Natural numbers and prime numbers: a conjecture

Arnaud Mayeux

Natural numbers and prime numbers: a conjecture

May 5, 2020

Arnaud Mayeux

Abstract: We state a conjecture about natural and prime numbers. Let $\mathbb{I} = \{1, 2, 3, 4, 5, 6, 7, \ldots\}$ be the set of non zero natural integers. We first define a class of functions $\mathbb{I} \to \mathbb{I}$ called the natural functions, they are built using addition, multiplication and elevation. Such functions are strictly increasing if they are not constant. We conjecture that for every non constant natural function f, we have $f(\mathbb{I}) \not\subset \mathbb{P}$ where $\mathbb{P} \subset \mathbb{I}$ is the set of prime numbers. This conjecture, if it is true, generalizes a result of Euler about Fermat's numbers.

Contents

Introduction

Fermat [3] conjectured that $\{2^{2^n} + 1 \mid n \text{ positive integers}\} \subset \mathbb{P}$. Euler [1] [2] proved that this is wrong, i.e. $\{2^{2^n} + 1 \mid n \text{ positive integers}\} \not\subset \mathbb{P}$. We say that a function $f : \mathbb{I} \to \mathbb{I}$ with variable n is a natural function if it is built using formal (and coherent) combinations of the symbols $n, \{a \in \mathbb{I}\}, +, \times, \wedge$. Here $\wedge$ means elevation to the power. We prove that every natural function is constant or strictly increasing. We then conjecture that for every natural function f, we have $f(\mathbb{I}) \not\subset \mathbb{P}$. This conjecture generalizes Euler's result, since $n \mapsto 2^{2^n} + 1 = 2 \wedge (2 \wedge n) + 1$ is a natural function. In this text we formally introduce notation and definitions. Then we state our conjecture and prove it in some cases. We also discuss implications of our conjecture.

1 Notation and definition

Let

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, \dots\}$$

be the set of positive integers. Let

$$\mathbb{I} = \{1, 2, 3, 4, 5, 6, 7, \dots\}$$

be the set of non zero positive integers. Let

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$$

be the set of prime numbers. Let $\mathcal{F}(\mathbb{I}, \mathbb{I})$ be the set of functions from $\mathbb{I}$ to $\mathbb{I}$.

Definition 1.1. *An elevation structure is a 4-uple $(E, +, \times, \wedge)$ where E is a set and*

1. *$+$ is a map $E \times E \to E$ sending a, b to $a + b$*
2. *$\times$ is a map $E \times E \to E$ sending a, b to $a \times b$*
3. *$\wedge$ is a map $E \times E \to E$ sending a, b to $a \wedge b$*

such that $\forall\ a, b, c \in E$ the following hold

1. $a + b = b + a$
2. $a + (b + c) = (a + b) + c$
3. $b \times a = a \times b$
4. $a \times (b \times c) = (a \times b) \times c$
5. $a \times (b + c) = a \times b + a \times c$
6. $(a \wedge b) \times (a \wedge c) = a \wedge (b + c)$
7. $(a \wedge b) \wedge c = a \wedge (b \times c)$.

We write $a_1 \wedge a_2 \wedge \dots \wedge a_n$ instead of $a_1 \wedge (a_2 \wedge (\dots \wedge a_n))$, be careful that $a \wedge (b \wedge c) \neq (a \wedge b) \wedge c$ in general. We write often $a_1^{a_2^{\cdot^{\cdot^{\cdot^{a_n}}}}}$ instead of $a_1 \wedge a_2 \wedge \dots \wedge a_n$. For example a^{b^c} means $a \wedge (b \wedge c)$.

A morphism of elevation structure from $(E, +, \times, \wedge)$ to $(F, +, \times, \wedge)$ is a map $M : E \to F$ such that $\forall\ a, b \in E$, we have $M(a + b) = M(a) + M(b)$, $M(a \times b) = M(a) \times M(b)$ and $M(a \wedge b) = M(a) \wedge M(b)$. We obtain a category.

Example 1.2.

1. $\mathbb{N}, +, \times, \wedge$ *is an elevation structure with* $a \wedge b := a^b$.

2. $\mathbb{I}, +, \times, \wedge$ *is an elevation structure.*

3. $\mathcal{F}(\mathbb{I}, \mathbb{I}), +, \times, \wedge$ *is an elevation structure with* $(f \wedge g)(n) := f(n) \wedge g(n)$.

