**Elementary Number Theory and Cryptography, Epiphany 2015**

Problem Sheet 4, (Due: Monday Mar 9, at 12:00 in CM116)

Please hand in Problems 1, 6(b), 8(a), 10(b), 11(c).
The Problems 3, 4(a), 5, 6(a), 10(a), 11(a) will be discussed in the tutorials, (depending on time).

1. In the lectures we stated the following lemma.

   Let $\frac{p_n}{q_n}$ be the $n^{th}$ convergent of the continued fraction of the irrational number $x$. If $a, b \in \mathbb{Z}$, with $1 \leq b < q_{n+1}$, then

   $$|q_n x - p_n| \leq |bx - a|.$$

   Using the lemma show that if $x$ is an irrational number, and $b$ an integer with $1 \leq b \leq q_n$ then the rational number $\frac{a}{b}$ satisfies

   $$|x - \frac{p_n}{q_n}| \leq |x - \frac{a}{b}|.$$

2. Let $x \in \mathbb{R}$ be such that $1.442 < x < 1.443$. Compute the first four partial quotients of the continued fraction expansion of $x$. Can you compute the fifth partial quotient of $x$ using only the information provided?

3. Let $d$ be a positive, non square, integer. If $\frac{p}{q}$ is a convergent of the continued fraction of $\sqrt{d}$, then
   $$p^2 - dq^2 = k,$$
   where $|k| < 1 + 2\sqrt{d}$. (Hint: Use Theorem 23 from the lectures.)

4. Evaluate each of the following infinite simple continued fractions:

   (a) $[3; 6, \overline{1, 2, 3}]$

   (b) $[2; 3, \overline{1, 2, 1}]$.

5. If $r = [a_0; a_1, a_2, \ldots, a_n] > 1$, show that $1/r = [0; a_0, a_1, a_2, \ldots, a_n]$.

6. Determine the infinite continued fraction representations of each irrational number below:

   (a) $\sqrt{5}$;

   (b) $\sqrt{7}$;

   (c) $(1 + \sqrt{13})/2$;

   (d) $(5 + \sqrt{37})/2$;

   (e) $(11 + \sqrt{30})/13$.

7. Let $[a_0; a_1, a_2, a_3, \ldots]$ be an infinite continued fraction. We define $\alpha^{odd} := \lim_{n\to\infty} C_{2n+1}$ and $\alpha^{even} := \lim_{n\to\infty} C_{2n}$. We have seen in the lectures that these limits exist. Show that $\alpha^{odd} = \alpha^{even}$.

8. For any natural number $n$ show that:

   (a) $\sqrt{n^2+1} = [n; \overline{2n}]$;

   (b) $\sqrt{n^2+2} = [n; \overline{n, 2n}]$;

   (c) $\sqrt{n^2+2n} = [n; \overline{1, 2n}]$.

9. Amongst the convergents of $\sqrt{15}$ find a rational number that approximates $\sqrt{15}$ with accuracy to four decimal places.

10. Find all positive solutions in $x$ and $y$ with $y < 200$ for the following equations:

    (a) $x^2 - 2y^2 = 1$;

    (b) $x^2 - 3y^2 = 1$;

    (c) $x^2 - 5y^2 = 1$.

11. Find two positive solutions in $x$ and $y$ of each of the following equations:

    (a) $x^2 - 23y^2 = 1$;

    (b) $x^2 - 26y^2 = 1$;

    (c) $x^2 - 33y^2 = 1$.