FORMALIZED MATHEMATICS
Vol. 23, No. 2, Pages 101–106, 2015
DOI: 10.1515/forma-2015-0010

DE GRUYTER
OPEN
degruyter.com/view/j/forma

Introduction to Diophantine Approximation

Yasushige Watase
Suginami-ku Matsunoki 6
3-21 Tokyo, Japan

Summary. In this article we formalize some results of Diophantine approximation, i.e. the approximation of an irrational number by rationals. A typical example is finding an integer solution (x, y) of the inequality $|x\theta - y| \leqslant 1/x$, where θ is a real number. First, we formalize some lemmas about continued fractions. Then we prove that the inequality has infinitely many solutions by continued fractions. Finally, we formalize Dirichlet's proof (1842) of existence of the solution [12], [1].

MSC: 11A55 11J68 03B35

Keywords: irrational number; approximation; continued fraction; rational number; Dirichlet's proof

MML identifier: `DIOPHAN1`, version: `8.1.04 5.32.1237`

The notation and terminology used in this paper have been introduced in the following articles: [24], [2], [6], [22], [14], [5], [11], [7], [8], [28], [20], [26], [3], [25], [19], [4], [9], [32], [15], [13], [21], [30], [31], [18], [23], [29], and [10].

1. Irrational Numbers and Continued Fractions

From now on i, j, k, m, n, m_1, n_1 denote natural numbers, a, r, r_1, r_2 denote real numbers, m_0, c_3, c_1 denote integers, and x_1, x_2, o denote objects.

Now we state the proposition:

(1) (i) $r = (\mathrm{rfs}\, r)(0)$, and

(ii) $r = (\mathrm{scf}\, r)(0) + (1/_{(\mathrm{rfs}\, r)(1)})$, and

(iii) $(\mathrm{rfs}\, r)(n) = (\mathrm{scf}\, r)(n) + (1/_{(\mathrm{rfs}\, r)(n+1)})$.

Let us assume that r is irrational. Now we state the propositions:

ISSN 1426–2630(Print), 1898-9934(Online)

(2) $(\mathrm{rfs}\,r)(n)$ is irrational.

PROOF: Reconsider $r_3 = (\mathrm{rfs}\,r)(n)$ as a real number. $(\mathrm{scf}\,r_3)(m) = (\mathrm{scf}\,r)(n+m)$ and $(\mathrm{rfs}\,r_3)(m) = (\mathrm{rfs}\,r)(n+m)$. Consider n_1 such that for every m_1 such that $m_1 \geqslant n_1$ holds $(\mathrm{scf}\,r_3)(m_1) = 0$. For every m_1 such that $m_1 \geqslant n_1$ holds $(\mathrm{scf}\,r)(n+m_1) = 0$. For every m such that $m \geqslant n_1 + n$ holds $(\mathrm{scf}\,r)(m) = 0$ by [28, (3)]. □

(3) (i) $(\mathrm{rfs}\,r)(n) \neq 0$, and

(ii) $(\mathrm{rfs}\,r)(1) \cdot (\mathrm{rfs}\,r)(2) \neq 0$, and

(iii) $(\mathrm{scf}\,r)(1) \cdot (\mathrm{rfs}\,r)(2) + 1 \neq 0$.

PROOF: $(\mathrm{rfs}\,r)(n) \neq 0$ by [21, (28), (42)]. $(\mathrm{rfs}\,r)(1) \neq 0$ and $(\mathrm{rfs}\,r)(2) \neq 0$. $(\mathrm{rfs}\,r)(1) = (\mathrm{scf}\,r)(1) + (1/_{(\mathrm{rfs}\,r)(1+1)})$. □

(4) (i) $(\mathrm{scf}\,r)(n) < (\mathrm{rfs}\,r)(n) < (\mathrm{scf}\,r)(n) + 1$, and

(ii) $1 < (\mathrm{rfs}\,r)(n+1)$.

The theorem is a consequence of (2) and (1).

(5) $0 < (\mathrm{scf}\,r)(n+1)$. The theorem is a consequence of (4).

Let us consider r and n. Observe that $(cn\,r)(n)$ is integer.

Let us assume that r is irrational. Now we state the propositions:

(6) $(cd\,r)(n+1) \geqslant (cd\,r)(n)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (cd\,r)(\$_1) \leqslant (cd\,r)(\$_1 + 1)$. $\mathcal{P}[0]$ by (4), [28, (7)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (4), [28, (7)], [21, (51)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(7) $(cd\,r)(n) \geqslant 1$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (cd\,r)(\$_1) \geqslant 1$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(8) $(cd\,r)(n+2) > (cd\,r)(n+1)$. The theorem is a consequence of (5) and (7).

