Euclid's theorem : a bit more

Autor(en): **Zorzi, Alberto**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **68 (2013)**

PDF erstellt am: **05.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-515904

Elem. Math. 68 (2013) 148 – 153
0013-6018/13/040148-6
DOI 10.4171/EM/233

Elemente der Mathematik

Euclid's theorem: a bit more

Alberto Zorzi

Alberto Zorzi graduated in mathematics at the University of Padova in 1983. Then he worked in the field of the computer science. Since 2006 he is professor at IUAV (Istituto Universitario Architettura Venezia), Italy. His interests are number theory and applications of mathematics.

1 Introduction

Euclid's theorem asserts that there are infinitely many prime numbers. It has numerous proofs; for example [1] describes the most elegant ones, while [4] gives a more exhaustive bibliography. We propose a new proof based on the observation that, substantially, the infinitude of prime numbers depends on how fast the result of the product grows when its operands increase. More specifically, we provide an explicit criterion to check the infinitude of primes for a class of operations on $\mathbb{N}$, which verifies such growth by computing a limit (see Theorem 4 and Corollary 5). Then we prove that the criterion is also necessary under certain conditions (Theorem 6).

2 Over the product

To define a set of operations on $\mathbb{N}$ we need to generalize a few notions and to introduce some terminology (see for example [3]). The set of natural numbers endowed with the product is a *monoid*. Moreover such monoid is *reduced*, *atomic* and *factorial* because 1 is

Mit der Addition und der Multiplikation natürlicher Zahlen sind wir von Kindesbeinen an vertraut. $\mathbb{N}$ erhält durch das gewöhnliche Produkt die Struktur eines Monoids mit unendlich vielen Atomen, den Primzahlen. Der Autor des vorliegenden Artikels geht der Frage nach, ob man $\mathbb{N}$ mit einer anderen Produktstruktur ausstatten kann, so dass ebenfalls ein Monoid mit unendliche vielen Atomen entsteht. Überraschenderweise existieren unendlich viele derartige Monoidstrukturen auf $\mathbb{N}$. Die Frage ob unendlich viele Atome existieren wird dabei auf die Berechnung eines Limes reduziert. Dies lässt den Satz von Euklid über die nicht abbrechende Folge der Primzahlen in neuem Licht erscheinen.

the only invertible element, each natural number > 1 is the product of primes and such factorizations are unique.

More formally, by a *monoid* we mean a set M with an associative and commutative operation which has the unit element e and satisfies the *cancelation law* (if $ac = bc$, then $a = b$ for all a, b, c in M).

Let $M^\times$ be the group of invertible elements of M, then M is *reduced* if $M^\times = \{e\}$. An element $a \in M$ is an *atom* if $a \notin M^\times$ and $a = bc$ (with $b, c \in M$) implies $b \in M^\times$ or $c \in M^\times$. The monoid M is called *atomic* if every element of $M \backslash M^\times$ is a finite product of atoms, while M is *factorial* if each factorization is unique (up to units and the order of the factors). An example of an atomic but not factorial monoid is illustrated in the Table 4: each natural number is a product of the atoms a and b, although the factorizations are not unique. If M is factorial then we will say that the *fundamental theorem of arithmetic* holds for M.

Our aim is to define an infinite class of atomic monoids on $\mathbb{N}$ and to provide a condition to guarantee that a specific monoid has infinitely many atomic elements (Theorem 4). Moreover, we show that the condition is also necessary if the monoid is factorial (Theorem 6).

Now, let us define a set of operations on natural numbers.

Definition 1. Let $\bigotimes$ (or $\bigotimes$-product) denote an operation on $\mathbb{N}$ such that:

(P1) $\bigotimes$ is associative and commutative;

(P2) $\bigotimes$ has unit element e;

(P3) if $a < b$, then $a \bigotimes c < b \bigotimes c$ for any $a, b, c \in \mathbb{N}$.

Notice that the usual product is a $\bigotimes$-product.

Let $\underline{a}^n = a \bigotimes \cdots \bigotimes a$ (n times) and $\underline{a}^0 = e$. From now on we will use underlined bases to represent $\bigotimes$-powers, otherwise the powers are computed by the normal product.

