Publ. Math. Debrecen
78/1 (2011), 245–249
DOI: 10.5486/PMD.2011.4804

Euclidean algorithm in different norms

By IMRE Z. RUZSA (Budapest) and PÉTER P. VARJÚ (Szeged)

Abstract. We describe those norm-like functions on the integers which admit a Euclidean algorithm.

1. Introduction

A *norm* on the ring of integers of an algebraic number field is a nonnegative integer-valued completely multiplicative function f. A useful (and quite rare) property it may have is the possibility of a *Euclidean algorithm*, which means that for any integers a, b, $b \neq 0$ we can find integers q, r such that $a = qb + r$ and $f(r) < f(b)$. A familiar example is $N(n) = |n|$ in $\mathbb{Z}$. Inspired by a question of Attila Pethő and Sándor Turjányi we explore which other norms on $\mathbb{Z}$ have this property.

First we describe a class of functions that can be used as such a norm. Let p be a prime and let γ and w be positive integers such that $w \geq p^\gamma$. If $x = p^k x' > 0$ where $p \nmid x'$ then set

$$f_{\gamma,p,w}(x) = f_{\gamma,p,w}(-x) = w^k x'^\gamma,$$

and set $f_{\gamma,p,w}(0) = 0$. (In particular, if $w = p^\gamma$, we recover the powers of the absolute value.)

2000 *Mathematics Subject Classification:* 11A05, 11A25.
Key words and phrases: norm, multiplicative function.
Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. K 61908, K 72731.
Supported by Fulbright Science and Technology Award No. 15073240.

The complete multiplicativity of these functions is clear. We check that they also satisfy the division property. Indeed, let $b = p^k b'$ where $p \nmid b'$. If $b|a$ then the statement is clear. Assume $b \nmid a$. There is a q such that

$$|b| > a - q|b| > a - (q+1)|b| > -|b|.$$

Set $r = a - q|b|$ or $r = a - (q+1)|b|$ such that $p^{k+1} \nmid r$. Then $r = p^l r'$ where $p \nmid r'$ and $l \leq k$. By definition, using $w \geq p^\gamma$ we get

$$f_{\gamma,p,w}(r) = w^l \left|\frac{r}{p^l}\right|^\gamma \leq w^k \left|\frac{r}{p^k}\right|^\gamma < w^k \left|\frac{b}{p^k}\right|^\gamma = f_{\gamma,p,w}(b),$$

which was to be proven.

Our aim is to show that the above list contains all functions for which there is a Euclidean algorithm.

Theorem. *Let $f : \mathbb{Z} \to \mathbb{Z}$ be a nonnegative completely multiplicative function. If f has the property that for all integers a, b, $b \neq 0$ we can find integers q, r such that $a = qb + r$ and $f(r) < f(b)$, then there is a prime p and positive integers γ and w with $w \geq p^\gamma$ such that $f = f_{\gamma,p,w}$.*

The first author posed this as a problem in the 2004 Schweitzer competition, and the proof below is based on the solution by the second author.

2. Proof

In the proof we shall use the following lemma.

Lemma. *Let n, m, l be integers such that $0 < n < m < l$, and n and m are coprime. If $l^k > km^{k+1}$ with some positive integer k, then there exist nonnegative integers $\alpha_0, \dots, \alpha_k$ such that*

$$l^k = \alpha_0 m^k + \alpha_1 m^{k-1} n + \cdots + \alpha_k n^k.$$

Proof. Note that such a representation obviously exists if the coefficients are allowed to be negative.

Let

$$l^k = \alpha'_0 m^k + \alpha'_1 m^{k-1} n + \cdots + \alpha'_k n^k$$

with some possibly negative integers α'_j. Let i be the least index for which $0 < \alpha'_i \leq n$ fails. If $i < k$, then we have $\alpha'_i = \alpha''_i + nq$ and $0 < \alpha''_i \leq n$ with some integer q. Set $\alpha''_{i+1} = \alpha'_{i+1} + mq$, and $\alpha''_j = \alpha'_j$ for $j \neq i, i+1$. Continue this process until we get a representation

$$l^k = \alpha_0 m^k + \alpha_1 m^{k-1} n + \cdots + \alpha_k n^k$$

with integers $0 < \alpha_j \leq n$ for all $j < k$. Then by assumption, we have $\alpha_k \geq l^k - knm^k \geq 0$, and the claim follows. □

Now we prove the main result.

Proof of the Theorem. Let f be a function satisfying the assumptions of the theorem. First note that $f(0) = f(0 \cdot n) = f(0)f(n)$ for each n, hence $f(0) = 0$ or $f \equiv 1$. In the second case, the condition fails with $a = b = 1$, so $f(0) = 0$.

For each n we have $f(n) = f(1 \cdot n) = f(1)f(n)$ which yields $f(1) = 1$ or $f \equiv 0$. The second case is impossible again. By

$$1 = f(1) = f((-1) \cdot (-1)) = f(-1)f(-1)$$

we have $f(-1) = 1$ or $f(-1) = -1$. By nonnegativity, only the first is possible. Consequently $f(-n) = f(-1)f(n) = f(n)$ in general.

Claim 1. If $x, y > 0$ then $f(x+y) > f(x)$ or $f(x+y) > f(y)$.

