PROOF OF BUNYAKOVSKY'S CONJECTURE

ROBERT DELOIN

Abstract. Bunyakovsky's conjecture states that under special conditions, polynomial integer functions of degree greater than one generate infinitely many primes.

The main contribution of this paper is to introduce a new approach that enables to prove Bunyakovsky's conjecture. The key idea of this new approach is that there exists a general method to solve this problem by using only arithmetic progressions and congruences.

As consequences of Bunyakovsky's proven conjecture, three Landau's problems are resolved: the n^2+1 problem, the twin primes conjecture and the binary Goldbach conjecture.

The method is also used to prove that there are infinitely many primorial and factorial primes.

Contents

1. Introduction

In 1837, the German mathematician P. G. L. Dirichlet (1805-1859) proved that an arithmetic progression $ax + b$ (an integer function of degree $m = 1$ where x, a and b are integers with $gcd(a, b) = 1$), generates infinitely many primes.

In 1854, seventeen years after Dirichlet's theorem, the conjecture of the Ukrainian mathematician Victor Y. Bunyakovsky (1804-1889) mentioned in [1] is already a try to generalize this theorem to functions of degree $m > 1$. This conjecture states that, under two conditions mentioned hereafter, a polynomial function of degree $m > 1$ generates infinitely many primes.

A recurrent question is then: are primes of a certain form infinitely many? And a recurrent answer is: it is conjectured that they are infinitely many, or even: it is not known if they are infinitely many. This question necessitates a classification of the different possible forms of primes.

As the most generally encountered form is the polynomial form, this one is studied here, with the result that Bunyakovsky's conjecture is proven as well as, consequently, three of the four problems of Landau: $n^2 + 1$, twin primes and Goldbach conjectures.

As the question is still unresolved for primorial and factorial primes, these conjectures are also proven here.

2. Preliminary notes

2.1. **Definition of polynomial integer functions.** General functions are said to be polynomial if their expression is a polynomial of degree m:

$$f(x) = c_m x^m + c_{m-1} x^{m-1} + c_{m-2} x^{m-2} + \ldots + c_2 x^2 + c_1 x + c_0$$

with $m \in \mathbb{N}$ and x and $c_i \in \mathbb{R}$, where $\mathbb{N}$ is the set of all positive integers and $\mathbb{R}$ the set of all real numbers.

If we choose x and c_i in $\mathbb{N}$, all values of $f(x)$ are in $\mathbb{N}$ so that $f(x)$ becomes a polynomial integer function $f(n)$.

Finally, with $c_0 = b$, any polynomial integer function $f(n)$ can be written:

$$f(n) = g(n).n + b = a_n n + b$$

$g(n)$ being a polynomial of degree $m - 1$ and a_n its values.

2.2. **Definition of polynomial primes.** Polynomial primes $q(n, f)$ (hereafter abbreviated as q_n) are the primes generated by polynomial integer functions $f(n)$ by a set of values of n:

$$q_n = c_m n^m + c_{m-1} n^{m-1} + c_{m-2} n^{m-2} + \ldots + c_2 n^2 + c_1 n + c_0$$

or, more simply, with $c_0 = b$:

$$q_n = g(n).n + b = a_n n + b$$

where $g(n)$ is a polynomial of degree m-1 and a_n its values.

2.3. **Useful congruences for 3^k.** Generally, the quantity $f(n) = g(n).n+b$ can be odd or even. Using the covering system of $\mathbb{N}$: $k \equiv \{1,2,3,4\} \mod 4$, we respectively get that the numbers 3^k belong to the four congruences:

$$3^k = 3^{\{1,2,3,4\} \mod 4} \equiv \{3,9,7,1\} \mod 10 \tag{1}$$

2.4. **A useful congruence for 3^10^u.** For a correct future use of the congruence for 3^{10^u}, we have first to establish it as follows.

