

Introduction to Diophantine Approximation. Part II

Yasushige Watase
Suginami-ku Matsunoki 3
Tokyo, Japan

Summary. In the article we present in the Mizar system [2], [3] the formalized proofs for Hurwitz' theorem [5, 1891] and Minkowski's theorem [???(1904)]. Both theorems are well known in the theory of Diophantine approximations as appeared in [4], [6].

A formal proof of Dirichlet's theorem, namely an inequation $|\theta - y/x| \leq 1/x^2$ has infinitely many integer solutions (x, y) where θ is an irrational number, was given in [8]. A finer approximation is given by Hurwitz' theorem: $|\theta - y/x| \leq 1/\sqrt{5}x^2$.

Minkowski's theorem concerns about an inequation of a product of non-homogeneous binary linear forms such that $|a_1x + b_1y + c_1| \cdot |a_2x + b_2y + c_2| \leq \Delta/4$ where $\Delta = |a_1b_2 - a_2b_1| \neq 0$, has at least one integer solution.

MSC: 03B35

Keywords:

MML identifier: DIOPHAN2, version: 8.1.06 5.45.1311

1. PRELIMINARIES

From now on r_1, r_2, r_3 denote non negative real numbers, n, m_1 denote natural numbers, s denotes a real number, i, j, i_1, j_1 denote integers, r denotes an irrational real number, and q denotes a rational number.

Now we state the propositions:

- (1) If $r_1 \cdot r_2 \leq r_3$, then $r_1 \leq \sqrt{r_3}$ or $r_2 \leq \sqrt{r_3}$.
- (2) $\sqrt{r_1 \cdot r_2} = \frac{r_1 + r_2}{2}$ if and only if $r_1 = r_2$.

- (3) $r_1 \cdot r_2 = (\frac{r_1+r_2}{2})^2$ if and only if $r_1 = r_2$. The theorem is a consequence of (2).
- (4) If i_1 and j_1 are relatively prime, then there exist integers s, t such that $s \cdot i_1 + t \cdot j_1 = 1$.
- (5) If $1 < s$ and $s + \frac{1}{s} < \sqrt{5}$, then $s < \frac{\sqrt{5}+1}{2}$ and $\frac{1}{s} > \frac{\sqrt{5}-1}{2}$.
- (6) If $q = \frac{i_1}{m_1}$ and $m_1 \neq 0$ and i_1 and m_1 are relatively prime, then $i_1 = \text{num } q$ and $m_1 = \text{den } q$.

Let f be a function. The functor **ZeroPointSet(f)** yielding a set is defined by the term

(Def. 1) $\text{dom } f \setminus \text{support } f$.

Now we state the proposition:

- (7) Let us consider a function f , and objects o_1, o_2 . Then $o_1 \in \text{ZeroPointSet}(f)$ if and only if $o_1 \in \text{dom } f$ and $f(o_1) = 0$.

2. HURWITZ' THEOREM [5, 1891]

Let r be an irrational real number and n be a natural number. Note that $(cdr)(n)$ is positive and natural.

Now we state the propositions:

- (8) Suppose $n > 1$ and $|r - \frac{(cnr)(n)}{(cdr)(n)}| \geq \frac{1}{\sqrt{5} \cdot ((cdr)(n))^2}$ and $|r - \frac{(cnr)(n+1)}{(cdr)(n+1)}| \geq \frac{1}{\sqrt{5} \cdot ((cdr)(n+1))^2}$. Then $\sqrt{5} > \frac{(cdr)(n+1)}{(cdr)(n)} + \frac{1}{\frac{(cdr)(n+1)}{(cdr)(n)}}$.
- (9) If $i = (cnr)(n)$ and $j = (cdr)(n)$, then i and j are relatively prime.
- (10) Suppose $n > 1$. Then
 - (i) $|r - \frac{(cnr)(n)}{(cdr)(n)}| < \frac{1}{\sqrt{5} \cdot ((cdr)(n))^2}$, or
 - (ii) $|r - \frac{(cnr)(n+1)}{(cdr)(n+1)}| < \frac{1}{\sqrt{5} \cdot ((cdr)(n+1))^2}$, or
 - (iii) $|r - \frac{(cnr)(n+2)}{(cdr)(n+2)}| < \frac{1}{\sqrt{5} \cdot ((cdr)(n+2))^2}$.

