Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
15 (1999), 19–26
www.bgytf.hu/~amapn

SOME NUMBER THEORETIC APPLICATIONS OF THE SMALLEST DENOMINATOR FUNCTION

Zoltán Boros and Árpád Száz

Abstract. We show that the smallest denominator function can be treated with a minimum amount of number theory. Moreover, this function can be used to nicely prove a number of fundamental divisibility and irrationality results.

Introduction

In [4], after summarizing some basic properties of real numbers and divisibility of integers, we presented a detailed study of the functions p and q defined by

$$q(x) = \min \{ n \in \mathbb{N} : \quad n\,x \in \mathbb{Z} \} \qquad \text{and} \qquad p(x) = x\,q(x)$$

for all $x \in \mathbb{Q}$, which made the investigation of the Riemann function considerably more easy.

In the present paper, we are going to show that most of the number theoretic background encountered in [4] is not actually needed for the investigation of the functions p and q. For example, an important divisibility theorem applied there can be substituted by a simple lemma concerning the function q. Moreover, we show that the functions p and q can also be well utilized in the proofs of several fundamental divisibility and irrationality results.

1. The necessary prerequisites

Troughout in the sequel, the letters $\mathbb{R}$, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ will stand for the sets of the real, natural, integer, and rational numbers, respectively.

Moreover, we assume that the reader is familiar with an appropriate system of axioms for the real numbers and some of its most important consequences such as the following theorem, for instance.

1991 *Mathematics Subject Classification.* 11-01; 11A99.
Key words and phrases. The smallest denominator function, divisibility and irrationality.
The authors' work was supported by the grants OTKA T-016846 and FKFP 0310/1997.

Theorem 1.1. *If A is a nonvoid subset of $\mathbb{Z}$ such that A is bounded below (resp. above) in $\mathbb{R}$, then* $\min(A)$ *(resp.* $\max(A)$ *) exists.*

Remark 1.2. From this theorem one can easily derive that $\mathbb{Z}$ cannot be bounded either below or above in $\mathbb{R}$.

Moreover, by Theorem 1.1, it is clear that for each $x \in \mathbb{R}$ the integral part

$$[\,x\,] = \max\{\,k \in \mathbb{Z} : \quad k \leq x\,\}$$

of x exists. Note that thus we have $[x] \in \mathbb{Z}$ such that $[x] \leq x < [x] + 1$.

Concerning the division in $\mathbb{Z}$, we shall only need here the following simple facts.

Definition 1.3. If $m, n \in \mathbb{Z}$ such that there exists a $k \in \mathbb{Z}$ such that $m = k\,n$, then we say that n divides m, and we write $n \,|\, m$.

Remark 1.4. Note that if $n \,|\, m$ and $m \neq 0$, then we necessarily have $|\,n\,| \leq |\,m|$.

Therefore, the family of all divisors of m is bounded, and thus we may also have the following

Definition 1.5. If $m, n \in \mathbb{Z}$ such that $m \neq 0$ or $n \neq 0$, then the number

$$(\,m\,;\,n\,) = \max\{\,k \in \mathbb{Z} : \quad k \,|\, m\,, \quad k \,|\, n\,\}$$

is called the greatest common divisor of m and n.

From this definition, we can at once see that $(\,m\,;\,n\,)$ is in $\mathbb{N}$. Moreover, we can easily prove the following

Theorem 1.6. *If* $k = (m\,;\,n)$, *and moreover* $m_1 = m/k$ *and* $n_1 = n/k$, *then* $m_1, n_1 \in \mathbb{Z}$ *such that* $(\,m_1;\, n_1) = 1$.

Proof. To prove the less obviuos part of the theorem, note that if $l = (\,m_1,\, n_1\,)$, then under the notations $m_2 = m_1/l$ and $n_2 = n_1/l$ we have $m = k\,l\,m_2$ and $n = k\,l\,n_2$. Hence, by the corresponding definitions, it is clear that $k\,l \leq k$. Therefore, we necessarily have $l \leq 1$, and hence $l = 1$.

