FIRST LECTURE FOR THE RESEARCH SCHOOL CIMPA 2015: "UNITS AND REGULATORS VIA CONTINUED FRACTIONS"

DANIEL C. MAYER

1. Lattice Minima and Units

1.1. Continued fractions.

Definition 1.1. Let $x \in \mathbb{R} \setminus \mathbb{Q}$ be an irrational number. The *continued fraction expansion* (CFE) of x is defined recursively by two sequences $(x_i)_{i \geq 0}$ and $(a_i)_{i \geq 0}$ such that

$$\begin{aligned} x_0 &:= x, \\ a_0 &:= \lfloor x_0 \rfloor, \\ x_i &:= \frac{1}{x_{i-1} - \lfloor x_{i-1} \rfloor}, \text{ for } i \geq 1, \\ a_i &:= \lfloor x_i \rfloor, \text{ for } i \geq 1. \end{aligned} \tag{1}$$

For each $i \geq 1$, the integer $a_i \geq 1$ is called the ith *partial quotient* and the real number $x_i > 1$ is called the ith *total* (or complete) *quotient* of the CFE of x, which is formally denoted by

$$[a_0, a_1, a_2, \ldots].$$

Remark 1.1. We have

$$x = x_0 = a_0 + \frac{1}{x_1} = a_0 + \frac{1}{a_1 + \frac{1}{x_2}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{x_3}}} = \cdots$$

Thus the construction of the partial and total quotients gives rise to finite representations of x in the form $x = [a_0, a_1, a_2, \ldots, a_{i-1}, x_i]$, for each $i \geq 0$.

Date: May 05, 2015.
2000 *Mathematics Subject Classification.* Primary 11Y40, 11Y65, 14H52, 14K22, 11R37, 11R29, 11R11; Secondary 11Y11, 11Y05.
Key words and phrases. algebraic number theory computations, continued fractions, elliptic curves, complex multiplication, primality, factorization, quadratic fields.

Algorithm 1.1. (Continued Fraction Algorithm, CFA)
Input: a real number $x \in \mathbb{R}$ and an upper bound $b \geq 0$.
Initialization:
$i \leftarrow 0$;
$a_0 \leftarrow \lfloor x \rfloor$; Store or output a_0;
$x \leftarrow x - a_0$;
Recursion:
`while` $((x > 0)$ `and` $(i \leq b))$ {
    $i \leftarrow i + 1$;
    $x \leftarrow \frac{1}{x}$;
    $a_i \leftarrow \lfloor x \rfloor$; Store or output a_i;
    $x \leftarrow x - a_i$;
}
Termination: either if some x is an integer or if $i > b$.
Output: the sequence of partial quotients $(a_0, a_1, a_2, \ldots)$.
Complexity: $O(b)$ steps.

Warning. The correct execution of Algorithm 1.1 depends on the precision of the input x and of the inversion $x \leftarrow \frac{1}{x}$.

Definition 1.2. The sequences of numerators and denominators of the *convergents* $\frac{P_i}{Q_i}$ for the CFE of $x \in \mathbb{R} \setminus \mathbb{Q}$ are defined recursively by

$$
\begin{aligned}
P_{-2} &:= 0, \\
Q_{-2} &:= 1, \\
P_{-1} &:= 1, \\
Q_{-1} &:= 0, \\
P_i &:= a_i P_{i-1} + P_{i-2}, \text{ for } i \geq 0, \\
Q_i &:= a_i Q_{i-1} + Q_{i-2}, \text{ for } i \geq 0.
\end{aligned} \tag{2}
$$

Theorem 1.1. *For each $i \geq 0$, the convergent $\frac{P_i}{Q_i}$ for the CFE of $x \in \mathbb{R} \setminus \mathbb{Q}$ coincides exactly with the rational approximation $[a_0, a_1, a_2, \ldots, a_i]$ of x. It satisfies the inequality*

$$\left| x - \frac{P_i}{Q_i} \right| < \frac{1}{Q_i Q_{i+1}} < \frac{1}{Q_i^2},$$

and for **even** *$i \geq 0$ the inequalities*

$$\frac{P_i}{Q_i} < \frac{P_{i+2}}{Q_{i+2}} < x < \frac{P_{i+3}}{Q_{i+3}} < \frac{P_{i+1}}{Q_{i+1}}.$$

