ma
the
ma
tisch

cen
trum

MC

AFDELING ZUIVERE WISKUNDE ZN 54/73 JUNE

A.E. BROUWER and H.W. LENSTRA Jr.
MULTIPLICATIVE DIVISION ALGORITHMS ON THE INTEGERS

amsterdam 1973

stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE ZN 54/73 JUNE

A.E. BROUWER and H.W. LENSTRA Jr.

MULTIPLICATIVE DIVISION ALGORITHMS ON THE INTEGERS

2e boerhaavestraat 49 amsterdam

BIBLIOTHEEK

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

AMS (MOS) subject classification scheme (1970): 10A05, 13A15, 13F10

Multiplicative division algorithms on the integers.

A.E. Brouwer, H.W. Lenstra Jr.

1. Introduction.

Let $\mathbb{Z}$ denote the ring of rational integers, and let W be a totally ordered set. A function $\phi : \mathbb{Z} - \{0\} \to W$ is called a division algorithm on $\mathbb{Z}$ if

(i) the image of ϕ is a well ordered subset of W;

(ii) for every $a, b \in \mathbb{Z}$, $b \neq 0$, there exist $q, r \in \mathbb{Z}$ such that

$$a = qb + r$$

$$r = 0 \text{ or } \phi(r) < \phi(b).$$

If W is the set of positive real numbers $\mathbb{R}_+$, we call ϕ multiplicative if

$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in \mathbb{Z}$, $ab \neq 0$.
Theorem 1 describes all multiplicative division algorithms on $\mathbb{Z}$, thus answering a question of R.K. Dennis [1].

Theorem 1.
Let $\phi : \mathbb{Z} - \{0\} \to \mathbb{R}_+$ be a multiplicative division algorithm. Then there exist a prime number p and real numbers $A > 0$, $B \geq 0$ such that

$$\phi(a) = |a|^A \cdot a_p^{\,B} \qquad \text{for all } a \in \mathbb{Z},\ a \neq 0;$$

here a_p denotes the largest power of p dividing a. Conversely, if p is a prime and $A > 0$, $B \geq 0$ are reals, then the function ϕ defined by the above equation is a multiplicative division algorithm on $\mathbb{Z}$.
Moreover, ϕ assumes only integral values if and only if both A and p^{A+B} are positive integers.

This theorem will be deduced from the following two results.

Theorem 2.

Let W be any well ordered set, and let $\phi : \mathbb{Z} - \{0\} \to W$ be a function. Then ϕ is a division algorithm on $\mathbb{Z}$ if and only if

$$\min \{\phi(r), \phi(-s)\} < \min \{\phi(r+s), \phi(-r-s)\}$$

for all $r, s \in \mathbb{Z}$, $r > 0$, $s > 0$.

Theorem 3.

Denote by $\mathbb{N}$ the set of positive integers. Suppose $\phi : \mathbb{N} \to \mathbb{R}_+$ satisfies

$$\phi(ab) = \phi(a).\phi(b)$$

$$\phi(a+b) \geq \min \{\phi(a), \phi(b)\}$$

for all $a, b \in \mathbb{N}$. Then there exist a prime number p and nonnegative real numbers A, B such that

$$\phi(a) = a^A \,.\, a_p{}^B$$

for all $a \in \mathbb{N}$.

In section 5 we show how theorem 3 can be used to sharpen a certain lemma from valuation theory.

2. Proof of theorem 2.

Let W be a well ordered set, and let $\phi : \mathbb{Z} - \{0\} \to W$ be a map. If ϕ satisfies the system of inequalities indicated in theorem 2, it is clear that ϕ is a division algorithm. In fact, for $a, b \in \mathbb{Z}$, $b \neq 0$, one can find $q, r \in \mathbb{Z}$ such that

$$a = q.b + r,$$
$$r = 0 \text{ or } \phi(r) < \phi(b),$$
$$|r| < |b|.$$

Conversely, assume ϕ is a division algorithm. Consider a triple (r,s,b) of integers such that

(2.1) $\qquad r > 0, \quad s > 0, \quad r + s = |b|.$

To prove theorem 2, it suffices to show

(2.2) $\qquad \phi(r) < \phi(b)$ or $\phi(-s) < \phi(b)$.

