Autumn Semester 2019

Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu
Coordinator: Dr. Danylo Radchenko

Solutions to Exercise Sheet 9

Exercise 9.1. Let $\{a_n\}_{n\geq 1}$ be a sequence of positive integers, let $a_0 \geq 0$ and define

$$\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}},$$

where the fraction p_n/q_n is written in lowest terms and $q_n > 0$. Denote $(p_{-2}, q_{-2}) = (0, 1)$ and $(p_{-1}, q_{-1}) = (1, 0)$. Let $x = [a_0; a_1, a_2, \dots] := \lim_{n\to\infty} p_n/q_n$.

(a) Show that $p_n = a_n p_{n-1} + p_{n-2}$ and $q_n = a_n q_{n-1} + q_{n-2}$, and $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$ for all $n \geq 0$. Deduce from this that $\lim_{n\to\infty} p_n/q_n$ exists;

(b) Show that $\operatorname{sgn}(x - \frac{p_n}{q_n}) = (-1)^n$ and $\frac{1}{q_n(q_{n+1}+q_n)} < |x - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}}$ for $n \geq 0$;

(c) Let $\alpha_m = [a_m; a_{m+1}, \dots]$. Show that $x = \frac{p_m \alpha_{m+1} + p_{m-1}}{q_m \alpha_{m+1} + q_{m-1}}$ and $\alpha_{m+1} = \frac{p_{m-1} - x q_{m-1}}{x q_m - p_m}$.

Solution. (a) Let us instead define p_n and q_n by the recursions $p_n = a_n p_{n-1} + p_{n-2}$ and $q_n = a_n q_{n-1} + q_{n-2}$ (they are well-defined for any choice of $\{a_n\}$). First, we show by induction that $p_n/q_n = [a_0; a_1, \dots, a_n]$: base is trivial, and the induction step is

$$\begin{aligned}\frac{p_{n+1}}{q_{n+1}} &= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = \frac{p_n + p_{n-1}/a_{n+1}}{q_n + q_{n-1}/a_{n+1}} = \frac{p_{n-1}(a_n + 1/a_{n+1}) + p_{n-2}}{q_{n-1}(a_n + 1/a_{n+1}) + q_{n-2}} \\ &= [a_0; a_1, \dots, a_{n-1}, a_n + 1/a_{n+1}] = [a_0; a_1, \dots, a_{n+1}],\end{aligned}$$

where we have used the induction assumption in the form $[a_0; a_1, \dots, a_{n-1}, z] = \frac{p_{n-1}z + p_{n-2}}{q_{n-1}z + q_{n-2}}$ for $z = a_n + 1/a_{n+1}$.

Next, note that $p_{-1}q_0 - p_0 q_{-1} = -1$ and using the recursion we compute

$$p_{n-1}q_n - p_n q_{n-1} = p_{n-1}(a_n q_{n-1} + q_{n-2}) - q_{n-1}(a_n p_{n-1} + p_{n-2}) = -(p_{n-2}q_{n-1} - p_{n-1}q_{n-2}),$$

therefore by induction $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$.

The identity $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$ implies that $\gcd(p_n, q_n) = 1$, and therefore p_n/q_n is the fraction $[a_0; a_1, \dots, a_n]$ written in lowest terms as claimed. Finally, from $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$ we see that

$$x = a_0 + \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{q_n q_{n-1}},$$

which converges since it is an alternating series and $\{q_n\}_{n\geq 1}$ are strictly increasing which can be seen from the recursion.