In particular, the limit of the sequence of convergents exists, equals x, and is also denoted by

$$[a_0, a_1, a_2, \ldots] := \lim_{i \to \infty} [a_0, a_1, a_2, \ldots, a_i] = \lim_{i \to \infty} \frac{P_i}{Q_i} = x.$$

Theorem 1.2. *Let $x \in \mathbb{R}$ be a real number. The continued fraction expansion $x = [a_0, a_1, \ldots]$ of x is*

1. *finite $x = [a_0, \ldots, a_n]$, for some integer $n \geq 0$, if and only if $x \in \mathbb{Q}$ is a rational number,*
2. *infinite and periodic $x = [a_0, \ldots, a_{p-1}, \overline{a_p, \ldots, a_{p+\ell-1}}]$, for some preperiod $p \geq 0$ and some period length $\ell \geq 1$, if and only if $x \in \mathbb{Q}(\sqrt{D})$, for some square free $D > 1$, is a quadratic irrationality.*

For quadratic irrationalities, the CFE can be determined with less precision requirements, using integer arithmetic only.

Theorem 1.3. *Let $D > 1$ be a non-square positive integer and $x = \frac{M_0+\sqrt{D}}{N_0} \in \mathbb{Q}(\sqrt{D})$ be a quadratic irrationality, with integers $N_0 \neq 0$ and M_0 such that N_0 divides $D - M_0^2$. Let the (necessarily periodic) CFE of x be $x = [a_0, a_1, \ldots]$.*
If the sequences of coefficients $(M_i)_{i\geq 1}$ and denominators $(N_i)_{i\geq 1}$ are defined recursively by

$$\begin{aligned} M_i &:= a_{i-1}N_{i-1} - M_{i-1}, \\ N_i &:= \frac{D - M_i^2}{N_{i-1}} \end{aligned} \tag{3}$$

then

1. *the total quotients of the CFE of x are given by the expressions $x_i = \frac{M_i+\sqrt{D}}{N_i}$ for $i \geq 1$,*
2. *the denominators are also given by $N_i = a_{i-1}(M_{i-1} - M_i) + N_{i-2}$ for $i \geq 2$, in particular they are integers and $D - M_i^2 = N_iN_{i-1}$ for $i \geq 1$,*
3. *the coefficients and denominators are bounded by $|M_i| < \sqrt{D}$ and $1 \leq N_i \leq D$, for sufficiently large $i \geq 0$, and*
4. *a connection with the numerators P_i and denominators Q_i of the convergents for the CFE of x is given by Scheffler's formula*

$$\mathrm{Norm}_{K|\mathbb{Q}}(\nu_1^j(1)) = \frac{(P_{i-1}N_0 - Q_{i-1}M_0)^2 - DQ_{i-1}^2}{N_0^2} = (-1)^i\frac{N_i}{N_0}.$$

In particular, if $x = \sqrt{D}$ with $M_0 = 0$ and $N_0 = 1$ is a pure square root, then the bounds can be improved to $0 \leq M_i < \sqrt{D}$, $1 \leq N_i < 2\sqrt{D}$, and the relation $P_{i-1}^2 - DQ_{i-1}^2 = (-1)^iN_i$ implies firstly that

$$P_{i-1}^2 \equiv (-1)^iN_i \pmod{D},$$

and secondly that

$$(P_{i-1}Q_{i-1}^{-1})^2 \equiv D \pmod{p} \text{ and thus } \left(\frac{D}{p}\right) = +1,$$

for every prime factor p of N_i.

Example 1.1. We determine the fundamental unit $\varepsilon > 1$ and its norm for the discriminants $d \in \{12, 57\}$ (resp. the associated square free radicands D).

(1) $d = 12,\ D = 3$:
since $d = 3 \cdot 4 \equiv 0 \pmod 4$, start with $x_0 = \sqrt{3} \approx 1.732$, $a_0 = 1$,
$M_0 = 0$, $N_0 = 1$, $N_{-1} = \frac{D - M_0^2}{N_0} = \frac{3-0}{1} = 3$;

$M_1 = a_0 N_0 - M_0 = 1 \cdot 1 - 0 = 1$,
$N_1 = a_0(M_0 - M_1) + N_{-1} = 1 \cdot (0 - 1) + 3 = -1 + 3 = 2$,
$x_1 = \frac{M_1 + \sqrt{D}}{N_1} = \frac{1+\sqrt{3}}{2} \approx 1.366$, $a_1 = 1$;