As $3^{10} = 59049 \equiv -1 \mod 10$ and $(3^{10})^2 = 3^{20^1} \equiv 3^{20^u} \equiv 1 \mod 10$:

$$3^{10^{2u}} = 3^{100^u} = (3^{20^u})^{5^u} \equiv 1 \mod 10$$
$$3^{10^{2u+1}} = 3^{10\times 10^{2u}} = (3^{10^{2u}})^{10} \equiv 1 \mod 10$$

so that:

$$3^{10^u} \equiv 1 \mod 10 \text{ for any integer } u > 1 \tag{2}$$

3. Proof of Bunyakovsky's conjecture

As odd primes $n = p$ are always part of the arithmetic progressions $p = A + 6k$ with $A = \{1,5\}$ and $k \in \mathbb{Z}\backslash 0$ where $\mathbb{Z}\backslash 0$ is the set of all integers, negative or positive, zero excepted , we have:

$$q_p = p.g(p) + b = a_p p + b = (A + 6k)a_p + b$$

As $\mathbb{Z}\backslash 0$ is covered by any of the systems of 10^u congruences $k \equiv \pm\{1, ..., 10^u\}$ mod 10^u with $u > 0$, we choose, with $u > 1$, one of these covering systems.

Then, for $k = \alpha + j10^u$ with $1 \leqslant \alpha \leqslant 10^u$ and for b such that $\gcd(A+6k, b) = 1$ and according to Fermat's little theorem for primes, we get that for any prime $q_p = (A + 6k)._{a_p} + b > 3$, we have:

$$3^{q_p} \equiv 3 \mod q_p \tag{3}$$

$$3^{(A+6k)a_p+b} \equiv 3 \mod q_p$$
$$3^b 3^{(A+6k)a_p} \equiv 3 \mod q_p$$
$$3^b 3^{Aa_p} 3^{6ka_p} \equiv 3 \mod q_p$$
$$3^b (3^A)^{a_p} (3^k)^{6a_p} \equiv 3 \mod q_p$$
$$3^b (3^A)^{a_p} (3^{\alpha+j10^u})^{6a_p} \equiv 3 \mod q_p$$

$$3^b (3^A)^{a_p} (3^\alpha)^{6a_p} (3^{10^u})^{6ja_p} \equiv 3 \mod q_p \tag{4}$$

and , with $u > 1$, $A = 1$ or 5, $b \leqslant 10^u$ with b such that $\gcd(A+6k, b) = 1$ and $1 \leqslant \alpha \leqslant 10^u$, we notice that the explicit constants 3^b, 3^A, 3^α and 3^{10^u} of (4) will not change modulo q_p when we consider $q_p > L = 3^{10^u}$.

Proof. **Hypothesis.** If polynomial primes were infinitely many, there would not exist any limit L beyond which there would be no more polynomial primes $q_p = (A + 6k)a_p + b$.

This means that, with $q_p > L = 3^{10^u}$ and choosing with the integer $u > 1$ one covering system of $\mathbb{N}$, with $k = \alpha + j10^u$ relations (3) and (4) should be verified for infinitely many q_p's.

But, we have on one hand, for the left side of (3), with a direct calculus for all odd prime q_p:

$$\begin{array}{ccc} \text{From (1)} & \text{and} & \text{as } q_p \text{ is an odd prime:} \\ 3^{q_p} & \equiv & \{3 \text{ or } 7\} \mod 10 \\ 3^{q_p} \mod q_p & \equiv & (\{3 \text{ or } 7\} \mod 10) \mod q_p \end{array}$$

and, on the other hand for the right side, as q_p is an odd prime:

$$\begin{array}{ccc} q_p + \{3 \text{ or } 7\} & \equiv & even \mod 10 \\ \{3 \text{ or } 7\} \mod q_p & \equiv & (even \mod 10) \mod q_p \end{array}$$

and we find that (3) is impossible for any $u > 1$, as we always have:

$$(\{3 \text{ or } 7\} \mod 10) \mod q_p \neq (even \mod 10) \mod q_p.$$

So, with this impossibility, we get the (weird but fortunately temporary) result that for any $u > 1$, there exist a limit $L_u = 3^{10^u}$ beyond which there are no more polynomial primes q_p. As the smallest limit is obtained for $u = 2$, we can even conclude that there are no polynomial primes $q_p = p.a_p + b$ beyond:

$$L_2 = 3^{10^2} = 3^{100} = 515377520732011331036461129765621272702107522001$$

But this is a wrong contradiction of the reality which cannot be proven for all polynomials but can be proven when divisible polynomials are discarded, leaving only indivisible polynomials to our consideration.