This is done with induction on $\phi(b)$. So assume the assertion is true for all triples (r',s',b') as above for which $\phi(b') < \phi(b)$.

If $\phi(-b) < \phi(b)$, the induction hypothesis, applied to the triple $(r,s,-b)$, yields $\phi(r) < \phi(-b)$ or $\phi(-s) < \phi(-b)$, and (2.2) follows. Therefore assume $\phi(-b) \geq \phi(b)$, so

(2.3) $\qquad \phi(|b|) \geq \phi(b), \qquad \phi(-|b|) \geq \phi(b).$

Now choose d in the residue class (r mod b) such that $\phi(d)$ is minimal (remark that 0 is not in this residue class, by (2.1)). Because ϕ is a division algorithm, we have

(2.4) $\qquad \phi(d) < \phi(b).$

We distinguish three cases:

(i) $\quad d > |b|$

(ii) $\quad d < -|b|$

(iii) $\quad d \in \{r, -s\}$.

In case (iii), (2.2) follows by (2.4). In each of the cases (i) and (ii) we derive a contradiction.

Case (i). The triple $(r',s',b') = (d-|b|,|b|,d)$ has the properties corresponding to (2.1). By (2.4) we may apply the induction hypothesis, and we find

$$\phi(d-|b|) < \phi(d) \text{ or } \phi(-|b|) < \phi(d).$$

But the first alternative is excluded by the minimality assumption on $\phi(d)$, and the second one by (2.3) and (2.4).

Case (ii). Applying the induction hypothesis to the triple $(r',s',b') =$

$= (|b|, -d-|b|, d)$ we get

$$\phi(|b|) < \phi(d) \quad \text{or} \quad \phi(d+|b|) < \phi(d).$$

The first possibility contradicts (2.3) and (2.4), the second one our choice of d.
This finishes the proof of theorem 2.

3. Proof of theorem 3.

Let $\phi : \mathbb{N} \to \mathbb{R}_+$ satisfy

(3.1) $$\phi(ab) = \phi(a) \cdot \phi(b)$$

(3.2) $$\phi(a+b) \geq \min\{\phi(a), \phi(b)\},$$

for all a, $b \in \mathbb{N}$. From (3.1) it follows that $\phi(1) = 1$, and using (3.2) inductively we find $\phi(a) \geq 1$ for all $a \in \mathbb{N}$. Define

$$\psi(a) = \frac{\log \phi(a)}{\log a} \qquad \text{for } a \in \mathbb{N},\ a \geq 2.$$

Then $\psi(a) \geq 0$, and $\phi(a) = a^{\psi(a)}$, for $a \geq 2$.

We first construct a natural number $k \geq 2$ such that

(3.3) $$\psi(a) \geq \psi(k) \qquad \text{for all } a \geq 2.$$

Let p be any prime number, $\alpha = \psi(p)$. If $\psi(q) \geq \alpha$ for all primes q, then $k = p$ works. So choose a prime q such that $\beta = \psi(q) < \alpha$. If $\psi(r) \geq \beta$ for all $r \geq 2$ we can take $k = q$. So let $r \geq 2$ be a natural number such that $\gamma = \psi(r) < \beta$. Then $\beta > 0$, and replacing $\phi(a)$ by $\phi(a)^{1/\beta}$ for all a we may suppose

$$\phi(q) = q, \quad \beta = 1, \quad 0 \leq \gamma < 1 < \alpha.$$

Now choose a natural number M such that

(3.4) $\qquad M \geq r$

(3.5) $$\frac{M^{1-\gamma}}{pq} > \frac{1}{\sqrt{(1-p^{\gamma-\alpha})}} .$$

Let $k \in \mathbb{N}$, $2 \leq k \leq M$ be chosen such that

$$\delta = \psi(k) = \min \{\psi(a) \mid 2 \leq a \leq M\}.$$

By (3.4) we have $\delta \leq \gamma < 1$.