Remark 1.7. One can, quite similarly, show that if $(\,m\,;\,n) = 1$, then $(m + k\,n\,;\,n) = 1$ for all $k \in \mathbb{Z}$.

2. The smallest denominator function

In [4], to precisely define and easily investigate the Riemann function, we have introduced the following two interesting functions defined only for rational numbers.

Definition 2.1. For each $x \in \mathbb{Q}$, we define

$$q(x) = \min \{ n \in \mathbb{N} : \quad n x \in \mathbb{Z} \} \qquad \text{and} \qquad p(x) = x\, q(x)\,.$$

Remark 2.2. Note that, by the definition of $\mathbb{Q}$ and Theorem 1.1, the definition of $q(x)$ is correct. Moreover, we have $q(x) \in \mathbb{N}$ and $p(x) \in \mathbb{Z}$ for all $x \in \mathbb{Q}$.

By computing some of the values of q, we can easily get to the following

Lemma 2.3. *If $x \in \mathbb{Q}$ and $n \in \mathbb{Z}$ such that $n x \in \mathbb{Z}$, then $q(x) | n$.*

Proof. If $n > 0$, then by the condition $n x \in \mathbb{Z}$ and the definition of $q(x)$, it is clear that $q(x) \leq n$, and hence $1 \leq n/q(x)$. Therefore, by defining

$$k = \left[n/q(x) \right],$$

we have $1 \leq k$, and hence $k \in \mathbb{N}$. Moreover, it is clear that

$$k \leq n/q(x) < k+1\,, \qquad \text{and hence} \qquad k\, q(x) \leq n < k\, q(x) + q(x)\,.$$

Therefore, by defining

$$r = n - k\, q(x)\,,$$

we have $0 \leq r < q(x)$. Hence, since

$$r x = n x - k\, q(x)\, x = n x - k\, p(x) \in \mathbb{Z}\,,$$

by the definition of $q(x)$ it is clear that $r = 0$, and thus $n = k\, q(x)$.

While, if $n < 0$, then it is clear that $-n > 0$ and $(-n)\, x = -n\, x \in \mathbb{Z}$. Therefore, by the above proof, we have $q(x) | (-n)$, and hence $q(x) | n$. Finally, to complete the proof, we note that if $n = 0$, then the assertion of the lemma trivially holds.

Now, by using the above lemma, we can also easily prove the next fundamental

Theorem 2.4. *If $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, then*

$$p\left(\frac{m}{n} \right) = \frac{m}{(m\,;\, n)} \qquad \textit{and} \qquad q\left(\frac{m}{n} \right) = \frac{n}{(m\,;\, n)}\,.$$

Proof. Define

$$x = m/n\,, \qquad k = (m\,;\, n)\,, \qquad m_1 = m/k\,, \qquad n_1 = n/k\,.$$

Then, by Theorem 1.6, it is clear that $m_1 \in \mathbb{Z}$ and $n_1 \in \mathbb{N}$ such that

$$n_1\, x = m_1 \qquad \text{and} \qquad (\, m_1\,,\, n_1) = 1\,.$$

Hence, by using Lemma 2.3, we can infer that there exists an $l \in \mathbb{N}$ such that

$$n_1 = l\, q(x)\,, \qquad \text{and thus} \qquad m_1 = n_1\, x = l\, q(x)\, x = l\, p(x)\,.$$

Therefore, we necessarily have $l = 1$, and thus $p(x) = m_1$ and $q(x) = n_1$.

Remark 2.5. From Theorem 2.4, by Theorem 1.6, we can at once see that

$$\big(p(x)\,;\,q(x)\big) = 1\,.$$

for all $x \in \mathbb{Q}$.

Now, the further properties of the functions p and q, with the only exception of [4, Theorem 3.6], can be easily established without using any number theoretic results.