Here, the word indivisible has to be understood with Bunyakovsky's meaning which is described by two conditions [1]:
(A) the coefficients of the polynomial have to verify: gcd(coefficients) = 1;
(B) the polynomial has to be irreducible, that is to say, not divisible by any other polynomial of degree d with $0 \leqslant d < m$. It excludes, by instance:

$$\text{with } m = 2 \text{ and } d = 1\text{: } n^2 - b^2 = (n - b)(n + b)$$

and:

$$\text{with } m = 2 \text{ and } d = 0\text{: } n^2 + n + 2 = 2\left(\frac{n(n+1)}{2} + 1\right)$$

as $n(n + 1)/2$ is always an integer and 2 is the polynomial of degree $d = 0$.

The contradiction is wrong as it can be proven that bigger primes $q_n = g(n).n + b$ always exist beyond L_2 as follows.

Let's notice that even if n is not prime, for any odd prime $q_n = g(n).n + b$, n cannot be a multiple rb of b as then:

$$q_n = g(n).n + b = rb.g(rb) + b = b(r.g(rb) + 1)$$

is composite, which is impossible for a prime (except if $b = 1$ and $r.g(rb) + 1$ is prime, see note below). Therefore, if c is constrained to vary from 1 to $b - 1$, n can only belong to a set of $b - 1$ arithmetic progressions of modulus b:

$$n = rb + c \text{ with } 0 < c < b \text{ and } r \in \mathbb{Z}\backslash 0$$

that contain infinitely many primes and thus, all q_n's can only belong to the infinite set of arithmetic progressions (as $r \in \mathbb{Z}\backslash 0$):

$$q_n = g(n).n + b = (rb + c)g(rb + c) + b$$

which, as $\gcd(rb + c, b) = 1$ and according to Dirichlet's theorem, all contain infinitely many primes. This proves that infinitely many odd primes $q_n = n.g(rb + c) + b$ of form $q_n = g(n).n + b$ exist beyond L_2 and, in turn, proves that, under Bunyakovsky's conditions, polynomial primes $q_n = g(n).n + b$ are infinitely many, which is Bunyakovsky's conjecture. □

Note. When $b = 1$, as there is no possible integer c such that $0 < c < b = 1$, the infinitely many arithmetic progressions $n = rb + c$ become the infinitely many constant values $n = r$ so that the infinitely many arithmetic progressions $q_n = g(rb + c).n + b$ become:

$$q_n = g(r).n + 1$$

that can provide primes: for each integer r, each of these infinitely many arithmetic progressions $g(r).n + 1$ where $\gcd(g(r), 1) = 1$ provides, when evaluated at $n = r$, only one number $q_r = g(r).r + 1$ that, according to Dirichlet's theorem, is either composite or prime. So, the infinitely many arithmetic progressions $g(r).n + 1$ issued from indivisible polynomials (with Bunyakovsky's meaning) together provide infinitely many primes $q_r = g(r).r + 1$ coming in accordance with Dirichlet's theorem. This proves that the above main proof is also valid when $b = 1$.

It has to be noticed that, as Dirichlet's theorem does not exactly defines which primes appear in an arithmetic progression, the present proof of Bunyakovsky's conjecture does not and cannot do it as well, as it is based on this theorem.

4. Extension to fourth Landau's problem

The fourth Landau's problem is the question: are there infinitely many primes q_n such that $q_n = n^2 + 1$? This problem was mentioned as unsolved in 1912 at the fifth International Congress of Mathematicians (ICM) in Cambridge by Landau.

Proof. As Bunyakovsky's proven conjecture is now a theorem stating that polynomial primes $q_n = g(n).n + b$ are infinitely many, considering $g(n) = n$ and $b = 1$ which make that $q_n = n^2 + 1$ and $\gcd(g(n), b) = \gcd(n, 1) = 1$ for any n, this conjecture is also proven. □

