Math 288X: Algorithms in Algebra and Number Theory

Fall 2021

Problem set #3

Problem 1. Show that for a real number $x \in \mathbb{R}$, you can compute $1/x$ up to a relative error of at most 2^{-n} in time $\mathcal{O}(n)$ (using only the first n nonzero digits of x) on an $\mathcal{O}(\log n)$-bit RAM.

Problem 2 (Binary gcd)**.**

a) Let $x, y \in \mathbb{Z}$ with $v_2(x) < v_2(y) < \infty$. Show that there is a unique pair (q, r) satisfying $x = qy + r$ where $q \in \mathbb{Q}$ is a rational number whose denominator is a power of 2 satisfying $|q| < 1$, and r is an integer with $v_2(r) > v_2(y)$. We will write $q = \lfloor x/y \rfloor_2$ and $r = x \bmod_2 y$.

b) Show that you can compute $\lfloor x/y \rfloor_2$ and $x \bmod_2 y$ for (binary) integers with $\leqslant n$ bits in time $\mathcal{O}(n)$ on an $\mathcal{O}(\log n)$-bit RAM.

c) Let a_0 be an odd integer and let a_1 be an even integer. As long as $a_{i+1} \neq 0$, let $a_{i+2} = a_i \bmod_2 a_{i+1}$. Assume that a_0 and a_1 have at most n (binary) digits. Show that this process terminates after $\mathcal{O}(n)$ steps. (For some $k \leqslant \mathcal{O}(n)$, we have $a_{k+1} = 0$.)
Hint: Think about how quickly the sequence $a_0, a_1, a_2, \ldots$ can grow. How quickly must it grow if $a_i \neq 0$?

d) Show that if $a_k \neq 0$, $a_{k+1} = 0$, then the greatest common divisor of a_0 and a_1 is the odd part $a_k \cdot 2^{-v_2(a_k)}$ of a_k.

Like before, we assume that arithmetic in K can be done in $\mathcal{O}(1)$.

Problem 3.

a) Let $f, g \in K[X]$ be polynomials of degree at most $n \geqslant 0$. Show that you can compute $\gcd(f, g)$ in time

$$\mathcal{O}\left(\mu(n)\left(1 + \log\left(\frac{n+1}{m+1}\right)\right)\right),$$

where $m \geqslant 0$ is the degree of $\gcd(f, g)$.

b) Given polynomials $f_1, \dots, f_k \in K[X]$ of degree at most n, show that you can compute $\gcd(f_1, \dots, f_k)$ in time $\mathcal{O}(\mu(n)(k + \log(n+1)))$.

Problem 4 (Chinese remainders)**.** Let $f_1, \dots, f_k, r_1, \dots, r_k \in K[X]$ be polynomials of degree at most $n \geqslant 0$ and assume that $f_1, \dots, f_k$ are pairwise coprime. Show that you can find a polynomial $g \in K[X]$ of degree less than nk such that $g \equiv r_i \mod f_i$ for all i in time $\mathcal{O}(\mu(nk)\log(nk)\log(k))$ (for large n, k).

Problem 5. a) Show that for large n, the integer $n!$ has $\theta(n \log n)$ digits.

b) Show that you can compute $n!$ in time $\mathcal{O}(n \log n)$ on an $\mathcal{O}(\log n)$-bit RAM.
Hint: Compute $\binom{2m}{m} = \frac{(2m)!}{m!^2}$. How often does a prime p divide $\binom{2m}{m}$?