3. Two number theoretic applications of the functions p and q

By using Lemma 2.3 and Theorem 2.4, we can now easily prove a slight extension of a basic divisibility theorem [5, Proposition 1.1.1, p. 5].

Theorem 3.1. *If* $m_1, m_2, n \in \mathbb{Z}$ *such that* $n \,|\, m_1 m_2$, *and moreover* $k = (m_1; n)$, *then* $n \,|\, k\,m_2$.

Proof. If $n > 0$, then by defining $x = m_1/n$ we have

$$m_2\,x \;=\; m_1 m_2/n \;\in\; \mathbb{Z}$$

Therefore, by Lemma 2.3, there exists an $l \in \mathbb{Z}$ such that

$$m_2 = l\,q(x)\,.$$

On the other hand, from Theorem 2.4, we know that

$$q(x) = n/k\,.$$

Therefore, we have $k\,m_2 = l\,n$, and hence $n \,|\, k\,m_2$.

While, if $n < 0$, then since $n \,|\, m_1 m_2$ we also have $-n \,|\, m_1 m_2$. Hence, since $0 < -n$, by the first part of the proof we can already state that $-n \,|\, k\,m_2$. And thus, $n \,|\, k\,m_2$ is also true.

Finally, if $n = 0$, then because of $m_1|n$ we can only have $k = |\,m_1|$. Therefore, in this case, the assertion $n|k\,m_2$ is an immediate consequence of the condition $n|m_1 m_2$.

Remark 3.2. In the sequel, we shall show that the $k = 1$ particular case of the above theorem can also be proved by using only Lemma 2.3.

Moreover, it is also worth mentioning that the following theorem can also be proved more easily by using Lemma 2.3 and Theorem 2.4 instead of Theorem 3.1.

Theorem 3.3. *If* $m, n \in \mathbb{Z}$ *such that* $m \neq 0$ *or* $n \neq 0$, *and moreover* $\alpha, \beta \in \mathbb{Z}$, *then the following assertions are equivalent:*

(1) $\alpha m + \beta n = 0$;

(2) $\exists\, l \in \mathbb{Z}: \quad \alpha = l n / (m; n), \quad \beta = -l m / (m; n)$.

Proof. If the assertion (1) holds and $n \neq 0$, then under the notation $x = m/n$ we evidently have

$$\alpha x = -\beta \in \mathbb{Z}.$$

Therefore, by Lemma 2.3, there exists an $l \in \mathbb{Z}$ such that

$$\alpha = l\, q(x), \qquad \text{and thus} \qquad \beta = -\alpha x = -l\, q(x)\, x = -l\, p(x).$$

Hence, by using Theorem 2.4, it can be easily seen that the assertion (2) also holds.

The converse implication $(2) \Longrightarrow (1)$ is quite obvious.

Remark 3.4. Unfortunately, to solve the more general Diophantine equation $\alpha m + \beta n = k$, Lemma 2.3, which is actually a particular case of [4, Theorem 1.18], is certainly not sufficient.

4. Some further applications of the functions p and q

From Theorem 3.1, by induction, we can easily get the following more general

Theorem 4.1. *If* $m_1, m_2, n \in \mathbb{Z}$ *and* $l \in \mathbb{N}$ *such that* $n \mid (m_1)^l m_2$, *and moreover* $k = (m_1; n)$, *then* $n \mid k^l m_2$.

Proof. From Theorem 3.1 we know that the assertion of the theorem is true for $l = 1$. Moreover, if $i \in \mathbb{N}$, then again by using Theorem 3.1 we can see that

$$n \;\big|\; (m_1)^{i+1} m_2, \qquad \text{i.e.,} \qquad n \;\big|\; m_1\big((m_1)^i m_2\big)$$

implies

$$n \;\big|\; k\big((m_1)^i m_2\big), \qquad \text{i.e.,} \qquad n \;\big|\; (m_1)^i (k\, m_2).$$

Therefore, if the assertion of the theorem is true for $l = i$, then it is also true for $l = i + 1$.