5. Extension to other conjectures

With $g(n) = a$, a being any non-null integer constant, we get:

$$q_n = a.n + b$$

and Bunyakovsky's conjecture proven for polynomials of degree $m > 1$ reduces to Dirichlet's theorem and so, to infinitely many arithmetic progressions that are polynomials of degree $m = 1$ which, according to this theorem, generate infinitely many primes q_n for infinitely many n's which in turn, belong to infinitely many arithmetic progressions:

$$n = rb + c \text{ with } 0 < c < b \text{ and } r \in \mathbb{Z}\backslash 0$$

This is particularly true for odd primes q_n obtained with odd a's, infinitely many odd $n = rb + c$ which according to Dirichlet's theorem include infinitely many primes, and even b's such that $\gcd(a, b) = 1$. So, with $a = 1$ and even b's ($b = 2k$) it is true for the infinitely many polynomials $q_n = p + 2k$ of degree $m = 1$ based on odd primes p's instead of simply odd n's. This proves that the following conjectures generate infinitely many primes:

$$\begin{gathered} q_p = p + 2 \text{ (twin primes conjecture, Landau's second problem)}, \\ q_p = p + 4 \text{ (cousin primes conjecture)}, \\ q_p = p + 6 \text{ (sexy primes conjecture)}, \\ \text{and generally for:} \\ q_p = p + 2k \text{ for all } k \geqslant 0, \text{ (de Polignac's conjecture)} \end{gathered}$$

and with even a's, odd or even n's and odd b's such that $\gcd(a, b) = 1$, it is also particularly true for $n = p$, $a = 2$ and $b = 1$, that is to say for the conjecture:

$$q_p = 2p + 1 \text{ (Sophie Germain primes conjecture)}$$

6. Extension to the binary Golbach conjecture

Landau's first problem is the binary Goldbach conjecture. It states that any even number $2n \geqslant 4$ can be written as the sum of two primes, or symbolically:

$$2n = p_1 + p_2 \text{ for any } n \text{ such that } 2n \geqslant 4$$

We have seen with de Polignac's conjecture $q_p = p + 2k$ proven in last section, that Bunyakovsky's theorem implies that the odd primes $q_p = p + 2n$ are infinitely many for all odd primes p and all $n \geqslant 0$. But this does not prove that q_p can be any prime. And this has to be proven first, as follows.

Proof. Considering $n = 0$ and all odd primes p, we get: $q_p = p + 2n = p$. This means that the subset of numbers:

$$\{q_{p,2n=0}\} = \{p\}$$

is the set $\mathbb{P}\backslash 2$ of all odd primes, which are infinitely many as proven by Euclid.

Now, also considering $n \geqslant 1$, we then have, for $2n \geqslant 0$ and $p \geqslant 3$ (but limited here to $2n \leqslant 20$ and to $p \leqslant 41$ for a problem of line width):

Table 1: Subsets of primes $\{q_{p,2n=0,20} = p + 2n\}$

$\{q_p = p + 0\}$	=	**3**	5	7	11	13	17	19	23	29	31	37	41
$\{q_p = p + 2\}$	=		**5**	7		13		19			31		
$\{q_p = p + 4\}$	=			**7**	11		17		23				41
$\{q_p = p + 6\}$	=				11	13	17	19	23	29		37	
$\{q_p = p + 8\}$	=				**11**	13		19			31	37	
$\{q_p = p + 10\}$	=					**13**	17		23	29			41
$\{q_p = p + 12\}$	=						17	19	23	29	31		41
$\{q_p = p + 14\}$	=						**17**	19			31	37	
$\{q_p = p + 16\}$	=							**19**	23	29			
$\{q_p = p + 18\}$	=								23	29	31	37	41
$\{q_p = p + 20\}$	=								**23**		31	37	
...													

As the first odd prime p to be considered in each of the subsets $\{q_{p,2n\geqslant 2} = p + 2n\}$ is always $p = 3$ and as any odd prime q_p can be written $q_p = 3 + 2n$ because $3+2n$ is an arithmetic progression that covers all odd numbers greater than 1 and consequently all odd primes (boldface in the table), it proves that the set of all the subsets $\{q_{p,2n>0} = p + 2n\}$ constitutes a covering system of all odd primes greater than three or that the symbolic equation $q_p = p + 2n$ is valid for any odd prime $p \geqslant 3$, any $n \geqslant 1$ but also for all odd primes $q_p \geqslant 5$. □

We can now proceed with the binary Goldbach conjecture.