(9) $(cd\,r)(n) \geqslant n$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (cd\,r)(\$_1) \geqslant \$_1$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (7), (5), [21, (40)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

Now we state the proposition:

(10) If $c_3 = (cn\,r)(n)$ and $c_1 = (cd\,r)(n)$ and $c_3 \neq 0$, then c_3 and c_1 are relatively prime.

Let us assume that r is irrational. Now we state the propositions:

(11) (i) $(cd\,r)(n+1) \cdot (\mathrm{rfs}\,r)(n+2) + (cd\,r)(n) > 0$, and

(ii) $(cd\,r)(n+1)\cdot(\mathrm{rfs}\,r)(n+2)-(cd\,r)(n)>0$.

The theorem is a consequence of (7), (4), and (6).

(12) $(cd\,r)(n+1)\cdot((cd\,r)(n+1)\cdot(\mathrm{rfs}\,r)(n+2)+(cd\,r)(n))>0$. The theorem is a consequence of (7) and (11).

(13) $r=(cn\,r)(n+1)\cdot(\mathrm{rfs}\,r)(n+2)+(cn\,r)(n)/_{(cd\,r)(n+1)\cdot(\mathrm{rfs}\,r)(n+2)+(cd\,r)(n)}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv r=(cn\,r)(\$_1+1)\cdot(\mathrm{rfs}\,r)(\$_1+2)+(cn\,r)(\$_1)/_{(cd\,r)(\$_1+1)\cdot(\mathrm{rfs}\,r)(\$_1+2)+(cd\,r)(\$_1)}$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(14) $((cn\,r)(n+1)/_{(cd\,r)(n+1)})-r=(-1)^n/_{(cd\,r)(n+1)\cdot((cd\,r)(n+1)\cdot(\mathrm{rfs}\,r)(n+2)+(cd\,r)(n))}$. The theorem is a consequence of (7), (11), and (13).

Now we state the propositions:

(15) If r is irrational and n is even and $n>0$, then $r>(cn\,r)(n)/_{(cd\,r)(n)}$. The theorem is a consequence of (12) and (14).

(16) If r is irrational and n is odd, then $r<(cn\,r)(n)/_{(cd\,r)(n)}$. The theorem is a consequence of (12) and (14).

(17) Suppose r is irrational and $n>0$. Then $|r-((cn\,r)(n)/_{(cd\,r)(n)})|+|r-((cn\,r)(n+1)/_{(cd\,r)(n+1)})|=|((cn\,r)(n)/_{(cd\,r)(n)})-((cn\,r)(n+1)/_{(cd\,r)(n+1)})|$. The theorem is a consequence of (15) and (16).

Let us assume that r is irrational. Now we state the propositions:

(18) $|r-((cn\,r)(n)/_{(cd\,r)(n)})|>0$.

(19) $(cd\,r)(n+2)\geqslant 2\cdot(cd\,r)(n)$. The theorem is a consequence of (5), (7), and (6).

(20) $|r-((cn\,r)(n+1)/_{(cd\,r)(n+1)})|<1/_{(cd\,r)(n+1)\cdot(cd\,r)(n+2)}$. The theorem is a consequence of (7), (4), and (14).

(21) (i) $|r\cdot(cd\,r)(n+1)-(cn\,r)(n+1)|<|r\cdot(cd\,r)(n)-(cn\,r)(n)|$, and

(ii) $|r-((cn\,r)(n+1)/_{(cd\,r)(n+1)})|<|r-((cn\,r)(n)/_{(cd\,r)(n)})|$.

The theorem is a consequence of (13), (11), (4), (7), (18), and (6).

Now we state the propositions:

(22) If r is irrational and $m>n$, then $|r-((cn\,r)(n)/_{(cd\,r)(n)})|>|r-((cn\,r)(m)/_{(cd\,r)(m)})|$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv |r-((cn\,r)(n)/_{(cd\,r)(n)})|>|r-((cn\,r)(n+1+\$_1)/_{(cd\,r)(n+1+\$_1)})|$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. □

(23) If r is irrational, then $|r-((cn\,r)(n)/_{(cd\,r)(n)})|<1/_{(cd\,r)(n)^2}$.

Proof: $|r - ((cn\,r)(n)/_{(cd\,r)(n)})| < 1/_{(cd\,r)(n)^2}$ by [28, (43)], (7), [16, (1)], (6). □

(24) Let us consider a subset S of $\mathbb{Q}$, and r. Suppose r is irrational and $S = \{p$, where p is an element of $\mathbb{Q}$: $|r - p| < 1/_{(\mathrm{den}\,p)^2}\}$. Then S is infinite.

