MATH843: Assignment 4

Due: March. 22, 2013

Name: .....

1. Let α be an irrational real number. Show that there are infinitely many convergents $\frac{p_n}{q_n}$ of α such that
$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{\sqrt{5}q_n^2}.$$
[HINT: look at 3 consecutive convergents]

2. Let $\theta > \sqrt{5}$. Prove that for $\alpha = \frac{1}{2} - \frac{1}{2}\sqrt{5}$ there are only finitely many convergents such that
$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{\theta q_n^2}.$$

3. Let α be an irrational real number. Consider the continued fraction expansion $\alpha = [a_0; a_1, \ldots, a_n, \ldots]$ and the convergents $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$ (this is following the notation we have used in the lectures).
   (a) Prove that $p_{n+2}q_n - p_n q_{n+2} = (-1)^n a_{n+2}$.
   (b) Prove that $\frac{p_{n+1}}{p_n} = [a_{n+1}, a_n, \ldots, a_0]$.
   (c) Prove that $\frac{q_{n+1}}{q_n} = [a_{n+1}, a_n, \ldots, a_1]$.

4. As we have seen, we have
$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{k-1}, 2a_0}.]$$
Prove that the repeating part is a palindrome, i.e., that $a_i = a_{k-i}$ for $i = 1, \ldots, k-1$.
(As we've seen, if α is a reduced quadratic number, then so is minus the inverse of its conjugate, i.e., $-\frac{1}{\bar{\alpha}}$. What is its (purely periodic!) continued fraction expansion?)
General hint: It's good to at least once in your life compute a few continued fractions expansions of quadratics to get a bit of a feel for what happens during the computations.

5. *Shank's factorization method.* This is not a very good factorization method in the sense that you have to be "lucky" for the method to work well. However, the "luck" is hard to predict, so in some cases the method works surprisingly well. It is an improvement over Fermat's factorization method and the fundamental idea is actually the same as in modern "state of the art" factorization methods.
   (a) Suppose $\alpha > 1$ and that p_n/q_n is a convergent of α. Check that
$$|p_n^2 - \alpha^2 q_n^2| < 2\alpha$$
   (b) Let $m \in \mathbb{Z}_{>0}$ be a non-square, let $\alpha = \sqrt{m}$. Show that there is an integer k_n with $|k_n| < 2\sqrt{m}$ such that $p_n^2 \equiv k_n \pmod{m}$.
   (c) Argue that if k_n itself is a square then the congruence $p_n^2 \equiv k_n \pmod{m}$ can often be used to extract a non-trivial factor of m.
   (d) Use Shank's factorization method to factorize 3552223 (use a computer and show which convergents work for you and why).