$M_2 = a_1 N_1 - M_1 = 1 \cdot 2 - 1 = 12 - 7 = 1$,
$N_2 = a_1(M_1 - M_2) + N_0 = 1 \cdot (1 - 1) + 1 = 1$,
$x_2 = \frac{M_2 + \sqrt{D}}{N_2} = \frac{1+\sqrt{3}}{1} \approx 2.732$, $a_2 = 2$;

$M_3 = a_2 N_2 - M_2 = 2 \cdot 1 - 1 = 1$,
$N_3 = a_2(M_2 - M_3) + N_1 = 2 \cdot (1 - 1) + 2 = 2$, and periodicity $x_3 = x_1$ sets in.

Consequently, the CFE is given by $x = [1; \overline{1, 2}]$ with even period length $\ell = 2$.
However, for the representation $\varepsilon = P_{\ell-1} + Q_{\ell-1} \cdot \sqrt{3}$ of the fundamental unit with $\ell - 1 = 1$ we need the successive numerators and denominators of convergents:

$P_0 = a_0 P_{-1} + P_{-2} = 1 \cdot 1 + 0 = 1$, $Q_0 = a_0 Q_{-1} + Q_{-2} = 1 \cdot 0 + 1 = 1$,
$P_1 = a_1 P_0 + P_{-1} = 1 \cdot 1 + 1 = 2$, $Q_1 = a_1 Q_0 + Q_{-1} = 1 \cdot 1 + 0 = 1$,

$\varepsilon = 2 + \sqrt{3}$ is the fundamental unit of $K = \mathbb{Q}(\sqrt{3})$ with norm

$$\mathrm{Norm}_{K|\mathbb{Q}}(\varepsilon) = (2 + \sqrt{3}) \cdot (2 - \sqrt{3}) = 4 - 3 = +1,$$

and the regulator is given by

$$R = \log(\varepsilon) = \log(2 + \sqrt{3}) \approx 1.3169579.$$

(2) $d = D = 57$:
since $d = 7 \cdot 8 + 1 \equiv 1 \pmod 8$, start with $x_0 = \frac{1}{2}(-1 + \sqrt{57}) \approx 3.2749$, $a_0 = 3$,
$M_0 = -1$, $N_0 = 2$, $N_{-1} = \frac{D - M_0^2}{N_0} = \frac{57-1}{2} = 28$;

$M_1 = a_0 N_0 - M_0 = 3 \cdot 2 - (-1) = 6 + 1 = 7$,
$N_1 = a_0(M_0 - M_1) + N_{-1} = 3 \cdot (-1 - 7) + 28 = -24 + 28 = 4$,
$x_1 = \frac{M_1 + \sqrt{D}}{N_1} = \frac{7+\sqrt{57}}{4} \approx 3.637$, $a_1 = 3$;

$M_2 = a_1N_1 - M_1 = 3 \cdot 4 - 7 = 12 - 7 = 5,$
$N_2 = a_1(M_1 - M_2) + N_0 = 3 \cdot (7 - 5) + 2 = 6 + 2 = 8,$
$x_2 = \frac{M_2+\sqrt{D}}{N_2} = \frac{5+\sqrt{57}}{8} \approx 1.5687,\ a_2 = 1;$

$M_3 = a_2N_2 - M_2 = 1 \cdot 8 - 5 = 3,$
$N_3 = a_2(M_2 - M_3) + N_1 = 1 \cdot (5 - 3) + 4 = 6,$
$x_3 = \frac{M_3+\sqrt{D}}{N_3} = \frac{3+\sqrt{57}}{6} \approx 1.758,\ a_3 = 1;$

$M_4 = a_3N_3 - M_3 = 1 \cdot 6 - 3 = 3,$
$N_4 = a_3(M_3 - M_4) + N_2 = 1 \cdot (3 - 3) + 8 = 8,$
$x_4 = \frac{M_4+\sqrt{D}}{N_4} = \frac{3+\sqrt{57}}{8} \approx 1.3187,\ a_4 = 1;$

$M_5 = a_4N_4 - M_4 = 1 \cdot 8 - 3 = 5,$
$N_5 = a_4(M_4 - M_5) + N_3 = 1 \cdot (3 - 5) + 6 = 4,$
$x_5 = \frac{M_5+\sqrt{D}}{N_5} = \frac{5+\sqrt{57}}{4} \approx 3.137,\ a_5 = 3;$