(b) From part (a) we see that $\{q_n\}_{n\geq 0}$ is nondecreasing, $\{q_n\}_{n\geq 1}$ is strictly increasing, and moreover

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n+1}}{q_n q_{n-1}}.$$

From this we see that

$$\operatorname{sgn}\left(\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}}\right) = \operatorname{sgn}\left(\frac{(-1)^n}{q_{n-1}} \frac{(q_n - q_{n-2})}{q_n q_{n-2}}\right) = (-1)^n .$$

Thus, $p_0/q_0 < p_2/q_2 < \cdots < p_{2n}/q_{2n} < p_{2n+1}/q_{2n+1} < p_{2n-1}/q_{2n-1} < \cdots < p_1/q_1$. This shows the first claim. Note that as a corollary, x lies in the interval with endpoints p_n/q_n and p_{n+1}/q_{n+1} for all n, therefore

$$\left|x - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}} .$$

Similarly, since p_{n+2}/q_{n+2} and p_n/q_n are on one side of x, we see that

$$\left|x - \frac{p_n}{q_n}\right| > \left|\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n}\right| = \frac{q_{n+2} - q_n}{q_n q_{n+1} q_{n+2}} = \frac{a_{n+2}}{q_n(a_{n+2}q_{n+1} + q_n)} \geq \frac{1}{q_n(q_{n+1} + q_n)} .$$

(c) In part (a) we have proved that $[a_0; a_1, \ldots, a_m, z] = \frac{p_m z + p_{m-1}}{q_m z + q_{m-1}}$. On the other hand, by definition of α_{m+1} we have $[a_0; a_1, \ldots, a_m, \alpha_{m+1}] = x$. This proves the first claim. Solving for α_{m+1} in $x = \frac{p_m \alpha_{m+1} + p_{m-1}}{q_m \alpha_{m+1} + q_{m-1}}$ we obtain $\alpha_{m+1} = \frac{p_{m-1} - x q_{m-1}}{x q_m - p_m}$.

Exercise 9.2. Let α be a quadratic irrational. Show that the continued fraction representation $\alpha = [a_0; a_1, a_2, \ldots]$ is eventually periodic, i.e., $a_n = a_{n+T}$ for all $n \geq N$ for some $T > 0$, $N \geq 0$.

Solution. Let α satisfy $f(\alpha) = 0$, where $f(x) = Ax^2 + Bx + C$, with $A, B, C \in \mathbb{Z}$. Let $\alpha_m = [a_m; a_{m+1}, \ldots]$, so that $\alpha = \frac{p_{m-1}\alpha_m + p_{m-2}}{q_{m-1}\alpha_m + q_{m-2}}$ for $m \geq 0$ (by Exercise 9.1(c)). After plugging this expression into f and clearing denominators, we get that α_m satisfies $A_m \alpha_m^2 + B_m \alpha_m + C_m = 0$, where $A_m, B_m, C_m \in \mathbb{Z}$.

We have $A_m = q_{m-1}^2 f(p_{m-1}/q_{m-1})$ and $C_m = q_{m-2}^2 f(p_{m-2}/q_{m-2})$. Moreover, since $\det\begin{pmatrix} p_{m-1} & q_{m-1} \\ p_m & q_m \end{pmatrix} = \pm 1$, we have $B_m^2 - 4A_m C_m = B^2 - 4AC$ (one can also verify this directly).

Since α is irrational, f has an single root at $x = \alpha$, and therefore $f'(\alpha) \neq 0$. By Exercise 9.1(b) p_{m-2}/q_{m-2} and p_{m-1}/q_{m-1} both converge to α and lie on different sides of it. Therefore, for sufficiently large m we have $f(p_{m-1}/q_{m-1})f(p_{m-2}/q_{m-2}) < 0$, and therefore $A_m C_m < 0$ for all sufficiently large m. But since $B_m^2 - 4A_m C_m = B^2 - 4AC$ is a fixed number, this implies that $|A_m C_m|$ and B_m^2 are bounded.

This means that there are only finitely many possibilities for (A_m, B_m, C_m), and therefore, for α_m. This implies that $\alpha_N = \alpha_{N+T}$ for some $N \geq 0$, $T > 0$. This proves that $a_{n+T} = a_n$ for $n \geq N$, by definition of α_m.