Indeed, assume the contrary and consider a counterexample for which $f(x+y)$ is minimal. We apply the division assumption with $b = x + y$ and $a = y$ to get an integer q with

$$f(y - q(x+y)) < f(x+y).$$

There may be several such values of q; select one for which $|q|$ is minimal. By assumption $q \neq 0$ and $q \neq 1$. Assume first that $q > 1$; the other case, namely $q < 0$, can be handled similarly. Then we have

$$f(qx + (q-1)y) < f(x+y) \leq f((q-1)x + (q-2)y),$$

where the second inequality follows from the minimality of q. But then we can replace x and y by $x' = x + y$ and $y' = (q-1)x + (q-2)y$, and this is a counterexample for the claim with $f(x' + y') < f(x+y)$, a contradiction.

Claim 2. If $x_1, x_2, \ldots, x_k > 0$ then at least one of the inequalities $f(x_1 + \cdots + x_k) > f(x_i)$ holds $(1 \leq i \leq k)$.

For $k = 2$ this is the statement of the previous claim. For higher values of k we use induction. Assume that $k > 2$ and the claim holds for $k - 1$. Then

$$\begin{aligned} f(x_1 + \cdots + x_{k-1} + x_k) &> \min\{f(x_1 + \cdots + x_{k-1}), f(x_k)\} \\ &> \min\{f(x_1), \ldots, f(x_{k-1}), f(x_k)\}, \end{aligned}$$

by the previous claim and by the induction hypothesis.

Claim 3. If $0 < n < m < l$, and n and m are coprime, then $f(n) < f(l)$ or $f(m) < f(l)$.

Assume to the contrary that $f(l) \le f(n)$ and $f(l) \le f(m)$. For large enough k we have $l^k > km^{k+1}$. Applying the Lemma we get a representation

$$l^k = \alpha_0 m^k + \alpha_1 m^{k-1} n + \cdots + \alpha_k n^k,$$

with nonnegative integers α_j. For arbitrary i we have

$$f(l^k) = f(l)^k \le f(m)^{k-i} f(n)^i = f(m^{k-i} n^i) \le f(\alpha_i m^{k-i} n^i),$$

which contradicts the previous claim.

We resume the proof of the Theorem. There may or may not be positive prime powers p, q such that $p < q$ and $f(p) \ge f(q)$. Assume first that such prime powers do exist.

Let r be an arbitrary prime, not dividing pq.

Now if for some positive integers α, β we have $q^\alpha > r^\beta$, then applying Claim 3 with $n = \min(p^\alpha, r^\beta)$, $m = \max(p^\alpha, r^\beta)$ and $l = q^\alpha$, we get $f(q^\alpha) > f(r^\beta)$. Conversely, when $q^\alpha < r^\beta$, then setting $n = p^\alpha$, $m = q^\alpha$ and $l = r^\beta$ we get $f(q^\alpha) < f(r^\beta)$.

These observations together imply

$$f\left(q^{\lfloor \beta \log r / \log q \rfloor}\right) < f(r^\beta) < f\left(q^{\lceil \beta \log r / \log q \rceil}\right).$$

By multiplicativity, we obtain

$$\frac{\lfloor \beta \log r / \log q \rfloor}{\beta} < \frac{\log f(r)}{\log f(q)} < \frac{\lceil \beta \log r / \log q \rceil}{\beta}.$$

Letting $\beta \to \infty$, we get

$$\log(f(r)) = \log r \frac{\log f(q)}{\log q},$$

whence

$$f(r) = r^\gamma \tag{2.1}$$

with a positive real constant $\gamma = \log f(q) / \log q$ independent of r.

We have this equality for all primes r not dividing p or q. Notice that since $\gamma = \log f(q) / \log q$, (2.1) holds for the prime divisor of q also. Let p' be the prime divisor of p, and set $w = f(p')$. Then $f = f_{\gamma, p', w}$, and

$$\frac{\log w}{\log p'} = \frac{\log(f(p))}{\log p} > \frac{\log(f(q))}{\log q} = \gamma,$$

which yields $w > p'^\gamma$.

If $p < q$ implies $f(p) < f(q)$ for all prime powers p and q, then we get (2.1) for arbitrary primes in a similar (and somewhat easier) way.

Finally we show that γ is an integer. Since $f(n) = n^\gamma$ whenever n is not divisible by p, the function $g(x) = (px+1)^\gamma$ is integer for positive integer values of x. Consider its k'th difference for an integer $k > \gamma$. This is integer as well, and we have

$$\Delta^k g(n) = g^{(k)}(t) = \gamma(\gamma-1)\dots(\gamma-k+1)p^k(pt+1)^{\gamma-k}$$

for some real $t \in [n, n+k]$. Since the right hand side tends to 0, it must vanish for large n, hence so does one of the factors $\gamma - j$. □

IMRE Z. RUZSA
ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS
H-1364 BUDAPEST, P.O. BOX 127
HUNGARY

E-mail: ruzsa@renyi.hu

PÉTER P. VARJÚ
DEPARTMENT OF MATHEMATICS
PRINCETON UNIVERSITY
PRINCETON, NJ 08544
USA

AND

ANALYSIS AND STOCHASTICS RESEARCH GROUP
OF THE HUNGARIAN ACADEMY OF SCIENCES
UNIVERSITY OF SZEGED
SZEGED
HUNGARY

E-mail: pvarju@princeton.edu

(Received January 4, 2010; revised May 18, 2010)