$M_6 = a_5N_5 - M_5 = 3 \cdot 4 - 5 = 12 - 5 = 7,$
$N_6 = a_5(M_5 - M_6) + N_4 = 3 \cdot (5 - 7) + 8 = -6 + 8 = 2,$
$x_6 = \frac{M_6+\sqrt{D}}{N_6} = \frac{7+\sqrt{57}}{2} \approx 7.2749,\ a_6 = 7;$

$M_7 = a_6N_6 - M_6 = 7 \cdot 2 - 7 = 14 - 7 = 7,$
$N_7 = a_6(M_6 - M_7) + N_5 = 7 \cdot (7 - 7) + 4 = 4,$ and periodicity $x_7 = x_1$ sets in.

Consequently, the CFE is given by $x = [3; \overline{3, 1, 1, 1, 3, 7}]$ with even period length $\ell = 6$. However, for the representation $\varepsilon = P_{\ell-1} + Q_{\ell-1} \cdot \frac{1}{2}(1 + \sqrt{57})$ of the fundamental unit with $\ell - 1 = 5$ we need the successive numerators and denominators of convergents:

$P_0 = a_0P_{-1} + P_{-2} = 3 \cdot 1 + 0 = 3,\ Q_0 = a_0Q_{-1} + Q_{-2} = 3 \cdot 0 + 1 = 1,$
$P_1 = a_1P_0 + P_{-1} = 3 \cdot 3 + 1 = 10,\ Q_1 = a_1Q_0 + Q_{-1} = 3 \cdot 1 + 0 = 3,$
$P_2 = a_2P_1 + P_0 = 1 \cdot 10 + 3 = 13,\ Q_2 = a_2Q_1 + Q_0 = 1 \cdot 3 + 1 = 4,$
$P_3 = a_3P_2 + P_1 = 1 \cdot 13 + 10 = 23,\ Q_3 = a_3Q_2 + Q_1 = 1 \cdot 4 + 3 = 7,$
$P_4 = a_4P_3 + P_2 = 1 \cdot 23 + 13 = 36,\ Q_4 = a_4Q_3 + Q_2 = 1 \cdot 7 + 4 = 11,$
$P_5 = a_5P_4 + P_3 = 3 \cdot 36 + 23 = 131,\ Q_5 = a_5Q_4 + Q_3 = 3 \cdot 11 + 7 = 40,$

$\varepsilon = 131 + 40 \cdot \frac{1}{2}(1 + \sqrt{57}) = 151 + 20\sqrt{57}$ is the fundamental unit of $K = \mathbb{Q}(\sqrt{57})$ with norm

$$\mathrm{Norm}(\varepsilon) = (151 + 20\sqrt{57}) \cdot (151 - 20\sqrt{57}) = 22801 - 400 \cdot 57 = 22801 - 22800 = +1,$$

and the regulator is given by

$$R = \log(\varepsilon) = \log(151 + 20\sqrt{57}) \approx 5.71041605.$$

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[2] W. Bosma, J. J. Cannon, C. Fieker, and A. Steels (eds.), *Handbook of Magma functions* (Edition 2.21, Sydney, 2015).

[3] H. Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics **138**, Springer, 1996.

[4] H. Cohen, *Advanced topics in computational number theory*, Graduate texts in mathematics **193**, Springer, 2000.

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming — a System for Computational Discrete Algebra*, Version 4.7.7, Aachen, Braunschweig, Fort Collins, St. Andrews, 2015, (`http://www.gap-system.org`).

[6] The MAGMA Group, *MAGMA Computational Algebra System*, Version 2.21-3, Sydney, 2015, (`http://magma.maths.usyd.edu.au`).

[7] Oracle, *JDK* 7u80, *Java SE*, and *NetBeans*, Version 8.0.2, Redwood City, CA, 2015, (`http://www.oracle.com`).

[8] The PARI Group, *PARI/GP*, Version 2.7.3, Bordeaux, 2015, (`http://pari.math.u-bordeaux.fr`).

[9] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of mathematics and its applications, Cambridge University Press, 1990.

[10] S.S. Wagstaff, Jr., *The Joy of Factoring*, Student Mathematical Library (STML), Vol. **68**, American Mathematical Society (AMS), 2013.

Naglergasse 53, 8010 Graz, Austria

E-mail address: `algebraic.number.theory@algebra.at`

URL: `http://www.algebra.at`