**ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY II**
**SOLUTIONS FOR PROBLEM SHEET 4**
**EPIPHANY TERM 2015**

(1) Assume that we had

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

After multiplying with $q_n$, and noticing that $q_n > 0$ we get

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

where the last inequality follows from the given fact that $b \leq q_n$. Hence we get $|q_n x - p_n| > |bx - a|$. Contradiction.

(2) Compute the first five partial quotients of 1.442 and 1.443:

$$\frac{1442}{1000} = \frac{721}{500} = 1 + \frac{221}{500}; \quad \frac{500}{221} = 2 + \frac{58}{221}; \quad \frac{221}{58} = 3 + \frac{47}{58};$$
$$\frac{58}{47} = 1 + \frac{11}{47}; \frac{47}{11} = 4 + \frac{3}{11}.$$

So $1.442 = [1; 2, 3, 1, 4, ...]$. By analogy we get $1.443 = [1; 2, 3, 1, 7...]$. Now we have that

$$[1; 2, 3, 1, 4] > 1.443 > x > 1.442 > [1; 2, 3, 1, 7].$$

Therefore the first four partial quotients of $x$ are $1, 2, 3$ and $1$. However the fifth partial quotient of a number between 1.442 and 1.443 can be anything between 4 and 7. So it is not possible to compute the exact its value if no more information is provided.

(3) If $p/q$ is a convergent of $\sqrt{d}$ then we have by the theorem that

$$|\sqrt{d} - \frac{p}{q}| < \frac{1}{q^2}$$

and hence $|q\sqrt{d} - p| < \frac{1}{q}$. But then

$$|p + q\sqrt{d}| = |(p - q\sqrt{d}) + 2q\sqrt{d}| < \frac{1}{q} + 2q\sqrt{d} < (1 + 2\sqrt{d})q$$

Hence we have

$$|p^2 - dq^2| = |(p - q\sqrt{d})(p + q\sqrt{d})| < \frac{1}{q}(1 + 2\sqrt{d})q = 1 + 2\sqrt{d},$$

which shows the statement of the exercise.

(4) (a) We set $x = [\overline{1; 2, 3}]$. That is $x = [1; 2, 3, x]$. Forming the table

| | | | | |
|---|---|---|---|---|
| $a_k$ : | 1 | 2 | 3 | $x$ |
| $p_k$ : | 1 | 3 | 10 | $10x + 3$ |
| $q_k$ : | 1 | 2 | 7 | $7x + 2$ |

That is, $x = (10x+3)/(7x+2)$ gives $7x^2-8x-3 = 0$, $x = (4+\sqrt{37})/7$. Now we have $[3; 6, \overline{1, 2, 3}] = [3; 6, x]$. Again we have

$$\begin{array}{lccc} a_k: & 3 & 6 & x \\ p_k: & 3 & 19 & 19x+3 \\ q_k: & 1 & 6 & 6x+1 \end{array}$$

That is $y = \frac{19x+3}{6x+1} = \frac{19(\frac{4+\sqrt{37}}{7})+3}{6(\frac{4+\sqrt{37}}{7})+1} = \frac{97+19\sqrt{37}}{31+6\sqrt{37}}$

(b) We set $x = \overline{[1;2,1]}$. That is $x = [1;2,1,x]$. Forming the table

$$\begin{array}{lcccc} a_k: & 1 & 2 & 1 & x \\ p_k: & 1 & 3 & 4 & 4x+3 \\ q_k: & 1 & 2 & 3 & 3x+2 \end{array}$$

That is $x = \frac{4x+3}{3x+2}$, or equivalently we have the equation $3x^2-2x-3=0$, the positive solution of which is $x = \frac{2+\sqrt{10}}{3}$. Again as before we obtain that

$$[2;3,\overline{1,2,1}] = \frac{7x+2}{3x+1} = \frac{7\sqrt{10}+20}{3\sqrt{10}+9}.$$

(5) Let us write $r = \frac{a}{b}$, with $a,b > 0$ and $a,b \in \mathbb{Z}$. Then we have that $a = a_0 b + r_0$. In particular if we consider $\frac{1}{r} = \frac{b}{a}$ $b > a$, and hence

$$b = 0a + b$$

and then $b = a_0 a + r_0$. That is $1/r = [0; a_0, a_1, a_2, \ldots]$.

(6) (a) $\sqrt{5} = \mathbf{2} + (\sqrt{5}-2)$, $(\sqrt{5}-2)^{-1} = \sqrt{5}+2 = \mathbf{4} + (\sqrt{5}-2)$; this relation will appear again and again. Therefore, $\sqrt{5} = [2;\overline{4}]$.

(b) $\sqrt{7} = \mathbf{2} + (\sqrt{7}-2)$; $(\sqrt{7}-2)^{-1} = (\sqrt{7}+2)/3 = \mathbf{1} + (\sqrt{7}-1)/3$; $3/(\sqrt{7}-1) = (\sqrt{7}+1)/2 = \mathbf{1} + (\sqrt{7}-1)/2$; $2/(\sqrt{7}-1) = (\sqrt{7}+1)/3 = \mathbf{1} + (\sqrt{7}-2)/3$; $3/(\sqrt{7}-2) = \sqrt{7}+2 = \mathbf{4} + (\sqrt{7}-2)$. We obtained again $\sqrt{7}-2$ and, therefore, from now on the proess will be periodic. So, $\sqrt{7} = [2;\overline{1,1,1,4}]$.