The theorem is a consequence of (8) and (5).

Let us consider r . The functor **HWZSet(r)** yielding a subset of \mathbb{Q} is defined by the term

(Def. 2) $\{p, \text{ where } p \text{ is a rational number} : |r - p| < \frac{1}{\sqrt{5} \cdot ((\text{den } p)^2)}\}$.

The functor **HWZSet1(r)** yielding a subset of \mathbb{N} is defined by the term

(Def. 3) $\{x, \text{ where } x \text{ is a natural number} : \text{there exists a rational number } p \text{ such that } p \in \text{HWZSet}(r) \text{ and } x = \text{den } p\}$.

The functor **TRANQN** yielding a function from \mathbb{Q} into \mathbb{N} is defined by

(Def. 4) for every rational number x , $it(x) = \text{den } x$.

Now we state the propositions:

(11) $(\text{TRANQN})^\circ(\text{HWZSet}(r)) = \text{HWZSet1}(r)$.

(12) If $\text{HWZSet}(r)$ is finite, then $\text{HWZSet1}(r)$ is finite. The theorem is a consequence of (11).

Let us consider r . One can check that $\text{HWZSet1}(r)$ is non empty.

Now we state the proposition:

(13) Let us consider a natural number h . If $h \in \text{HWZSet1}(r)$, then $h > 0$.

Let us consider r . Note that $\text{HWZSet1}(r)$ is infinite.

Now we state the proposition:

(14) HURWITZ'S THEOREM (NUMBER THEORY):

$\{q : |r - q| < \frac{1}{\sqrt{5} \cdot (\text{den } q)^2}\}$ is infinite. The theorem is a consequence of (12).

From now on $c_0, c_1, c_2, u, a_0, b_0$ denote real numbers.

Let a_0, b_0, c_0 be real numbers. The functor $\text{LF}(a_0, b_0, c_0)$ yielding a function from $\mathbb{Z} \times \mathbb{Z}$ into \mathbb{R} is defined by

(Def. 5) for every integers x, y , $it(x, y) = a_0 \cdot x + b_0 \cdot y + c_0$.

3. MINKOWSKI'S THEOREM [???](1904)

Now we state the proposition:

(15) Let us consider an element ρ of \mathbb{R} , and integers p, q . Suppose p and q are relatively prime. Then there exist elements x, y of \mathbb{Z} such that $|p \cdot x - q \cdot y + \rho| \leq \frac{1}{2}$. The theorem is a consequence of (4).

In the sequel a, b denote real numbers and n denotes an integer.

Now we state the propositions:

(16) If $n \leq b \leq n + 1$, then $|n - b| \cdot |n + 1 - b| \leq \frac{1}{4}$.

(17) If a is not an integer and $(n = \lfloor a \rfloor$ or $n = \lfloor a \rfloor + 1)$, then $|a - n| < 1$.

(18) Suppose $|n - a| \cdot |n + 1 - a| \leq \frac{1}{4}$ and $|n - b| \cdot |n + 1 - b| \leq \frac{1}{4}$. Then

(i) $|n - a| \cdot |n - b| \leq \frac{1}{4}$, or

(ii) $|n + 1 - a| \cdot |n + 1 - b| \leq \frac{1}{4}$.

The theorem is a consequence of (1).

(19) Suppose $|a - n| \cdot |b - n| \cdot |a - n - 1| \cdot |b - n - 1| \leq \frac{|a-b|^2}{4}$. Then

(i) $|a - n| \cdot |b - n| \leq \frac{|a-b|}{2}$, or

(ii) $|a - n - 1| \cdot |b - n - 1| \leq \frac{|a-b|}{2}$.

The theorem is a consequence of (1).

(20) Suppose $(n - b) \cdot (n + 1 - a) > 0$ and $(a - n) \cdot (n + 1 - b) > 0$. Then

(i) $(n - b) \cdot (n + 1 - a) + (a - n) \cdot (n + 1 - b) = a - b$, and

(ii) $|a - n| \cdot |b - n| \cdot |a - n - 1| \cdot |b - n - 1| \leq \frac{|a-b|^2}{4}$.