Let $\left(\mathbb{N}, \bigotimes\right)$ denote the set $\mathbb{N}$ endowed with the operation $\bigotimes$.

Proposition 2. *For any $\bigotimes$-product, $\left(\mathbb{N}, \bigotimes\right)$ is a reduced atomic monoid and $e = 1$.*

Proof. According to properties (P1), (P2) and (P3), $\left(\mathbb{N}, \bigotimes\right)$ is a monoid. Let us suppose by contradiction that $1 < e$. Then $\underline{1}^2 = 1 \bigotimes 1 < e \bigotimes 1 = 1 < e$ and there should exist a strictly decreasing sequence $1, \underline{1}^2, \underline{1}^3, \ldots$ of natural numbers less than e; thus $e = 1$. The monoid is reduced because $a \bigotimes b > a, b$ if $a, b > 1$ (by property (P3)).

Finally, to see that the monoid is atomic it suffices to apply the last inequality and to imitate the usual proof for the standard product (as in [2]). □

3 An infinite class of operations

To prove that there are infinitely many $\bigotimes$-products, below we illustrate an algorithm to build a generic $\bigotimes$-product. The operation is described by showing how to compute $a \bigotimes b$ for any pair of natural numbers a and b (Table T), and how to represent each natural number as a $\bigotimes$-product of atoms (Table N).

Notice that the Table T must be symmetric because $\bigotimes$ is commutative, so it is sufficient to fill only the entries $a \bigotimes b$ with $a \leq b$.

To build a $\bigotimes$-product proceed as follows.

Step 1. Fix the atoms, which are written in the Table N, and set n equal to 2.

Step 2. Associate a result k to $2 \bigotimes n$. The number k is selected by picking a number from the Table N so that the rows and the columns of the Table T remain increasing sequences (according to property (P3)).

Step 3. The same number k must be the result of all the expressions equivalent to $2 \bigotimes n$ with respect to the associative and the commutative properties. Fill the corresponding entries in the Tables T and N.

Step 4. Increase n by 1 and go back to Step 2.

For example, let $a = 2$ and $b = 4$ be the atoms. Then a and b are inserted in the Table N: see Table 1 and Table 2 (where the atoms are in boldface).

Let us set $2 \bigotimes 2 = 3$, and thus $\underline{a}^2 = 3$. Then we set $2 \bigotimes 3 = 5$ (which gives $\underline{a}^3 = 5$) and $2 \bigotimes 4 = 6$ ($a \bigotimes b = 6$). Next $2 \bigotimes 5 = 7$, so $a \bigotimes \underline{a}^3 = 7$; but $a \bigotimes \underline{a}^3 = \underline{a}^2 \bigotimes \underline{a}^2$ and therefore also $3 \bigotimes 3 = 7$. In the same way we obtain $2 \bigotimes 6 = 3 \bigotimes 4 = 8$, since $a \bigotimes (a \bigotimes b) = \underline{a}^2 \bigotimes b$, and $2 \bigotimes 7 = 3 \bigotimes 5 = 9$ by $a \bigotimes \underline{a}^4 = \underline{a}^2 \bigotimes \underline{a}^3$. For the next step we have $2 \bigotimes 8 = 3 \bigotimes 6 = 5 \bigotimes 4$ because $a \bigotimes (\underline{a}^2 \bigotimes b) = \underline{a}^2 \bigotimes (a \bigotimes b) = \underline{a}^3 \bigotimes b$. But the entry $4 \bigotimes 4$ (which corresponds to $\underline{b}^2$) still does not have a value. So, to respect property (P3), we set $4 \bigotimes 4 = 10$ and $2 \bigotimes 8 = 11$.

Then the process begins again associating a value to $2 \bigotimes 9$.

$\boldsymbol{T}$	2	3	4	5	6	7	8	9	10	…
2	3	5	6	7	8	9	11	12	13	…
3		7	8	9	11	12	…	…	…	…
4			10	11	13	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…

Table 1 T gives the results of the $\bigotimes$-product

$\boldsymbol{N}$	2	3	4	5	6	7	8	9	10	11	…
	$\boldsymbol{a}$	$\underline{a}^2$	$\boldsymbol{b}$	$\underline{a}^3$	$a \bigotimes b$	$\underline{a}^4$	$\underline{a}^2 \bigotimes b$	$\underline{a}^5$	$\underline{b}^2$	$\underline{a}^3 \bigotimes b$	…

Table 2 N represents each natural number as a $\bigotimes$-product of atoms

Some remarks.

