The Divisors of Natural Numbers introduced as the Fixed Points of the Euclidean Algorithm on the Tower of Initial Segments

Peter H. N. Luschny

21. Juni 2025

"La rigueur n'a jamais eu pour objet que de sanctionner et de légitimer les conquêtes de l'intuition." – Jacques Hadamard

0.1 THE CONTEXT FROM A BIRD'S EYE VIEW

The concept of divisibility and divisors can be understood in various ways, even at the elementary level. One can consider the natural numbers from different perspectives, such as:

- (1) treating them as a commutative semiring,
- (2) examining them through a lattice-theoretical perspective,
- (3) or analyzing them from a more general algebraic viewpoint.

In this discussion, we will focus solely on the first framework. However, we will place our considerations within a context we refer to as the *Tower of Initial Segments*, which, unlike traditional conceptualizations, consistently results in a finite set of divisors.

0.2 ABSTRACT

We advocate the introduction of the concept of a divisor of a nonnegative integer n, wherein the defining condition

$$k \textit{ is a divisor of } n \iff \textit{there exists } m \in \mathbb{U} \textit{ such that } m \cdot k = n,$$

the domain $\mathbb{U}$ is not selected to be $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, but rather the initial segment of the natural numbers, denoted as $\overline{n} = \{0, 1, 2, 3, \ldots, n\}$.

The intuitive idea we are pursuing views natural numbers less as a fixed structure and more as a process of expansion that builds the triangle of the initial segments $\overline{n}$ starting with $\overline{0}$, where at each step, the divisors can be defined and characterized by a fixed point theorem based on the greatest common divisor. This concept is constructively realized through the Euclidean algorithm.

As a result, we can conclude that the set of divisors of a nonnegative number is always finite. This proposition is not only intuitively satisfying but also well-suited for application in algebraic computing programs. However, this conclusion cannot be drawn when using the standard definition with $\mathbb{U} = \mathbb{N}$.

0.3 DIVISIBILITY OF NATURAL NUMBERS

Let's start with an error message displayed by the computer algebra program Maple when asked about the divisors of 0: *"Error: Divisors cannot represent all positive divisors of* 0.*"*

If you are not familiar with the formal definition of the term 'divisor,' this error message might be surprising. After all, the sequence of divisors $T(n)$ for $n \geqslant 1$ begins like this:

```
T(1) = {1};          T(2) = {1, 2};    T(3) = {1, 3};
T(4) = {1, 2, 4};    T(5) = {1, 5};    T(6) = {1, 2, 3, 6};
```

Trivially, 0 divides 0 (no division operation is involved here). Therefore, one might reasonably expect that the divisors of 0 could be represented by the set $\{0\}$.

This paper aims to demonstrate that this interpretation can be supported with formal reasoning, and it will provide the necessary definitions. Central to this discussion is a variant of the Euclidean algorithm, which we will present as an operation

$$\beta : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

whose initial values are given in the following table.

```
n\k [0, 1, 2, 3, 4, 5, 6, 7, 8, 9,10, ...
----------------------------------------
[0] [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, ...
[1] [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, ...
[2] [2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, ...
[3] [3, 1, 1, 3, 1, 1, 3, 1, 1, 3, 1, ...
[4] [4, 1, 2, 1, 4, 1, 2, 1, 4, 1, 2, ...
[5] [5, 1, 1, 1, 1, 5, 1, 1, 1, 1, 5, ...
[6] [6, 1, 2, 3, 2, 1, 6, 1, 2, 3, 2, ...
[7] [7, 1, 1, 1, 1, 1, 1, 7, 1, 1, 1, ...
...
```

Before we define the function β, let us first consider some consequences that follow from it. The set $D = \{\beta(n, k) : k \geqslant 0\}$ is a subset of $\overline{n} = \{0, 1, 2, \ldots, n\}$, and it has the property that for every $d \in D$, there exists a $d' \in D$ such that $d \cdot d' = n$. Therefore, D can be legitimately called the *set of divisors of* n.

In the case where $n = 0$, we have $T(0) = D = \{\beta(0,0)\} = \{0\}$, which is as expected. However, this definition does not align with the standard definitions found in number theory textbooks. According to those definitions, carefully stated for non-negative integers n, d, and m:

$$d \in T(n) \iff \exists m : m \cdot d = n.$$

When $n = 0$, this condition leads to an infinite set $T(n)$ because *all* integers $d \geqslant 0$ satisfy it if we choose $m = 0$.