We assert that k has property (3.3). Otherwise, let $a \in \mathbb{N}$ be minimal such that $\psi(a) < \delta = \psi(k)$. We derive a contradiction. By definition of δ, we have $a > M$, so (3.5) implies $a^{1-\gamma} / (pq) > 1$, i.e. $q.a^{\gamma} < \frac{1}{p}.a.$. Let q^n be the highest power of q which is smaller than $q.a^{\gamma}$. Then

$$a^{\gamma} \leq q^n < q.a^{\gamma} < \frac{1}{p}a.$$

Choose $c \in \{1, 2, \ldots, p\}$ such that $a + c.q^n \equiv 0 \bmod p$. Then

$$c.q^n < p.q.a^{\gamma} < a.$$

Therefore (3.5) yields

$$(1 - \frac{c^2q^{2n}}{a^2})^{\delta} > 1 - \frac{c^2q^{2n}}{a^2} \geq 1 - (pqa^{\gamma-1})^2$$

$$> 1 - \sqrt{(1-p^{\gamma-\alpha})}^2 = p^{\gamma-\alpha}.$$

Also

$$0 < a - c.q^n < a, \qquad 0 < \frac{a+c.q^n}{p} < a$$

so the minimality condition on a implies

$$\phi(a-c.q^n) \geq (a-c.q^n)^{\delta}, \quad \phi(\frac{a+c.q^n}{p}) \geq (\frac{a+c.q^n}{p})^{\delta}.$$

Hence

$$\phi(a^2-c^2.q^{2n}) = \phi(p).\phi(a-c.q^n).\phi(\frac{a+c.q^n}{p})$$

$$\geqq p^{\alpha}.(a-c.q^n)^{\delta}.(\frac{a+c.q^n}{p})^{\delta}$$

$$= p^{\alpha-\delta}.(1 - \frac{c^2q^{2n}}{a^2})^{\delta}.a^{2\delta}$$

$$> p^{\alpha-\delta}.p^{\gamma-\alpha}.a^{2\delta}$$

$$\geq a^{2\delta}.$$

Also

$$\phi(c^2.q^{2n}) \geq \phi(q^{2n}) = q^{2n} \geq a^{2\gamma} \geq a^{2\delta}.$$

We conclude

$$\phi(a^2) \geq \min\{\phi(a^2-c^2.q^{2n}),\ \phi(c^2.q^{2n})\} \geq a^{2\delta},$$

$$\phi(a) \geq a^{\delta}, \qquad \psi(a) \geq \delta,$$

contradicting our choice of a. This finishes the construction of k.

Now fix k such that (3.3) holds. Putting $A = \psi(k)$ we have

(3.6) $$\psi(a) \geq A = \psi(k), \qquad \phi(a) \geq a^A \qquad \text{for all } a \geq 2.$$

If $\psi(p) = A$ for all primes p, theorem 3 follows by taking $B = 0$, p = any prime. So suppose

$$\psi(p) = A + B > A, \qquad B > 0,$$

for some prime p. We remark

(3.7) $$p|a \Rightarrow \phi(a) = \phi(\frac{a}{p}).\phi(p) \geq$$

$$\geq (\frac{a}{p})^A.p^{A+B} = a^A.p^B.$$

Since $\phi(k) = k^A$ it follows that $p \nmid k$.

To prove theorem 3 it is clearly sufficient to show that $\psi(s) = A$ for all primes $s \neq p$. So let s be a prime $\neq p$. Suppose $n, m \in \mathbb{N}$ satisfy

$$k^n > s^m.$$

If $N \in \mathbb{N}$ is divisible by $p - 1$ we have

$$p | k^{n.N} - s^{m.N}$$

and taking N sufficiently large we find by (3.7):

$$\begin{aligned}\phi(k^{n.N} - s^{m.N}) &\geq (k^{n.N} - s^{m.N})^A \, . \, p^B \\ &= k^{n.N.A} \, . \, (1 - \frac{s^{mN}}{k^{nN}})^A \, . \, p^B \\ &> k^{n.N.A} = \phi(k^{n.N}).\end{aligned}$$