1. The operation (partially) described in Table 1 and Table 2 is a $\bigotimes$-product and the corresponding monoid is factorial.
2. Different $\bigotimes$-products can have the same atoms. In fact, if we exchange two numbers in the Table T (maintaining the rows and the columns increasing) we obtain a new operation. For example, exchanging 9 with 10 we get another $\bigotimes$-product such that $\underline{a}^5 = 10$ and $\underline{b}^2 = 9$.

3. The limit $\lim_{n\to\infty} \log_n \underline{2}^n < \lim_{n\to\infty} \log_n (n+1)^2$ is finite (because each element less than $\underline{a}^n$ has a factorization $\underline{a}^r \bigotimes \underline{b}^s$ with $r, s < n$). This confirms that the monoid has a finite number of atoms (see Theorem 6).
4. As observed, the above $\bigotimes$-product respects the fundamental theorem of arithmetic. Otherwise the theorem does not hold if, for example, we set $2 \bigotimes 3 = 2 \bigotimes 4 = 5$ (the new operation is described in Tables 3 and 4). Notice that in any case the sequence $\underline{a}^n$ is strictly monotone for every atom a (because $\underline{a}^n = \underline{a}^m$ and $n > m$ would imply $\underline{a}^{n-m} = 1$, by the cancelation law).

T	2	3	4	5	6	7	8	9	10	11	…
2	3	5	5	6	8	8	9	11	11	12	…
3		6	6	8	9	9	11	12	12	…	…
4			7	8	9	10	11	12	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…

Table 3 The fundamental theorem of arithmetic does not hold

N	2	3	4	5	6	7	8	9	10	…
	a	$\underline{a}^2$	***b***	$\underline{a}^3$	$\underline{a}^4$	$\underline{b}^2$	$\underline{a}^5$	$\underline{a}^6$	$\underline{b}^3$	…
				$a \bigotimes b$	$\underline{a}^2 \bigotimes b$		$\underline{a}^3 \bigotimes b$	$\underline{a}^4 \bigotimes b$		…
				…	…	…	…	…	…	…

Table 4 Same numbers may have more distinct factorizations

For any integer $k > 1$ we can define a $\bigotimes$-product with atoms $2, 3, \ldots, k-1$ and setting $2 \bigotimes 2 = k$. Therefore all these operations have different operation-tables T and so they are distinct. Still, a $\bigotimes$-product satisfies the fundamental theorem of arithmetic (that is $\left(\mathbb{N}, \bigotimes\right)$ is factorial) if in the Table N different expressions are always associated to distinct numbers. This occurs if we always choose different results for different expressions $2 \bigotimes n$, and therefore the rows and the columns of T are *strictly* increasing sequences.

Summarizing we have the following.

Proposition 3. *There exist infinitely many factorial monoids* $\left(\mathbb{N}, \bigotimes\right)$.

4 When are there infinitely many atoms?

Fixed a $\bigotimes$-product, to establish if the corresponding monoid has infinitely many atoms we just need to evaluate a limit.

We will denote by $|X|$ the cardinality of the set X and by $[a, b]$ the natural numbers $\geq a$ and $\leq b$.

Theorem 4. *If* $\lim_{n\to\infty} \log_n \underline{2}^n = \infty$, *then* $\left(\mathbb{N}, \bigotimes\right)$ *contains infinitely many atoms.*

Proof. Let $A = \{n \in \mathbb{N} : n > 1\}$. It suffices to show that no finite subset $B = \{b_1, b_2, \ldots, b_r\}$ of A can generate A, that is $A \setminus \langle B\rangle \neq \emptyset$ if $\langle B\rangle$ denotes the infinite set of all the products of elements in B, that is

$$\langle B\rangle = \{\underline{b_1}^{\alpha_1} \bigotimes \cdots \bigotimes \underline{b_r}^{\alpha_r} : \alpha_i \geq 0\ \forall i, \alpha_j > 0\ \exists j\}.$$