Now, by using the $k = 1$ particular case of Theorem 4.1 and following the treatment of Niven [6, § 4.3, p. 57], we can also prove the following much more general divisibility theorem

Theorem 4.2. *If* $a_i \in \mathbb{Z}$ *for all* $i = 0, \ldots, n$, *and moreover* $x \in \mathbb{Q}$ *such that*

$$\sum_{i=0}^{n} a_i \, x^{n-i} = 0 \,,$$

then $q(x) \mid a_0$ *and* $p(x) \mid a_n$.

Proof. In this case, by making use of the equality $x = p(x)/q(x)$, we can easily see that

$$\sum_{i=0}^{n} a_i \, p(x)^{n-i} \, q(x)^i = 0 \,,$$

and hence

$$a_0 \, p(x)^n = -q(x) \sum_{i=1}^{n} a_i \, p(x)^{n-i} \, q(x)^{i-1}$$

and

$$a_n \, q(x)^n = -p(x) \sum_{i=0}^{n-1} a_i \, p(x)^{n-1-i} \, q(x)^i \,.$$

Therefore,

$$q(x) \,\big|\, p(x)^n \, a_0 \qquad \text{and} \qquad p(x) \,\big|\, q(x)^n \, a_n \,.$$

Hence, by Remark 2.5 and the $k = 1$ particular case of Theorem 4.1, the required assertions are immediate.

Now, as some important particular cases of the above theorem, we can also state the following two theorems.

Theorem 4.3. *If* $a_i \in \mathbb{Z}$ *for all* $i = 1, \ldots, n$, *and moreover* $x \in \mathbb{Q}$ *such that*

$$x^n + \sum_{i=1}^{n} a_i \, x^{n-i} = 0 \,,$$

then $x \in \mathbb{Z}$ *such that* $x \mid a_n$.

Theorem 4.4. *If* $n, k \in \mathbb{N}$, *then* $\sqrt[n]{k} \in \mathbb{N}$ *or* $\sqrt[n]{k} \in \mathbb{R} \setminus \mathbb{Q}$.

Moreover, as a useful application of the latter theorem, we can also easily establish the following

Example 4.5. If $n \in \mathbb{N} \setminus \{1\}$, then $\sqrt[n]{n} \in \mathbb{R} \setminus \mathbb{Q}$.

Namely, by using induction or the Bernoulli-inequality, we can at once see that in this case $1 < n < 2^n$, and hence $1 < \sqrt[n]{n} < 2$.

5. Some supplementary notes

It is worth noticing that the $k=1$ particular case of Theorem 3.1 can also be proved by using only Lemma 2.3.

Theorem 5.1. *If* $m_1, m_2, n \in \mathbb{Z}$ *such that* $n \mid m_1 m_2$ *and* $(m_1; n) = 1$, *then* $n \mid m_2$.

Proof. If $n \neq 0$, then by defining $x = m_2/n$, we evidently have

$$n\,x = m_2 \in \mathbb{Z} \qquad \text{and} \qquad m_1 x = m_1 m_2/n \in \mathbb{Z}.$$

Hence, by Lemma 2.3, it is clear that

$$q(x) \leq (\,m_1;\, n\,) = 1\,.$$

Therefore, only $q(x) = 1$, and hence $x \in \mathbb{Z}$ can hold true.

Remark 5.2. By using Theorem 5.1, we can easily see that if $m_1, m_2, n \in \mathbb{Z}$ such that $n \mid m_1 m_2$ and n is prime, then $n \mid m_1$ or $n \mid m_2$.

Namely, if $k = (m_1; n)$, then by using that n is prime we can see that $k = 1$ or $k = n$. Therefore, if $n \nmid m_1$, then $k = 1$. Thus, by Theorem 5.1, $n \mid m_2$.

The importance of the above assertion lies mainly in the fact that it allows of an easy proof of the unicity part of the prime factorization theorem [5, Theorem 1, pp. 3–5].