Using (3.2) with $a = k^{n.N} - s^{m.N}$ and $b = s^{m.N}$ we get

$$\phi(k^{n.N}) \geq \phi(s^{m.N})$$

$$\phi(k)^n \geq \phi(s)^m.$$

If $\phi(k) = 1$, $\psi(k) = 0$ we conclude $\phi(s) = 1$, $\psi(s) = 0 = A$, as desired. If $\phi(k) > 1$, the preceding discussion shows:

$$\frac{n}{m} > \frac{\log s}{\log k} \quad \Rightarrow \frac{n}{m} \geq \frac{\log \phi(s)}{\log \phi(k)} \, .$$

Since the rational numbers are dense in the reals this implies

$$\frac{\log s}{\log k} \geq \frac{\log \phi(s)}{\log \phi(k)}$$

$$A = \psi(k) = \frac{\log \phi(k)}{\log k} \geq \frac{\log \phi(s)}{\log s} = \psi(s).$$

By (3.6) we conclude $\psi(s) = A$, as desired.
This completes the proof of theorem 3.

4. Proof of theorem 1.

Let $\phi : \mathbb{Z} - \{0\} \to \mathbb{R}_+$ be a multiplicative division algorithm. Then $\phi(-1)^2 = \phi(1)^2 = \phi(1)$ so $\phi(-1) = 1$. Therefore $\phi(-a) = (a)$ for all a. From theorem 2 we get

$$\phi(a+b) > \min\{\phi(a),\phi(b)\}$$

for all $a > 0$, $b > 0$. Using theorem 3 we find a prime p and reals $A \geq 0$, $B \geq 0$ such that $\phi(a) = |a|^A \,.\, a_p^{\,B}$ for all $a \in \mathbb{Z}$, $a \neq 0$. Since

$$(p+1)^A = \phi(p+1) > \min\{\phi(p),\phi(1)\} = 1$$

we have $A > 0$. This proves the first part of theorem 1.

That, conversely, the function ϕ defined by $\phi(a) = |a|^A \,.\, a_p^{\,B}$ is a multiplicative division algorithm for any prime p and all $A > 0$, $B \geq 0$, is easy to check.

If A and p^{A+B} are positive integers, it is clear that ϕ assumes only integral values. To prove the converse, we recall a simple fact from analysis.

For a function $f : \mathbb{R}_+ \to \mathbb{R}$ we define $\Delta f : \mathbb{R}_+ \to \mathbb{R}$ by $\Delta f(x) = f(x+1) - f(x)$, and inductively $\Delta^1 f = \Delta f$, $\Delta^n f = \Delta.\Delta^{n-1} f$, $n \in \mathbb{N}$, $n \geq 2$.

<u>Lemma</u>

Let $f : \mathbb{R}_+ \to \mathbb{R}$ be n times differentiable, $n \in \mathbb{N}$. Then for all $y \in \mathbb{R}_+$ there exists a $v \in [y,y+n]$ such that

$$f^{(n)}(v) = \Delta^n f(y).$$

<u>Proof</u>. Let $h(x) = \sum_{i=0}^{n} h_i x^i$ be the unique polynomial of degree $\leq n$ for which $g(x) = f(x) - h(x)$ has zeros in $x = y, y+1, \ldots, y+n$. Using Rolle's theorem repeatedly we find $v \in [y, y+n]$ with

$$g^{(n)}(v) = 0.$$

Furthermore, it is clear that

$$\Delta^n g(y) = 0, \qquad \Delta^n h(x) = h^{(n)}(x) = n!h_n \qquad \text{for } x \in \mathbb{R}_+$$

so

$$\Delta^n f(y) = \Delta^n g(y) + \Delta^n h(y) = 0 + n!h_n = g^{(n)}(v) + h^{(n)}(v) = f^{(n)}(v).$$

This proves the lemma.

We apply this lemma with $f(x) = (p.x+1)^A$. Then $\phi[\mathbb{Z} - \{0\}] \subset \mathbb{Z}$ implies $f[\mathbb{N}] \subset \mathbb{Z}$, hence by induction on n we get

$$\Delta^n f(y) \in \mathbb{Z}, \qquad \text{for all } n,\ y \in \mathbb{N}.$$

Choose $n > A$ fixed. Then for y sufficiently large the lemma yields

$$|\Delta^n f(y)| \le \max_{v \in [y,y+n]} |f^{(n)}(v)| = |A.(A-1)\ldots(A-n+1).p^n(py+1)^{A-n}| < 1.$$

Hence $\Delta^n f(y) = 0$ for $y \in \mathbb{N}$ sufficiently large. So there exists a polynomial f_1 of degree $\le n - 1$ such that $f(y) = f_1(y)$ for all $y \in \mathbb{N}$ sufficiently large. Then

$$\lim_{y \in \mathbb{N}, y \to \infty} \frac{f_1(y)}{f(y)} = 1$$

so A = degree f_1 is an integer, which we knew already to be positive.
Also $\phi(p) = p^{A+B}$ is a positive integer.
This concludes the proof of theorem 1.