In our definition

$$d \in T(n) \iff d \in \{\beta(n,k) : k \geqslant 0\}$$

there is no existential quantifier that enforces such a result.

Notably, we can restrict the range of the definition to a subset of the domain of β—specifically, to the indices of the lower triangle of the value matrix—without affecting the resulting set:

$$d \in T(n) \iff d \in \{\beta(n,k) : 0 \leqslant k \leqslant n\}.$$

Using two fundamental properties of the greatest common divisor,

$$\gcd(n,k) = \gcd(n, n-k) \;\text{ and }\; \gcd(n,k) \leqslant k \text{ for } k > 0,$$

we can refine this equivalence to

$$d \in T(n) \iff d = \beta(n,d) \text{ and } d \in \bar{n}.$$

This can be expressed more memorably as:

> *The divisors of n are the fixed points of the function $x \to \beta(n,x)$ on the initial segment of the natural numbers.*

Consequently, the question *"Is d a divisor of n?"* is decided by the computability of β. But this is ensured because β serves as an embodiment of the Euclidean algorithm, as we will demonstrate. This relationship provides not only a constructive approach but also an efficient method for calculating the divisors, particularly in the binary form of the algorithm, that dates back to Josef Stein and is described below.

0.4 THE EUCLIDEAN BETA FUNCTION

The universe of our discourse consists of the nonnegative integers, which we will refer to as natural numbers, denoted as:

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

For any natural number n, we define:

$$\begin{aligned} \bar{n} &= \{0, 1, 2, 3, \dots, n\}, \quad \text{and} \\ \Delta_{\mathbb{N}} &= \{\bar{n} : n \in \mathbb{N}\}. \end{aligned}$$

Our goal is to define the concepts of divisors of n, primes of n, and the largest common divisor. To achieve this, we introduce a function β defined on $\mathbb{N} \times \mathbb{N}$ and establish the following notations and terminology:

$$\begin{array}{lcl|l} k \mid n & \Longleftrightarrow & \beta(n,k) = k & k \text{ divides } n; \\ k \perp n & \Longleftrightarrow & \beta(n,k) = 1 & k \text{ prime to } n; \\ k \wedge n & \Longleftrightarrow & \gcd(n,k) & \end{array}$$

The notation $k \mid n$ was introduced by Landau, while Graham, Knuth, and Patashnik suggested the notation $k \perp n$. The notation $k \wedge n$ is reminiscent of the representation of the greatest common divisor (gcd) as the intersection of multisets.

We have named the function *beta*, which stands for the *binary Euclidean divisor algorithm*. This function is defined as an operation

$$\beta : \mathbb{N} \times \mathbb{N} \to \mathbb{N}.$$

This operation can also be represented as a family of partial functions retaining the name and writing the first argument as a suffix, so

$$\begin{aligned} &\beta_n : \ \mathbb{N} \to \mathbb{N}, \\ &\beta_n(k) \mapsto \beta(n,k). \end{aligned}$$

When calculating this function, neither division nor the modulo operation (i.e., the remainder of integer division) is used.

0.5 IMPLEMENTATION OF THE BETA FUNCTION

To simplify things, we first introduce two auxiliary functions. The values of these two functions are also listed in the OEIS.

- A007814, the ruler sequence, or the 2-adic valuation of n.

```
ord : N \ {0} -> N \ {0},
ord(n) is the largest power of 2 that divides n.
ord: (1,2,3,4,5,6,7,8, ..) maps to (0,1,0,2,0,1,0,3, ..)
```

- A000265, the odd part of n.

```
odd : N \ {0} -> N \ {0},
odd(n) = n / 2^ord(n).
odd: (1,2,3,4,5,6,7,8, ..) maps to (1,1,3,1,5,3,7,1, ..)
```