Exercise 9.3. Let $\alpha = \frac{P+\sqrt{D}}{Q} > 1$ be a quadratic irrational such that $-1 < \alpha' < 0$, where $\alpha' = \frac{P-\sqrt{D}}{Q}$. Show that the continued fraction $\alpha = [a_0; a_1, \ldots]$ is purely periodic, i.e., $a_n = a_{n+T}$ for all $n \geq 0$.

Solution. Let $\alpha_m = [a_m; a_{m+1}, \dots]$. By the argument from the previous exercise α_m are satisfy quadratic equations with discriminant D, so that $\alpha_m = \frac{P_m + \sqrt{D}}{Q_m}$ for some $P_m, Q_m \in \mathbb{Z}$. Moreover, $\alpha'_m = \frac{P_m - \sqrt{D}}{Q_m}$.

Taking conjugates of $\alpha_m = a_m + \frac{1}{\alpha_{m+1}}$ we get $\alpha'_m = a_m + \frac{1}{\alpha'_{m+1}}$, and hence $\alpha'_{m+1} = \frac{1}{\alpha'_m - a_m}$. Since $\alpha'_0 = \alpha' \in (-1, 0)$, by induction we see that $-1 < \alpha'_m < 0$ for all $m \geq 0$.

By Exercise 9.2 we have $\alpha_N = \alpha_{N+T}$ for some $N \geq 0$. Assume that $N > 0$. Taking conjugates we get $\alpha'_N = \alpha'_{N+T}$. From $\alpha_{N-1} = a_{N-1} + 1/\alpha_N$ we get

$$-1/\alpha'_N = a_{N-1} - \alpha'_{N-1}\,,$$

which implies $a_{N-1} = \lfloor -1/\alpha'_N \rfloor$ since $-1 < \alpha'_{N-1} < 0$. Similarly, we get $a_{N+T-1} = \lfloor -1/\alpha'_{N+T} \rfloor$. Since $\alpha'_N = \alpha'_{N+T}$, we get $a_{N+T-1} = a_{N-1}$. From this, in turn, we get $\alpha_{N-1} = \alpha_{N+T-1}$. Repeating this argument we get that $\alpha_0 = \alpha_T$, so that $a_{n+T} = a_n$ for all $n \geq 0$.

Exercise 9.4. Let $D > 0$ be a non-square integer, let $[a_0; a_1, a_2, \dots]$ be the continued fraction representation of $\sqrt{D}$, and denote $\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n]$. Let T be the period of $\{a_n\}_{n \geq 0}$. Show that

$$p_{mT-1}^2 - D q_{mT-1}^2 = (-1)^{mT}\,, \quad m \geq 1\,.$$

(*Hint: apply Exercise 9.3 to* $\sqrt{D} + \lfloor \sqrt{D} \rfloor$ *and then use Exercise 9.1(c).*)

Solution. By Exercise 9.3 we know that $a_0 + \sqrt{D}$ has a purely periodic continued fraction. Therefore, if we denote $\alpha_m = [a_m; a_{m+1}, \dots]$, then $\alpha_{mT} = a_0 + \sqrt{D}$. By part (c) of Exercise 9.1 we have

$$\sqrt{D} = \frac{p_{mT-1}\alpha_{mT} + p_{mT-2}}{q_{mT-1}\alpha_{mT} + q_{mT-2}}$$

Plugging in the value of α_{mT} we get

$$\sqrt{D}(q_{mT-1}(a_0 + \sqrt{D}) + q_{mT-2}) = p_{mT-1}(a_0 + \sqrt{D}) + p_{mT-2}\,.$$

Since $\sqrt{D}$ is irrational, this is equivalent to

$$p_{mT-1} = a_0 q_{mT-1} + q_{mT-2}\,,$$
$$D q_{mT-1} = a_0 p_{mT-1} + p_{mT-2}\,.$$

Multiplying the first identity by p_{mT-1} and the second by q_{mT-1} and taking the difference we obtain

$$p_{mT-1}^2 - D q_{mT-1}^2 = q_{mT-2} p_{mT-1} - q_{mT-1} p_{mT-2} = (-1)^{mT}\,,$$

as claimed.