5. Valuations of the natural numbers.

Let R be a commutative domain and $F : R \to \mathbb{R}_+ \cup \{0\}$ a function.
Suppose there exists a constant $C \in \mathbb{R}_+$ such that

$$F(a) = 0 \iff a = 0$$

(5.1) $$F(ab) = F(a)F(b)$$

(5.2) $$F(a+b) \le C \cdot \max\{F(a), F(b)\}$$

for all $a, b \in R$. Then F is called a valuation of R.

By analogy, let us call a function $F : \mathbb{N} \to \mathbb{R}_+$ a valuation of $\mathbb{N}$ if there is a constant $C \in \mathbb{R}_+$ such that (5.1) and (5.2) hold for all $a, b \in \mathbb{N}$.

The following lemma is frequently used to determine all valuations of $\mathbb{Z}$, cf. [2], ch.I, §3, lemma 3.

Lemma

Let F be a valuation of $\mathbb{N}$. Then either $F(a) \le 1$ for all $a \in \mathbb{N}$, or there is a $\lambda \in \mathbb{R}_+$ such that $F(a) = a^{\lambda}$ for all $a \in \mathbb{N}$.

For the proof of this lemma we refer to [2].
Using theorem 3, we can complete the conclusion of the lemma in the following way.

Theorem 4.

Let $F : \mathbb{N} \to \mathbb{R}_+$ be a function. Then F is a valuation of $\mathbb{N}$ if and only if there exist a prime p and real numbers λ, μ such that $\mu \le 0$, $\lambda\mu \ge 0$, $F(a) = a^{\lambda} \cdot a_p^{\mu}$ for all $a \in \mathbb{N}$.

Proof of theorem 4, cf. [2], ch. I, §3, lemma 4. First assume F is a valuation of $\mathbb{N}$.
If $F(a) = a^{\lambda}$ for some $\lambda \in \mathbb{R}_+$ and all $a \in \mathbb{N}$ we can put $\mu = 0$, p= any prime number. So by the lemma we may assume $F(a) \le 1$ for all a. Let $n \in \mathbb{N}$, $N = 2^n - 1$. By induction on n, we get from (5.2)

$$F\left(\sum_{i=0}^{N} a_i\right) \le C^n \cdot \max\{F(a_i) \mid 0 \le i \le N\}, \qquad \text{for } a_i \in \mathbb{N}.$$

Applying this to

$$(a+b)^N = \sum_{i=0}^{N} \binom{N}{i} a^i b^{N-i}$$

and using

$$F(\binom{N}{i} a^i b^{N-i}) \leq F(a)^i \, . \, F(b)^{N-i} \leq \max \{F(a), F(b)\}^N$$

we find

$$F((a+b)^N) \leq C^n \, . \, \max \{F(a), F(b)\}^N.$$

Taking N-th roots and letting n go to infinity we conclude

$$F(a+b) \leq \max \{F(a), F(b)\}.$$

Define $\phi(a) = F(a)^{-1}$; then theorem 3 applies to ϕ, so there is a prime p and there are reals $A \geq 0$, $B \geq 0$ such that

$$\phi(a) = a^A \, . \, a_p^{\,B}$$

for all $a \in \mathbb{N}$. Putting $\lambda = -A$ and $\mu = -B$ proves the "only if"part. The "if"-part may be left to the reader.

References.

1. R.K. Dennis, Which are the multiplicative algorithms on **Z**?, Oral Comm. Plans s. Bex, 4 (1973) 1 - 8.
2. A. Weil, Basic number theory, Springer, Berlin etc., 1967.