(c) $(1+\sqrt{13})/2 = \mathbf{2} + (\sqrt{13}-3)/2$; $2/(\sqrt{13}-3) = (\sqrt{13}+3)/2 = \mathbf{3} + (\sqrt{13}-3)/2$. So, we obtained $[2;\overline{3}]$.

(d) $(5+\sqrt{37})/2 = \mathbf{5} + (\sqrt{37}-5)/2$; $2/(\sqrt{37}-5) = \mathbf{1} + (\sqrt{37}-1)/6$; $6/(\sqrt{37}-1) = \mathbf{1} + (\sqrt{37}-5)/6$; $6/(\sqrt{37}-5) = (\sqrt{37}+5)/2$ and we obtained $[\overline{5;1,1}]$.

(7) For any $n \in \mathbb{N}$ we have

$$0 \leq |\alpha^{odd} - \alpha^{even}| < |C_{2n+1} - C_{2n}| = |\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}}| = |\frac{(-1)^{2n}}{q_{2n}q_{2n+1}}| < \frac{1}{q_n^2}$$

But as $n \to \infty$ we have that $q_n \to \infty$, and so $\alpha^{even} = \alpha^{odd}$.

(8) (a) First, prove that $x = \overline{[2n]}$ satisfies the equation $2n + 1/x = x$ and therefore equals $n + \sqrt{n^2+1}$.

(b) Similarly, first prove that $x = \overline{[n;2n]}$ satisfies the equation $2nx^2 - 2n^2x - n = 0$.

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

(9) We know that

$$\left|\sqrt{15} - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

Find that $\sqrt{15} = [3;\overline{1,6}]$. Then compute the $p_n$ and $q_n$ until $q_n q_{n+1} > 10,000$.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $a_k:$ | 3 | 1 | 6 | 1 | 6 | 1 | 6 |
| $p_k:$ | 3 | 4 | 27 | 31 | 213 | 244 | 1677 |
| $q_k:$ | 1 | 1 | 7 | 8 | 55 | 63 | 433 |

Because $q_5q_6 = 63 \cdot 433 > 10,000$ we can take $p_5/q_5 = 244/63$.

(10) (a) Here $\sqrt{2} = [1; \overline{2}]$ and all solutions appear in the form $(x, y) = (p_{2n-1}, q_{2n-1})$, where $n \in \mathbb{N}$.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $a_k:$ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| $p_k:$ | 1 | 3 | 7 | 17 | 41 | 99 | 239 |
| $q_k:$ | 1 | 2 | 5 | 12 | 29 | 70 | 169 |

This gives $q_7 > 200$ and $(x, y) = (3, 2), (17, 12), (99, 70)$.

(b) Here $\sqrt{3} = [1; \overline{1, 2}]$ and all solutions appear in the form $(p_{2n-1}, q_{2n-1})$.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $a_k:$ | 1 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 |
| $p_k:$ | 1 | 2 | 5 | 7 | 19 | 26 | 71 | 97 | 265 | 362 |
| $q_k:$ | 1 | 1 | 3 | 4 | 11 | 15 | 41 | 56 | 153 | 209 |

This gives $q_9 > 200$ and $(x, y) = (2, 1), (7, 4), (26, 15), (97, 56)$.

(c) Here $\sqrt{5} = [2; \overline{4}]$ and all solutions appear in the form $(p_{2n-1}, q_{2n-1})$.

| | | | | | |
|---|---|---|---|---|---|
| $a_k:$ | 2 | 4 | 4 | 4 | 4 |
| $p_k:$ | 2 | 9 | 38 | 161 | 682 |
| $q_k:$ | 1 | 4 | 17 | 72 | 305 |

This gives $q_5 > 200$ and solutions are $(9, 4)$ and $(161, 72)$.

(11) (a) Find that $\sqrt{23} = [4; \overline{1, 3, 1, 8}]$. The period has length $n = 4$ (even!), therefore the first two positive solutions are $(p_3, q_3)$ and $(p_7, q_7)$.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $a_k:$ | 4 | 1 | 3 | 1 | 8 | 1 | 3 | 1 |
| $p_k:$ | 4 | 5 | 19 | 24 | 211 | 235 | 916 | 1151 |
| $q_k:$ | 1 | 1 | 4 | 5 | 44 | 49 | 191 | 240 |

Therefore, $(p_3, q_3) = (24, 5)$ and $(p_7, q_7) = (1151, 240)$.

(b) Find that $\sqrt{26} = [5; \overline{10}]$. The period has length $n = 1$ (odd!), therefore the first two positive solutions are $(p_1, q_1)$ and $(p_3, q_3)$.

| | | | | |
|---|---|---|---|---|
| $a_k:$ | 5 | 10 | 10 | 10 |
| $p_k:$ | 5 | 51 | 515 | 5201 |
| $q_k:$ | 1 | 10 | 101 | 1020 |

Therefore, $(p_1, q_1) = (51, 10)$ and $(p_3, q_3) = (5201, 1020)$.

(c) Find that $\sqrt{33} = [5; \overline{1, 2, 1, 10}]$. The period has length $n = 4$ (even!), therefore the first two positive solutions are $(p_3, q_3)$ and $(p_7, q_7)$.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $a_k:$ | 5 | 1 | 2 | 1 | 10 | 1 | 2 | 1 |
| $p_k:$ | 5 | 6 | 17 | 23 | 247 | 270 | 787 | 1057 |
| $q_k:$ | 1 | 1 | 3 | 4 | 43 | 47 | 137 | 184 |

Therefore, $(p_3, q_3) = (23, 4)$ and $(p_7, q_7) = (1057, 184)$.