(21) If $b < n < a < n + 1$, then $|a - n| \cdot |b - n| \cdot |a - n - 1| \cdot |b - n - 1| \leq \frac{|a-b|^2}{4}$.

The theorem is a consequence of (20).

(22) Suppose $(n - a) \cdot (n + 1 - b) > 0$ and $(b - n) \cdot (n + 1 - a) > 0$. Then

(i) $(n - a) \cdot (n + 1 - b) + (b - n) \cdot (n + 1 - a) = b - a$, and

(ii) $|a - n| \cdot |b - n| \cdot |a - n - 1| \cdot |b - n - 1| \leq \frac{|a-b|^2}{4}$.

(23) If $n + 1 < b$ and $n < a < n + 1$, then $|a - n| \cdot |b - n| \cdot |a - n - 1| \cdot |b - n - 1| \leq \frac{|a-b|^2}{4}$. The theorem is a consequence of (22).

(24) Suppose a is not an integer and $\lfloor a \rfloor \leq b \leq \lfloor a \rfloor + 1$. Then there exists an integer u such that

(i) $|a - u| < 1$, and

(ii) $|a - u| \cdot |b - u| \leq \frac{1}{4}$.

The theorem is a consequence of (16), (18), and (17).

(25) Suppose $|a - \lfloor a \rfloor| \cdot |b - \lfloor a \rfloor| \geq \frac{|a-b|}{2}$ and $|a - (\lfloor a \rfloor + 1)| \cdot |b - (\lfloor a \rfloor + 1)| \geq \frac{|a-b|}{2}$. Then

(i) a is an integer, or

(ii) $\lfloor a \rfloor \leq b$.

The theorem is a consequence of (21), (19), and (3).

(26) Suppose a is not an integer and $\lfloor a \rfloor > b$. Then there exists an integer u such that

(i) $|a - u| < 1$, and

(ii) $|a - u| \cdot |b - u| < \frac{|a-b|}{2}$.

The theorem is a consequence of (17) and (25).

(27) Suppose $|a - \lfloor a \rfloor| \cdot |b - \lfloor a \rfloor| \geq \frac{|a-b|}{2}$ and $|a - (\lfloor a \rfloor + 1)| \cdot |b - (\lfloor a \rfloor + 1)| \geq \frac{|a-b|}{2}$. Then

(i) a is an integer, or

(ii) $\lfloor a \rfloor + 1 \geq b$.

The theorem is a consequence of (23), (19), and (3).

(28) Suppose a is not an integer and $\lfloor a \rfloor + 1 < b$. Then there exists an integer u such that

(i) $|a - u| < 1$, and

(ii) $|a - u| \cdot |b - u| < \frac{|a-b|}{2}$.

The theorem is a consequence of (17) and (27).

(29) There exists an integer u such that

(i) $|a - u| < 1$, and

(ii) $|a - u| \cdot |b - u| \leq \frac{1}{4}$ or $|a - u| \cdot |b - u| < \frac{|a-b|}{2}$.

The theorem is a consequence of (24), (26), and (28).

In the sequel $a_1, a_2, b_1, b_2, c_1, c_2$ denote elements of \mathbb{R} , ϵ denotes a positive real number, r_1 denotes a non negative real number, and q, q_1 denote elements of \mathbb{Q} .

Now we state the propositions:

(30) There exists an element q of \mathbb{Q} such that

(i) $\text{den } q > \lfloor r_1 \rfloor + 1$, and

(ii) $q \in \text{HWZSet}(r)$.

PROOF: Reconsider $m = \lfloor r_1 \rfloor + 1$ as a natural number. There exists n such that $n \in \text{HWZSet1}(r)$ and $n > m$ by (13), [1, (19)], [7, (3)]. Consider n such that $n \in \text{HWZSet1}(r)$ and $n > m$. \square

(31) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $q \neq q_1$ and $a_2 \cdot (\text{den } q) + b_2 \cdot (\text{num } q) = 0$. Then $a_2 \cdot (\text{den } q_1) + b_2 \cdot (\text{num } q_1) \neq 0$.

