. Assume we've shown the claim for all $n' < n$. Now, lines 8–10 have running time $\mathcal{O}(3(\max(\deg(p), \deg(q), \deg(r), \deg(s)) + 1)) = \mathcal{O}(n+1)$ by induction. The remaining lines have running time $\mathcal{O}(n + 1)$, so the total running time is $\mathcal{O}(n + 1)$, completing the induction.

Problem 2. Assume you're given an algorithm that can multiply two polynomials $f, g \in R[X]$ of degrees less than n in time $T(n)$.

a) Describe an algorithm that can multiply two polynomials $f, g \in R[X]$ of degrees less than n and m with $n \geqslant m \geqslant 1$ in time $\mathcal{O}(\frac{n}{m} \cdot T(m))$.

b) Describe an algorithm that can multiply two polynomials $f, g \in R[X, Y]$ in which every monomial $X^i Y^j$ satisfies $i < n$ and $j < m$ in time $\mathcal{O}(T(2nm))$.
(Hint: Consider the polynomials $f(X, X^{2n-1})$ and $g(X, X^{2n-1})$.)

Problem 3. a) Let $m \geqslant n \geqslant k \geqslant 0$ be integers and let $g \in \mathbb{F}_p[X]$ be a polynomial of degree n. Choose a polynomial $f \in \mathbb{F}_p[X]$ with $\deg(f) < m$ uniformly at random. Show that $\deg(f \bmod g) < k$ with probability $p^{-(n-k)}$.

b) For any polynomials f, g, let $s(f, g)$ be the number of steps taken by the Euclidean algorithm on f, g. (Specifically, $s(f, g) = 0$ if $g = 0$, and $s(f, g) = s(g, f \bmod g) + 1$ otherwise.) Let $n \geqslant 1$. Choose polynomials $f, g \in \mathbb{F}_p[X]$ with $\deg(f), \deg(g) < n$ uniformly at random. Show that the expected value of $s(f, g)$ is $\Omega(n)$. (In other words: there is a constant $C > 0$, independent of n and p, such that $\mathbb{E}(s(f, g)) \geqslant C \cdot n$.)

Problem 4. Show Lemma 1.1.1: Let $\zeta_n \in R$ be a root of the n-th cyclotomic polynomial ϕ_n. Then:

a) $\zeta_n^n = 1$.

b) For any $d \mid n$, ζ_n^d is a root of $\phi_{n/d}$.

c) For any $a \in \mathbb{Z}$,

$$\sum_{i \in \mathbb{Z}/n\mathbb{Z}} \zeta_n^{ai} = \begin{cases} 0, & a \not\equiv 0 \mod n, \\ n, & a \equiv 0 \mod n. \end{cases}$$