READING: Please read the handout on irreducibility of polynomials (last chapter of “Algebra review” handout.)

Recall that $\alpha$ is an algebraic number if $\alpha$ is a root of some nonzero polynomial $f$ with rational coefficients. If $f$ has the lowest possible degree then we call $f$ minimal polynomial of $\alpha$. The degree of $\alpha$ is the degree of its minimal polynomial.

Exercise 0.1. Show that the minimal polynomial is irreducible over $\mathbb{Q}$.

Exercise 0.2. Let $f \in \mathbb{C}[x]$ with $f(\alpha) = 0$. Then $\alpha$ is a multiple root of $f$ if and only if $f'(\alpha) = 0$.

Exercise 0.3. Show that if $f$ is an irreducible polynomial over $\mathbb{Q}$ then $f$ has no multiple roots in $\mathbb{C}$.

The following straightforward observation is used to great effect in many arguments about diophantine approximation and algorithm analysis.

Lemma 0.4. If $z \in \mathbb{Z}$ and $z \neq 0$ then $|z| \geq 1$.

Theorem 0.5. Liouville
Let $\alpha$ be an algebraic number of degree $n \geq 2$. Then

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^{n+1}}$$

has only a finite number of solutions $(p,q)$ ($p,q \in \mathbb{Z}$).

Sketch of proof:
By assumption we have $f \in \mathbb{Z}[x]$, $\deg(f) = n$, $f(\alpha) = 0$ and $\alpha$ is a simple root of $f$. Therefore $f$ can be written as $f(x) = (x - \alpha)g(x)$, where $g \in \mathbb{C}[x]$ and $g(\alpha) \neq 0$. Now

$$\left| \alpha - \frac{p}{q} \right| = \left| \frac{f\left(\frac{p}{q}\right)}{g\left(\frac{p}{q}\right)} \right| = \left| \frac{q^n f\left(\frac{p}{q}\right)}{q^n g\left(\frac{p}{q}\right)} \right| \geq \frac{1}{q^n g\left(\frac{p}{q}\right)} \sim \frac{1}{q^n |g(\alpha)|}.$$  

(1)
(Why does $f\left(\frac{p}{q}\right) \neq 0$?) So

\[
\frac{1}{q^{n+1}} \geq \left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n}.
\]

This implies that $q$ is bounded and therefore there are only a finite number of solutions.

**Problem 0.6. (Computational geometry.)** Suppose we are to find the shortest path between two points $A$ and $B$ in the plane, avoiding certain straight line segments (“obstacles”). The obstacles are perpendicular to $AB$ drawn such that they have “convex boundary.”

Can the number of candidate optimum paths be bounded by $n^c$, where $n$ is the number of obstacles? In other words can an algorithm be found limiting the number of candidate paths to a polynomial number.

**Open Problem 0.7.** Given positive integers $a_1, \ldots, a_k, b_1, \ldots, b_l$ can we decide in polynomial time (in terms of total bit length) if

\[
\sum \sqrt{a_i} > \sum \sqrt{b_i}?
\]

**Exercise 0.8.** Show

\[
\prod \sum_{\pm} \pm \sqrt{c_i} \in \mathbb{Z}
\]

where we are taking products over all assignments of signs, with the restriction that $\sqrt{c_i}$ always positive.

Suppose we assume that for no choice of signs does $\sum \pm \sqrt{c_i} = 0$. Then

\[
\left|\prod \sum_{\pm} \pm \sqrt{c_i}\right| \geq 1 \text{ implies } \left|\sum \pm \sqrt{c_i}\right| \geq \frac{1}{(\sum \sqrt{c_i})^{2^n-1}}.
\]

**Problem 0.9.** Find a sequence $\{c^n\}$ of sequences such that $c^n$ is a collection of $n$ n-digit numbers; with the additional property that for some choice of signs,

\[
-c \log \left|\sum \pm \sqrt{c_i^n}\right| \geq \|c^n\|^{N(c)}.
\]

Can $-\log \left|\sum \pm \sqrt{c_i^n}\right|$ grow faster than $n^{\text{const}^N}$?

Review seventh problem set.

**Exercise 0.10.** Show coefficient reduction does not affect the sequence $b_1^*, \ldots, b_n^*$.

**Exercise 0.11.** We denote the Lovász potential function by $\mathcal{P}$. Show

\[
\frac{\mathcal{P}_{\text{new}}}{\mathcal{P}_{\text{old}}} = \frac{\|b_i^{new*}\|}{\|b_i^{old*}\|}
\]

is a (what?) constant factor. (Hint: work only in the space spanned by $b_i$ and $b_{i+1}$.)