Proof: Define $\mathcal{F}$(natural number) $= (cn\,r)(\$_1 + 1)/_{(cd\,r)(\$_1+1)}$. Consider f being a sequence of real numbers such that for every natural number n, $f(n) = \mathcal{F}(n)$ from [17, Sch. 1]. For every real number o such that $o \in \mathrm{rng}\, f$ holds $o \in S$ by [21, (50)], (7), [15, (28)], [16, (1)]. f is one-to-one. □

(25) If r is irrational, then cocf r is convergent and $\lim \mathrm{cocf}\, r = r$.

Proof: For every real number p such that $0 < p$ there exists n such that for every m such that $n \leqslant m$ holds $|(\mathrm{cocf}\, r)(m) - r| < p$ by [27, (25)], [28, (3)], [17, (8)], [6, (52)]. □

2. Integer Solution of $|x\theta - y| \leqslant 1/x$

Let us observe that there exists a natural number which is greater than 1.

From now on t denotes a greater than 1 natural number.

Let us consider t. The functor EDI(t) yielding a sequence of subsets of $\mathbb{R}$ is defined by

(Def. 1) for every natural number n, $it(n) = [n/_t, n + 1/_t[$.

Now we state the propositions:

(26) (The partial unions of EDI(t))(i) $= [0, i + 1/_t[$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ (the partial unions of EDI(t))($\$_1$) $= [0, \$_1 + 1/_t[$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(27) Let us consider a real number r, and a natural number i. If $\lfloor r \cdot t \rfloor = i$, then $r \in (\mathrm{EDI}(t))(i)$.

(28) If $r_1, r_2 \in (\mathrm{EDI}(t))(i)$, then $|r_1 - r_2| < t^{-1}$.

(29) (The partial unions of EDI(t))($t - 1$) $= [0, 1[$. The theorem is a consequence of (26).

(30) Let us consider a real number r. Suppose $r \in [0, 1[$. Then there exists a natural number i such that

(i) $i \leqslant t - 1$, and

(ii) $r \in (\mathrm{EDI}(t))(i)$.

The theorem is a consequence of (29).

(31) Let us consider a real number r, and a natural number i. If $r \in (\mathrm{EDI}(t))(i)$, then $\lfloor r \cdot t \rfloor = i$.

(32) Let us consider a real number r. Suppose $r \in [0, 1[$. Then there exists a natural number i such that

(i) $i \leqslant t - 1$, and

(ii) $\lfloor r \cdot t \rfloor = i$.

The theorem is a consequence of (30) and (31).

Let us consider t and a. The functor $\mathrm{FDP}(t, a)$ yielding a finite sequence of elements of $\mathbb{Z}_t$ is defined by

(Def. 2) $\mathrm{len}\, it = t + 1$ and for every i such that $i \in \mathrm{dom}\, it$ holds $it(i) = \lfloor \mathrm{frac}((i - 1) \cdot a) \cdot t \rfloor$.

Let us note that $\mathrm{rng}\, \mathrm{FDP}(t, a)$ is non empty.

Now we state the proposition:

(33) $\overline{\overline{\mathrm{rng}\, \mathrm{FDP}(t, a)}} \in \overline{\overline{\mathrm{dom}\, \mathrm{FDP}(t, a)}}$.

Let us consider t and a. One can verify that $\mathrm{FDP}(t, a)$ is non one-to-one.

3. Proof of Dirichlet's Theorem

Now we state the proposition:

(34) DIRICHLET'S APPROXIMATION THEOREM:
There exist integers x, y such that

(i) $|x \cdot a - y| < 1/_t$, and

(ii) $0 < x \leqslant t$.

The theorem is a consequence of (27) and (28).

References

[1] Alan Baker. *A Concise Introduction to the Theory of Numbers.* Cambridge University Press, 1984.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[6] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1980.

[13] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**): 35–40, 1990.

[14] Peter Jaeger. Elementary introduction to stochastic finance in discrete time. *Formalized Mathematics*, 20(**1**):1–5, 2012. doi:10.2478/v10037-012-0001-5.

[15] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[16] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**): 573–577, 1997.

[17] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[18] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.

[19] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[20] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[21] Bo Li, Yan Zhang, and Artur Korniłowicz. Simple continued fractions and their convergents. *Formalized Mathematics*, 14(**3**):71–78, 2006. doi:10.2478/v10037-006-0009-9.

[22] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.

[23] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[24] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[25] Christoph Schwarzweller. Proth numbers. *Formalized Mathematics*, 22(**2**):111–118, 2014. doi:10.2478/forma-2014-0013.

[26] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[27] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[28] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[29] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[30] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[31] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[32] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. Set sequences and monotone class. *Formalized Mathematics*, 13(**4**):435–441, 2005.

Received April 19, 2015