4. *Let* $a \in \mathbb{I}$*, then the evaluation map* $E_a : \mathcal{F}(\mathbb{I}, \mathbb{I}) \to \mathbb{I}$*,* $f \mapsto f(a)$*, is a morphism of elevation structure from* $\mathcal{F}(\mathbb{I}, \mathbb{I}), +, \times, \wedge$ *to* $\mathbb{I}, +, \times, \wedge$.

Let $P\Big(\mathcal{F}(\mathbb{I}, \mathbb{I})\Big)$ be the set of all parts of $\mathcal{F}(\mathbb{I}, \mathbb{I})$. Let $\mathcal{F}_s \in P\Big(\mathcal{F}(\mathbb{I}, \mathbb{I})\Big)$ be the part of functions constitued of the identity map $n \mapsto n$ and the constant maps $n \mapsto a$ for every $a \in \mathbb{I}$, we also call it the part of symbols.

We now define some operators on $P\Big(\mathcal{F}(\mathbb{I}, \mathbb{I})\Big)$.

Definition 1.3.

1. *Let* A_+ *be the map sending* $P \in P\Big(\mathcal{F}(\mathbb{I}, \mathbb{I})\Big)$ *to*

$$P \cup \{f \in \mathcal{F}(\mathbb{I}, \mathbb{I}) \mid \exists g \in P, \exists h \in P \text{ and } f = g + h\}.$$

2. *Let* $A_\times$ *be the map sending* $P \in P\Big(\mathcal{F}(\mathbb{I}, \mathbb{I})\Big)$ *to*

$$P \cup \{f \in \mathcal{F}(\mathbb{I}, \mathbb{I}) \mid \exists g \in P, \exists h \in P \text{ and } f = g \times h\}.$$

3. *Let* $A_\wedge$ *be the map sending* $P \in P\Big(\mathcal{F}(\mathbb{I}, \mathbb{I})\Big)$ *to*

$$P \cup \{f \in \mathcal{F}(\mathbb{I}, \mathbb{I}) \mid \exists g \in P, \exists h \in P \text{ and } f = g \wedge h\}.$$

We are now able to define the set of natural functions $\mathcal{F}_{Natural}$. Let Σ be the set of all finite words with letters $A_+, A_\times, A_\wedge$.

Definition 1.4. *We put* $\mathcal{F}_{Natural} = \bigcup_{\sigma \in \Sigma} \sigma(\mathcal{F}_s) \in P\Big(\mathcal{F}(\mathbb{I}, \mathbb{I})\Big)$*. The 4-uple* $\mathcal{F}_{Natural}, +, \times, \wedge$ *is an elevation structure.*

Example 1.5.

1. $\mathcal{F}_s \subset \mathcal{F}_{Natural}$

2. *The set of polynomial functions on* $\mathbb{I}$ $\mathcal{F}_{Polynomial}$ *is contained in* $\mathcal{F}_{Natural}$*. More precisely it is contained in* $\bigcup_{j,k \geq 0} A_+^j A_\times^k(\mathcal{F}_s)$.

3. *Fermat's function* $n \mapsto 2^{2^n} + 1$ *is contained in* $\mathcal{F}_{Natural}$*. More precisely it is contained in* $A_+ A_\wedge^2(\mathcal{F}_s)$.

4. The functions

$$n \mapsto n^n + n + 1$$
$$n \mapsto 7^n + 6$$
$$n \mapsto n^{4n^n + n^{23} + 2^n + 8} + n + 3$$
$$n \mapsto 2^{2^{2^{2^{2^n}}}} + 1$$

are natural functions.

Proposition 1.6. *A natural function $f \in \mathcal{F}_{natural}$ is constant or strictly increasing.*

Proof. By definition a function f is in $\mathcal{F}_{natural}$ is and only if there exists a finite word σ in letters $A_+, A_\times, A_\wedge$ such that $f \in \sigma(\mathcal{F}_s)$. We need the following definition.

Definition 1.7. *The length of a natural function $f \in \mathcal{F}_{Natural}$ is the number*

$$\min\{n \in \mathbb{N} \mid f \in \sigma(\mathcal{F}_s) \text{ with } \sigma \text{ a word of length } n\},$$

it is well defined.

Let us prove our result by induction on length. Consider the following assertion.