(32) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$. Then there exists an element q of \mathbb{Q} such that

(i) $\text{den } q > \lfloor r_1 \rfloor + 1$, and

(ii) $q \in \text{HWZSet}(r)$, and

(iii) $a_2 \cdot (\text{den } q) + b_2 \cdot (\text{num } q) \neq 0$.

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

(33) Let us consider real numbers a_1, b_1 , and integers n_1, d_1 . Suppose $d_1 > 0$ and $|\frac{a_1}{b_1} + \frac{n_1}{d_1}| < \frac{1}{\sqrt{5} \cdot (d_1^2)}$. Then there exists a real number d such that

(i) $\frac{n_1}{d_1} = -\frac{a_1}{b_1} + \frac{d}{d_1^2}$, and

(ii) $|d| < \frac{1}{\sqrt{5}}$.

(34) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $\frac{a_1}{b_1}$ is irrational. Then there exist elements x, y of \mathbb{Z} such that

(i) $|(\text{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\text{LF}(a_2, b_2, c_2))(x, y)| < \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$, and

(ii) $|(\text{LF}(a_1, b_1, c_1))(x, y)| < \epsilon$.

The theorem is a consequence of (32), (15), (29), and (33).

(35) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $\frac{a_2}{b_2}$ is irrational. Then there exist elements x, y of \mathbb{Z} such that

$$(i) |(\text{LF}(a_2, b_2, c_2))(x, y)| \cdot |(\text{LF}(a_1, b_1, c_1))(x, y)| < \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}, \text{ and}$$

$$(ii) |(\text{LF}(a_2, b_2, c_2))(x, y)| < \epsilon.$$

The theorem is a consequence of (34).

(36) Suppose $\text{ZeroPointSet}(\text{LF}(a_1, b_1, c_1)) \neq \emptyset$. Then there exist elements x, y of \mathbb{Z} such that $|(\text{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\text{LF}(a_2, b_2, c_2))(x, y)| \leq \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$.

The theorem is a consequence of (7).

(37) Suppose $\text{ZeroPointSet}(\text{LF}(a_2, b_2, c_2)) \neq \emptyset$. Then there exist elements x, y of \mathbb{Z} such that $|(\text{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\text{LF}(a_2, b_2, c_2))(x, y)| \leq \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$.

The theorem is a consequence of (7).

(38) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $b_1 \neq 0$ and $\frac{a_1}{b_1}$ is rational. Then there exist elements x, y of \mathbb{Z} such that $|(\text{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\text{LF}(a_2, b_2, c_2))(x, y)| \leq \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$. The theorem is a consequence of (15).

(39) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $b_2 \neq 0$ and $\frac{a_2}{b_2}$ is rational. Then there exist elements x, y of \mathbb{Z} such that $|(\text{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\text{LF}(a_2, b_2, c_2))(x, y)| \leq \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$. The theorem is a consequence of (38).

(40) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $b_1 = 0$. Then there exist elements x, y of \mathbb{Z} such that $|(\text{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\text{LF}(a_2, b_2, c_2))(x, y)| \leq \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$.

The theorem is a consequence of (35), (37), and (39).

(41) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$. Then there exist elements x, y of \mathbb{Z} such that $|(\text{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\text{LF}(a_2, b_2, c_2))(x, y)| \leq \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$. The theorem is a consequence of (34), (36), (40), and (38).

REFERENCES

- [1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(1):41–46, 1990.
- [2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.
- [3] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.
- [4] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1980.
- [5] Adolf Hurwitz. Ueber die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche. *Mathematische Annalen*, 39(2):279–284, B.G.Teubner Verlag, Leipzig, 1891.
- [6] Ivan Niven. *Diophantine Approximation*. Dover, 2008.
- [7] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(4):825–829, 2001.

- [8] Yasushige Watase. Introduction to Diophantine approximation. *Formalized Mathematics*, 23(2):101–106, 2015. doi:10.1515/forma-2015-0010.

Received November 29, 2017



The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.