Assignment 4

1. Call $c \in \mathbb{Z}_N^*$ good if $r = O(c)$ is even and $c^{r/2} \not\equiv -1 \pmod N$. Prove that if N is divisible by l distinct odd primes, then at least a fraction $1 - \frac{1}{2^{l-1}}$ of the elements of $\mathbb{Z}_N^*$ are good.

2. Show that if p and q are integers such that $|x - p/q| < \frac{1}{2q^2}$, then p/q is a convergent of the continued fraction expansion of x.

3. In the modified Grover's search problem, assume that there are x needles. Show that θ is given by $\cos\theta = \sqrt{1 - \frac{x}{N}}$ and therefore we can find a solution after $O\left(\sqrt{\frac{N}{x}}\right)$ queries.