P_n : *Proposition 1.6 is true for every $f \in \mathcal{F}_{Natural}$ of length $\leq n$.*

Let us prove by induction that P_n is true for every $n \in \mathbb{N}$. We need the following Lemmas.

Lemma 1.8. *Let $h, g \in \mathcal{F}_{Natural}$ be strictly increasing, then $h + g, h \times g, h \wedge g$ are strictly increasing.*

Proof. Let $i > j$ be integers in $\mathbb{I}$, then $h(i) > h(j)$ and $g(i) > g(j)$. So $h(i) + g(i) > h(j) + g(j)$, consequently $h + g$ is strictly increasing. Since $g(i) > g(j) \geq 1$ and $h(i) > h(j) \geq 1$; we have $h(i) \times g(i) > h(j) \times g(j)$ and consequently $h \times g$ is strictly increasing; we also have $h(i)^{g(i)} > h(j)^{g(j)}$ and consequently $h \wedge g$ is strictly increasing. □

Lemma 1.9. *Let $h \in \mathcal{F}_{Natural}$ be strictly increasing and $g \in \mathcal{F}_{Natural}$ be constant, then $h + g, h \times g, h \wedge g$ are strictly increasing.*

Proof. Let $i > j$ be integers in $\mathbb{I}$, then $h(i) > h(j)$ and $g(i) = g(j)$. So $h(i) + g(i) > h(j) + g(j)$, consequently $h + g$ is strictly increasing. Since $g(i) = g(j) \geq 1$ and $h(i) > h(j)$, we have $h(i) \times g(i) > h(j) \times g(j)$ and consequently $h \times g$ is strictly increasing. We have $h(i)^{g(i)} > h(j)^{g(j)}$ and consequently $h \wedge g$ is strictly increasing. □

Lemma 1.10. *Let $h \in \mathcal{F}_{Natural}$ be strictly increasing and $g \in \mathcal{F}_{Natural}$ be constant, then $g \wedge h$ is strictly increasing except if $g = 1$. If $g = 1$, $g \wedge h$ is constant.*

Proof. Let $i > j$ be integers in $\mathbb{I}$. If $g = 1$ then $g(i)^{h(i)} = g(j)^{h(j)} = 1$ and $g \wedge h$ is constant. In the other case $g(i) = g(j) > 1$ and $h(i) > h(j)$, consequently $g(i)^{h(i)} > g(j)^{h(j)}$. This ends the proof. □

Now let us start our induction. If $n = 0$, then f is constant or the identity map and thus satisfies P_0. Now assume that P_n is true and let us prove that P_{n+1} is true. Let f of length $n+1$. By definition, there are h, g of length $\leq n$ such that $f = h + g$ or $f = h \times g$ or $f = g \wedge h$ or $f = h \wedge g$. By induction hypothesis h and g are constant or strictly increasing. Assume first both are constant. Then f is obviously constant. If both are strictly increasing, then f is strictly increasing by Lemma 1.8. If h is strictly increasing and g is constant, then by Lemma 1.9, $h+g$, $h \times g$ and $h \wedge g$ are strictly increasing, and by Lemma 1.10, $g \wedge h$ is strictly increasing or constant. If h is constant and g is strictly increasing, we deduce, in the same way, that $h + g$, $h \times g$, $h \wedge g$ and $g \wedge h$ are strictly increasing or constant. Consequently, f is constant or strictly increasing. This ends the induction and the proof of Proposition. □

Remark 1.11. *The map $\mathbb{N} \to \mathbb{N}$, $n \mapsto n^n$ is neither constant nor strictly increasing since $0^0 = 1^1 \neq 2^2$. Its restriction to $\mathbb{I}$ is a strictly increasing natural function.*

2 Statement of the conjecture and proof of it in some cases

2.1 Statement

We now state our conjecture.