One often writes $n \gg \mathrm{ord}(n)$ for $n/2^{\mathrm{ord}(n)}$ in programming languages. This translates to shifting the binary representation of n by $\mathrm{ord}(n)$ places to the right. We will also use this notation in the following functions written in Python.

```python
def odd(n: int) -> int:
    if n < 0: n = -n
    while not n & 1: n >>= 1
    return n

def ord(n: int) -> int:
    return (n & -n).bit_length() - 1

def beta(n: int, k: int) -> int:
    if k == 0 or n == 0: return n
    a = odd(k)
    b = odd(n)
    while a != b:
        t = b - a
        if a < b:
            b = a
        a = odd(t)
    return a << ord(n|k)
```

```
def Divisors(n: int) -> list[int]:
    return [k for k in range(n + 1) if beta(n, k) == k]

def Primes(n: int) -> list[int]:
    return [k for k in range(n + 1) if beta(n, k) == 1]

def divides(k: int, n: int) -> bool:
    return beta(n, k) == k

def isprime(n: int) -> bool:
    return (n > 1 and
            not any(k for k in range(2, n) if beta(n, k) != 1))

def Codivisors(n: int) -> list[tuple[int, int]]:
    D = Divisors(n)
    return [(D[k], D[-k-1]) for k in range(len(D))]
```

0.6 NUMBERS PRIME TO N

The main function $\beta(n,k)$ introduced above are registered in the OEIS as

- A384447, $\beta(n,k) = \gcd(n,k)$ if $n > 0$ otherwise 0.
- A109004, $\gcd(n,k)$ for $n \geqslant 0, k \geqslant 0$.

For arguments $0 \leqslant k \leqslant n$ the function A384447 is identical to A109004.

In addition to the relation *k divides n*, we also introduce the relation *k is prime to n*, following a suggestion of Donald Knuth. Alternatively, one may refer to this relation as *k is relatively prime to n* or *k is coprime to n*.

In this case we refer to the generating function as *primes of*, replacing the defining condition $\beta(n,k) = k$ with the condition $\beta(n,k) = 1$.

So we now have two functions: the *divisors of* n and the *primes of* n, which return lists of integers. They can be looked up in the OEIS at

- A027750, row n lists the divisors of n;
- A038566, for $n \geqslant 2$.

The lists of divisors of n $[\beta(n,k) = k]$ and primes of n $[\beta(n,k) = 1]$ begin:

```
         A027750              A038566
|  n |  Divisors of ...     | Primes of ...          |
|  0 |  [0]                 | []                     |
|  1 |  [1]                 | [0, 1]                 |
|  2 |  [1, 2]              | [1]                    |
|  3 |  [1, 3]              | [1, 2]                 |
|  4 |  [1, 2, 4]           | [1, 3]                 |
|  5 |  [1, 5]              | [1, 2, 3, 4]           |
|  6 |  [1, 2, 3, 6]        | [1, 5]                 |
|  7 |  [1, 7]              | [1, 2, 3, 4, 5, 6]     |
|  8 |  [1, 2, 4, 8]        | [1, 3, 5, 7]           |
|  9 |  [1, 3, 9]           | [1, 2, 4, 5, 7, 8]     |
| 10 |  [1, 2, 5, 10]       | [1, 3, 7, 9]           |
```

The corresponding counting functions are A000005 and A384710.

0.7 THE TOWER OF THE INITIAL SECTIONS

As introduced, the definition of a divisor can be expressed as follows:

$$k \text{ divides } n \iff k \text{ is a divisor of } n \iff k \text{ is a fixed point of } \beta_n.$$

In our notation, Python's range$(n + 1)$ is $\bar{n}$ and represents the initial segment of the natural numbers up to and including n, as given in A002262. The function 'Divisors' is defined as follows:

$$\text{Divisors} : n \mapsto D_n = \{k \in \bar{n} : \beta(n,k) = k\} \subseteq \bar{n}.$$

This function assigns to each n the fixed points of β_n. It is important to note that D_n is always non-empty; equality $\bar{n} = D_n$ occurs only in the case when $n = 0$. Furthermore, the set of divisors D_n is closed under the iteration of the *Divisors* function, which means:

$$\text{Divisors}(n) = \bigcup_{d \in \text{Divisors}(n)} \text{Divisors}(d).$$

The foundation of our considerations is the tower of the initial sections $\Delta_{\mathbb{N}} = \{(n,k) : 0 \leqslant k \leqslant n\}$ of the natural numbers, given in A002262.