Moreover, it is also worth mentioning that following the ideas of Beigel [1], Theorem 4.3 can also be proved by using only Definition 2.1.

Theorem 5.3. *If* $a_i \in \mathbb{Z}$ *for all* $i = 1, \ldots, n$, *and moreover* $x \in \mathbb{Q}$ *such that*

$$x^n + \sum_{i=1}^{n} a_i\, x^{n-i} = 0\,,$$

then $x \in \mathbb{Z}$ *such that* $x \mid a_n$.

Proof. To prove the essential part of the theorem, it is enough to show that

$$x_k = x\,p(x)^{\,n-k} \in \mathbb{Z} \qquad \text{for all} \qquad k = 1, 2, \cdots, n\,.$$

Namely, this implies in particular that $x = x_n \in \mathbb{Z}$.

To prove the above apparently more general assertion, note that

$$x_1 = x\,p(x)^{\,n-1} = x^n\,q(x)^{\,n-1} = -\sum_{i=1}^{n} a_i\, p(x)^{n-i}\, q(x)^{i-1} \in \mathbb{Z}\,.$$

Moreover, if $k \in \{1, 2, \cdots, n-1\}$ such that $x_k \in \mathbb{Z}$, then the number

$$r = \langle x_{k+1} \rangle\, q(x) = x_{k+1}\, q(x) - [\, x_{k+1}]\, q(x) = p(x)^{n-k} - [\, x_{k+1}]\, q(x)$$

satisfies not only $0 \leq r < q(x)$ and $r \in \mathbb{Z}$, but also

$$r\, x = p(x)^{n-k}\, x - [\, x_{k+1}]\, q(x)\, x = x_k - [\, x_{k+1}]\, p(x) \in \mathbb{Z}\, .$$

Therefore, by the definition of $q(x)$, we can only have $r = 0$, and hence $\langle x_{k+1} \rangle = 0$.

Moreover, it is also noteworthy that the following particular case of Theorem 4.4 has an even more simple proof.

Theorem 5.4. *If* $k \in \mathbb{N}$, *then* $\sqrt{k} \in \mathbb{N}$ *or* $\sqrt{k} \in \mathbb{R} \setminus \mathbb{Q}$.

Proof. If $x = \sqrt{k} \in \mathbb{Q}$, then the number

$$r = \langle\, x \,\rangle\, q(x) = x\, q(x) - [x]\, q(x) = p(x) - [x]\, q(x)$$

satisfies not only $0 \leq r < q(x)$ and $r \in \mathbb{Z}$, but also

$$r\, x = x^2 q(x) - [x]\, x\, q(x) = k\, q(x) - [x]\, p(x) \in \mathbb{Z}\, ,$$

Therefore, by the definition $q(x)$, we can only have $r = 0$, and hence $\langle\, x \,\rangle = 0$.

References

1. R. Beigel, *Irrationality without number theory*, Amer. Math. Monthly **98** (1991), 332–335.
2. Z. Boros and Á. Száz, *Functions which should preceed the Riemann function*, Technical Report (Inst. Math. Inf., Univ. Debrecen) **95/131**, 17 pp. (Hungarian)
3. Z. Boros and Á. Száz, *Some further applications of the smallest denominator function*, Technical Report (Inst. Math. Inf., Univ. Debrecen) **95/133**, 7 pp. (Hungarian)
4. Z. Boros and Á. Száz, *The smallest denominator function and the Riemann function*, Acta Math. Acad. Paed. Nyíregyhásiensis **14** (1998), 1–17, www.bgytf.hu/~amapn.
5. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, Berlin, 1982.
6. I. Niven, *Numbers: Rational and Irrational*, The Mathematical Association of America, Washington, 1961.

(Received November 4, 1998)

Institute of Mathematics and Informatics,
Lajos Kossuth University,
H-4010 Debrecen, Pf. 12, Hungary
E-mail address: boros@math.klte.hu and szaz@math.klte.hu