Math 288X: Algorithms in Algebra and Number Theory

Fall 2021

Problem set #8

Problem 1. Check that the algorithm described in Theorem 14.3 indeed has running time $\widetilde{\mathcal{O}}(n^{10} + n^8(\log B)^2)$.

Problem 2. Consider a random access machine with the following additional operation: Set register r_i to 0 or 1 uniformly at random (and independently of previous random numbers).

a) Show that for any $n \geqslant 2$, you can compute a uniformly random element of $\{1, \ldots, n\}$ in expected time $\mathcal{O}(\log n)$ on an $\mathcal{O}(\log n)$-bit RAM as above.

b) Show that there is no number T and algorithm that returns a uniformly random element of $\{1, 2, 3\}$ in (guaranteed) time $\leqslant T$ on a RAM as above.

Problem 3. a) Show that every Carmichael number is odd.

b) Show that $n \geqslant 1$ is a Carmichael number if and only if it is squarefree and $p - 1 \mid n - 1$ for every prime p dividing n.

c) Show that a Carmichael number cannot be divisible by exactly two prime numbers.

Problem 4. Show that $n \geqslant 2$ is prime if and only if $(X + 1)^n = X^n + 1$ in the polynomial ring $(\mathbb{Z}/n\mathbb{Z})[X]$.

Problem 5. Show that the algorithm described in the proof of Lemma 15.9 actually finds a proper divisor with probability at least $\frac{1}{2}$.

Problem 6 (Pépin's test)**.** Let $n \geqslant 1$ and consider the Fermat number $F_n = 2^{2^n} + 1$. Show that F_n is prime if and only if $3^{(F_n-1)/2} \equiv -1 \mod F_n$. **Hint:** Use quadratic reciprocity. If the congruence holds, then what is the order of 3 modulo F_n?

Problem 7 (Hermite normal form)**.** Let R be a principal ideal domain and assume we can do arithmetic in R in $\mathcal{O}(1)$. Furthermore, assume that for any $x, y \in R$, we can compute $g = \gcd(x, y)$ and elements $a, b \in R$ with $g = ax + by$ (as well as x/g and y/g) in $\mathcal{O}(1)$. Consider an $m \times n$-matrix A with entries in R. We say that A is in *Hermite normal form* if no two nonzero rows in A have the same number of leading zeros. Show that we can in time $\mathcal{O}(m^2 n)$ compute a matrix $B \in \mathrm{SL}_m(R)$ such that BA is in Hermite normal form.