Conjecture 2.1. *Let $f \in \mathcal{F}_{Natural}$ be a non constant natural function. Then*

$$f(\mathbb{I}) \not\subset \mathbb{P}.$$

Proposition 2.2. *Conjecture 2.1 is true in the following cases.*

1. *Let $f \in \mathcal{F}_{Polynomial}$, assume f is non constant, then $f(\mathbb{I}) \not\subset \mathbb{P}$.*

2. *Let $a \in \mathbb{I}_{>1}$, $b \in \mathbb{N}$ and f be $n \mapsto a^n + b$, then $f(\mathbb{I}) \not\subset \mathbb{P}$.*

3. *Let f be $n \mapsto 2^{2^n} + 1$, the Fermat function. Then $f(\mathbb{I}) \not\subset \mathbb{P}$.*

Proof. 1. Since f is non constant, it is strictly increasing by 1.6, so there exits $n \in \mathbb{I}$ such that $f(n) > 1$. Let $p \in \mathbb{P}$ such that $p \mid f(n)$. Then $f(n) = 0 \mod p$. Since f is polynomial, we have

$$f(n+p) = f(n) \mod p.$$

So we have

$$p \mid f(n) \quad , \quad p \mid f(n+p) \quad , \quad 1 < f(n) < f(n+p).$$

This implies that $f(n+p)$ is not a prime number. So $f(\mathbb{I}) \not\subset \mathbb{P}$.

2. Let $n \in \mathbb{I}_{>1}$. Then $f(n) = a^n + b > 1$. Let $p \in \mathbb{P}$ such that $p \mid f(n)$. Then $a^n + b = 0 \mod p$. Assume first that $p \nmid a$, then by Fermat's little theorem

$$a^{n+(p-1)} + b = a^n + b = 0 \mod p.$$

So we have

$$p \mid f(n) \,, \quad p \mid f(n+(p-1)) \,, \quad 1 < f(n) < f(n+(p-1)).$$

This implies that $f(n+p-1)$ is not a prime number. Now if $p \mid a$, then $p < f(n)$ and $f(n)$ is not a prime number. So we have proved that $f(\mathbb{I}) \not\subset \mathbb{P}$.

3. We have $f(5) = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417$, as Euler [1] [2] computed. So $f(\mathbb{I}) \not\subset \mathbb{P}$.

□

2.2 Reformulation: $\mathbb{P}$ is supernatural

An infinite subset of $\mathbb{I}$ is said to be natural if it is of the form $f(\mathbb{I})$ where $f \in \mathcal{F}_{Natural}$ is non constant. An infinite subset of $\mathbb{I}$ is said to be supernatural if it does not contain any natural subset of $\mathbb{I}$. Our conjecture is now equivalent to the following statement: $\mathbb{P}$ is supernatural.

3 Implications and remarks

In this section we discuss implications of our conjecture and comment it.

Proposition 3.1. *Assume Conjecture 2.1 is true. Let $f \in \mathcal{F}_{Natural}$ non constant, then $\{x \in f(\mathbb{I}) \mid x$ is not a prime number $\}$ is infinite.*

Proof. By 1.6, f is strictly increasing. It is enough to prove the following statement. *For all $k \in \mathbb{I}$, there exists $q \in \mathbb{N}_{>k}$, such that $f(q)$ is not a prime number.* So let $k \in \mathbb{I}$. Let us consider the function $g \in \mathcal{F}(\mathbb{I}, \mathbb{I})$ defined by $g(n) = f(n+k)$. The function g is natural. So there exists $d \in \mathbb{I}$ such that $g(d)$ is not a prime number. So $q := d + k$ is such that $q > k$ and $f(q)$ is not a prime number. This ends the proof.

□

Corollary 3.2. *Assume Conjecture 2.1 is true. Then there are infinitely many composed (i.e. not prime) Fermat's numbers.*

Proof. Apply 3.1 to Fermat's natural function $n \mapsto 2^{2^n} + 1$.

□

Proposition 3.3. *Assume Conjecture 2.1 is wrong. Then there exists a computable formula giving arbitrary big prime numbers*

Proof. If Conjecture 2.1 is wrong. There exists a non constant (and thus strictly increasing) natural function giving only prime numbers. It is computable. □

Remark 3.4. *In order to define natural functions in Definition 1.4, we have used* $+, \times, \wedge$. *One can define with the same formalism a larger class of function using moreover Knuth's up arrow* $\{\uparrow^n \mid n \geq 1\}$ *notation for hyperoperation* $(\uparrow^1 = \wedge)$. *Then one can extend Conjecture 2.1 to this larger class of functions.*

References

[1] Leonhard Euler. Observationes de theoremate quodam fermatiano aliisque ad numeros primos spectantibus. 1732.

[2] Leonhard Euler. Theoremata circa divisors numerorum. 1747.

[3] Pierre Fermat. *Œuvres de Pierre Fermat. I.* Collection Sciences dans l'Histoire. Librairie Scientifique et Technique Albert Blanchard, Paris, 1999.