Since all relevant information of β is already encoded in the values of this number triangle, we can interpret the function β as a line-by-line transformation from A002262 to A109004.

```
        A002262          =>          A109004
-------------------------------------------------
[ 0]                        [ 0]
[ 0, 1]                     [ 1, 1]
[ 0, 1, 2]                  [ 2, 1, 2]
[ 0, 1, 2, 3]               [ 3, 1, 1, 3]
[ 0, 1, 2, 3, 4]            [ 4, 1, 2, 1, 4]
[ 0, 1, 2, 3, 4, 5]         [ 5, 1, 1, 1, 1, 5]
[ 0, 1, 2, 3, 4, 5, 6]      [ 6, 1, 2, 3, 2, 1, 6]
...
```

This allows us to construct both triangles row by row at the same time.

0.8 EXISTENCE AND INTUITION

The transformation presented in the previous table aligns with our intuition. On the left side, the natural numbers are constructed as a sequence of progressively expanding initial sections of $\mathbb{N}$, a concept that is intuitively understood from the axiomatizations of natural numbers. At the same time, the divisors of n are introduced on the right side as the values of this transformation.

This entire process embodies the approach that constructive mathematicians propose for introducing concepts. The fact that this process arises, more or less directly, from the Euclidean algorithm further reinforces the intuitive validity of this representation.

It is quite challenging to understand how one can arrive at a formalization that produces an infinite set at the very beginning of the above construction. In any case, I regard the standard formalization as a failure and prefer to follow the advice:

> *"The sole purpose of rigor has always been to sanction and legitimize the conquests of intuition."* – Jacques Hadamard

0.9 THE NUMBER OF DIVISORS IS FINITE

Theorem For all n in $\mathbb{N}$: The set of divisors of n is finite.

To prove this, we note that only numbers $\leqslant n$ can appear in row n of the value matrix of β. This implies that any fixed points, if they exist (in fact, at least one always does), must lie within the index range 0 to n. In other words, the divisors of n are located in the initial segment of a row, which means they appear to the left of or on the main diagonal of the value matrix.

Again we emphasize that this theorem does *not* align with the conventional textbook definition. Nonetheless, its validity holds in the our constructive setup, it has practical significance, and it is fundamentally rooted in intuition.

0.10 SUMMARY

At no point in the discussion of the concepts of divisibility, coprimality, divisors, codivisors, and the greatest common divisor, we found it necessary or advantageous to generate infinite sets.

The fact that the usual definition of 'divisor' leads to the conclusion that the divisors of zero form an infinite set strikes us as a strange artifact of a failed formalization. Not only does the usual conceptualization contradict the theoretical requirement for straightforward concepts, but it also proves to be highly impractical for applications in algebraic computing programs, as illustrated by the error message from Maple mentioned earlier.

This observation suggests that the standard definition was initially not intended for $n = 0$. Typically, arithmetic functions are defined only for $n \geqslant 1$, and in this range, both definitions are equivalent. However, if we wish to extend the definition to a larger domain, we must ensure that core properties, such as the finiteness of the set of divisors, are preserved.

A technical discussion of the binary Euclidean algorithm is in BinaryGcd. An outline of some more advanced parts of the theory based on the tower of initial segments can be found in MoebiusCompanion and in A382883.

0.11 POSTSCRIPT

There is a saying in computer science that succinctly states, “Garbage in, garbage out.“ This means that flawed information as input will lead to problematic or incorrect results.

This insight is also relevant in other formal contexts, such as mathematics. In mathematics, ‘input‘ refers, in particular, to definitions and the formulation of assumptions. The above considerations are an example of the former.

A pitfall of the latter type was reported by Loeffler and Stoll [1], who overlooked an assumption in a corner case while formalizing the Riemann Hypothesis in the context of Lean. They warn:

> *"Mistakes in formalizing the statements of conjectures might lead to mathematicians believing that a conjecture had been proved (or disproved), when in fact* [...] *an oversight in formulating the conjecture in some mathematically uninteresting corner case [has been proved]."*

What both cases illustrate is that the validity of a statement is established long before the formal proof, and that marginal cases, which are often not given enough attention, can play a crucial role.

1 David Loeffler and Michael Stoll, Formalizing zeta and L-functions in Lean.