For any positive integer m let us consider the powers with bounded exponent, so let

$$B_m = \{\underline{b_1}^{\alpha_1} \bigotimes \cdots \bigotimes \underline{b_r}^{\alpha_r} : 0 \leq \alpha_i \leq m\ \forall i, \alpha_j > 0\ \exists j\}$$

and set $m_k = \max\{n \in \mathbb{N} : \underline{2}^n \leq 10^k\}$. Then

$$\langle B\rangle \bigcap [2, 10^k] = B_{m_k} \bigcap [2, 10^k]$$

for every positive k. Indeed $B_{m_k} \subseteq \langle B\rangle$, $\underline{b}^{m_k+1} \geq \underline{2}^{m_k+1} > 10^k$ for each $b \in B$, and according to property (P3).

The claim is proved if $\lim_{k\to\infty} \log_{m_k} 10^k = \infty$. In fact, in this case, for any positive integer r there exists a $\overline{k}$ such that $2(m_k + 1)^r < m_k^{2r} < 10^k$ when $k > \overline{k}$, because $m_k \to \infty$ as $k \to \infty$. So $\left|B_{m_k}\right| \leq (m_k+1)^r < \frac{10^k}{2} < \left|[2, 10^k]\right|$ and $[2, 10^k] \setminus \langle B\rangle = [2, 10^k] \setminus B_{m_k} \neq \emptyset$, that is $A \setminus \langle B\rangle \neq \emptyset$.

What remains is to verify that $\lim_{k\to\infty} \log_{m_k} 10^k = \infty$.

If $\lim_{n\to\infty} \log_n \underline{2}^n = \infty$, then $\lim_{m_k\to\infty} \log_{m_k} \underline{2}^{m_k} = \infty$ and therefore $\lim_{k\to\infty} \log_{m_k} 10^k = \infty$ (because $\lim_{k\to\infty} m_k = \infty$ and $\underline{2}^{m_k} \leq 10^k$). □

Corollary 5 (Euclid's theorem)**.** *The usual product has infinitely many primes.*

Proof. In fact $\lim_{n\to\infty} \log_n 2^n = \infty$. □

The sufficient condition of Theorem 4 is also necessary if the fundamental theorem of arithmetic holds.

Theorem 6. *If the monoid* $\left(\mathbb{N}, \bigotimes\right)$ *is factorial and contains infinitely many atoms, then*

$$\lim_{n\to\infty} \log_n \underline{2}^n = \infty.$$

Proof. Let $p_1, p_2, \ldots, p_m$ be pairwise distinct atoms. If $p_i < \underline{2}^{n_i}$ for every i, then $\underline{p_1}^{\alpha} \bigotimes \underline{p_2}^{\alpha} \bigotimes \ldots \bigotimes \underline{p_m}^{\alpha} < \underline{2}^{\alpha u}$ when α is any positive integer and $u = \sum_{i=1}^m n_i$. Applying the fundamental theorem of arithmetic and the property (P3), we see that $\alpha^m < \underline{2}^{\alpha u}$. So $\log_{\alpha u} \underline{2}^{\alpha u} > \log_{\alpha u} \alpha^m = \frac{m}{1+\log_\alpha u}$, and setting $\alpha = u$ we get $\log_{u^2} \underline{2}^{u^2} > \frac{m}{2}$ for each m. This completes the proof because the sequence $\{\underline{2}^n\}$ is a strictly increasing sequence (it is seen by induction and applying property (P3)). □

References

[1] M. Aigner and G.M. Ziegler, *Proofs from THE BOOK* (third ed.), Springer-Verlag, 2000, pp. 3–6.

[2] H. Davenport, *The Higher Arithmetic* (seventh ed.), Cambridge Univ.Press, 1999.

[3] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations*, Chapman & Hall/CRC, 2006.

[4] F. Saidak, *A New Proof of Euclid's Theorem*, Amer. Math. Monthly, **113** (2006), pp. 937–938.

Alberto Zorzi
Università IUAV di Venezia
Tolentini S. Croce 191
I-30135 Venezia, Italy
e-mail: zorzi@iuav.it