Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 3

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, November 10th, at 12:05 pm.

1. Let
$$[b_0; b_1, b_2, b_3, \ldots] \tag{1}$$
be a continued fraction ($b_0 \in \mathbb{Z}$, $b_i \in \mathbb{N}$ for all $i \geq 1$).

We recursively define
$$\begin{aligned} P_{-1} &= 1, \quad P_0 = b_0, \quad P_k = b_k P_{k-1} + P_{k-2} \\ Q_{-1} &= 0, \quad Q_0 = 1, \quad Q_k = b_k Q_{k-1} + Q_{k-2} \end{aligned} \tag{2}$$
(If $[b_0; b_1, b_2, b_3, \ldots] = [b_0; b_1, b_2, \ldots, b_m]$ is finite, then $k \leq m$ in the recursion.)

Prove that for all $k \in \mathbb{N}$ (with $k \leq m$ in finite case) we have
$$[b_0; b_1, b_2, \ldots, b_k] = \frac{P_k}{Q_k},$$
where $[b_0; b_1, b_2, \ldots, b_k]$ is the k-th convergent for (1) and P_k, Q_k are defined by (2).

2. Prove that for (P_k) and (Q_k) defined above, the following identities hold:

(a) $P_k Q_{k-1} - Q_k P_{k-1} = (-1)^{k-1}$,

(b) $P_k Q_{k-2} - Q_k P_{k-2} = (-1)^k b_k$.

3. (a) Find $\dfrac{P_k}{Q_k} - \dfrac{P_{k-2}}{Q_{k-2}}$ and determine whether it is positive or negative (this may depend on k). Make a conclusion about monotonicity of subsequences of $\left(\dfrac{P_k}{Q_k}\right)$ with odd-/even-numbered terms.

(b) Now find $\dfrac{P_k}{Q_k} - \dfrac{P_{k-1}}{Q_{k-1}}$.

(c) Use (a) and (b) to show that if the original continued fraction is infinite, then the sequence $\left(\dfrac{P_k}{Q_k}\right)$ converges to a real number.

Remark. If we denote $x := \lim\limits_{k\to\infty} \dfrac{P_k}{Q_k}$, then we write $x = [b_0; b_1, b_2, b_3, \ldots]$.

4. If $\dfrac{P_k}{Q_k}$, where $k \in \mathbb{N}$, is a convergent for x and if another rational number $\dfrac{p}{q} \neq \dfrac{P_k}{Q_k}$ has denominator $0 < q \leq Q_k$, then $\left|x - \dfrac{P_k}{Q_k}\right| < \left|x - \dfrac{p}{q}\right|$. In other words, convergents are best rational approximations of real numbers. Prove this. You may use a more general fact – the theorem on the back of this page.

Remark 1. It follows, in particular, that $\left|x - \dfrac{P_k}{Q_k}\right| < \left|x - \dfrac{P_{k-1}}{Q_{k-1}}\right|$.

Remark 2. Note that not all of the best rational approximations are convergents.

Theorem. *If* $|qx-p| < |Q_kx-P_k|$, *where* $\dfrac{P_k}{Q_k}$ $(k \in \mathbb{N})$ *is the* k*-th convergent for* $x \in \mathbb{R}\setminus\mathbb{Q}$, $p \in \mathbb{Z}$ *and* $q \in \mathbb{N}$, *then* $q > Q_k$.

Proof. We prove by contradiction. Assume that $|qx-p| < |Q_kx-P_k|$ and that $q \leq Q_k$. Notice that then $q < Q_{k+1}$.

Consider the linear system of equations:

$$\begin{aligned} uP_k + vP_{k+1} &= p \\ uQ_k + vQ_{k+1} &= q \end{aligned} \tag{3}$$

Its matrix has determinant $P_kQ_{k+1} - Q_kP_{k+1} = (-1)^{k+1}$ (see Problem 2(a)), which means that there is a unique solution

$$(u, v)$$

to the system (3), and this solution is a pair of integers.

Step 1. We first show that both $u \neq 0$ and $v \neq 0$.
If $u = 0$, then $q = vQ_{k+1}$. So v is a positive integer, and therefore $q \geq Q_{k+1}$, which contradicts $q < Q_{k+1}$.
If $v = 0$, then $p = uP_k$, $q = uQ_k$, and we have $|qx-p| = |u| \cdot |Q_kx-P_k| \geq |Q_kx-P_k|$, which contradicts the assumption.

Step 2. Now we show that u and v have opposite signs.
Consider the second equation in (3) and substitute the solution (u, v) in it, that is,

$$q = uQ_k + vQ_{k+1}.$$

If both u and v are positive integers, then $q > Q_{k+1}$. If both are negative, then $q < 0$. However, we know that $0 < q < Q_{k+1}$.

Step 3. Now we can finish the proof. Since $x - \dfrac{P_k}{Q_k}$ and $x - \dfrac{P_{k+1}}{Q_{k+1}}$ have opposite signs (because x always lies between two consequtive convergents - this follows from Problem 3, think why), we have that

$$u(Q_kx - P_k) \text{ and } v(Q_{k+1}x - P_{k+1}) \text{ have the same sign.} \tag{4}$$

From (3) we find

$$qx - p = x(uQ_k + vQ_{k+1}) - (uP_k + vP_{k+1}) = u(Q_kx - P_k) + v(Q_{k+1}x - P_{k+1}).$$

Using (4) we get now

$$|qx-p| = |u(Q_kx-P_k)| + |v(Q_{k+1}x - P_{k+1})| > |u| \cdot |Q_kx - P_k| \geq |Q_kx - P_k|,$$

which contradicts the assumption. □