Proof. As the symbolic equation $q = p + 2n$ is now valid for any odd prime $p \geqslant 3$, any $n \geqslant 1$ and all odd primes $q \geqslant 5$, it is particularly true for all prime values n_p of n and the symbolic equation $q = p+2n$ is still valid when written:

$$q = p + 2n_p$$

or, renaming n_p by p_2 and p by p_1:

$$q = p_1 + 2p_2$$

This is still valid when written:

$$q - p_2 = p_1 + p_2 \tag{5}$$

But, as the symbolic equation $q = p+2n$ is now valid for all odd primes $q \geqslant 5$, any $n \geqslant 1$ and any primes $p_1 \geqslant 3$ and $p_2 \geqslant 3$, it implies that:

$$q = p_2 + 2n$$
or:
$$q - p_2 = 2n$$

for any $n \geqslant 1$ and we symbolically get from (5):

$$2n = p_1 + p_2$$

which proves the binary Goldbach conjecture for any $p_1 \geqslant 3$, $p_2 \geqslant 3$ and only $n \geqslant 3$. Finally, as:

$$\text{for } n = 2\text{: } 2n = 4 = 2 + 2$$

the binary Goldbach conjecture is proven for $n \geqslant 2$ or $2n \geqslant 4$ as required. □

7. Landau's four problems

As three of the four Landau's problems: $n^2 + 1$, twin primes and Goldbach's conjecture have been proven here and that the fourth one, Legendre's conjecture, has been proven in [3], the four Landau's problems are resolved.

8. Extension to primorial primes conjecture

8.1. **The primorial primes conjecture.** Primorial primes [4] [5] are primes of the form: $q_n = p_n\# + 1$ where $p_n\#$ is the primorial of p_n defined by $p_n\# = 2 \times 3 \times 5 \times 7 \times \ldots \times p_n$. As we have:

$$q_n = p_n\# + 1 = p_n.p_{n-1}\# + 1$$

we see that q_n is also of the form $g(n).n + b$ where $n = p_n$ and $g(n) = p_{n-1}\#$ is the fully factorized polynomial function of n:

$$g(n) = 2 \times 3 \times 5 \times 7 \times 11 \times ... \times p_{n-1}$$

The primorial primes conjecture is the question: are there infinitely many primes $q_n = p_n\# + 1$ or infinitely many primes p_n such that $q_n = p_n\# + 1$ is also prime?

8.2. **A useful congruence for primorial primes.** As $q_n = p_{n-1}\# \times p_n + 1$, we also have:

$$\begin{array}{ccc} 3^{q_n} = 3^{p_{n-1}\# \times p_n + 1} & = & 3 \times 3^{p_{n-1}\#}(3^{p_{n-1}\#})^{p_n - 1} \\ \text{and, as from Fermat's little theorem,} & & \text{with } p_n > 3 \text{ being prime:} \\ (3^{p_{n-1}\#})^{p_n - 1} & \equiv & 1 \mod p_n \\ \text{we get: } 3^{q_n} \equiv 3 \times 3^{p_{n-1}\#} & \equiv & 3^{p_{n-1}\#+1} \mod p_n \\ 3^{q_n} & \equiv & 3^{q_{n-1}} \mod p_n \end{array}$$

As this congruence defines a recurrence on 3^{q_n} that begins with $3^{q_{n-1}} = 3^{q_1} = 3^{p_1\#+1} = 3^{2\#+1} = 3^3$, we finally have for any odd prime $p_n > 3$:

$$3^{q_n} \equiv 3^3 \mod p_n \tag{6}$$

8.3. **Proof of primorial primes conjecture.** As odd primes $n = p$ always belong to the arithmetic progressions $A + 6k$ with $A = \{1, 5\}$:

$$q_n = q_{n,k} = (A + 6k)p_{n-1}\# + 1$$

As $\mathbb{N}$ is completely covered by the system of 10^u congruences $k \equiv \{1, ..., 10^u\} \mod 10^u$, we can choose, with the integer $u > 1$, one of these covering systems.

For $k = \alpha + j10^u$ with $1 \leqslant \alpha \leqslant 10^u$ and for b such that $\gcd(A + 6k,\, b) = 1$, we get that for any prime $q_n = (A + 6k).g(n) + b$, we have from (6):

$$\begin{gathered} 3^{(A+6k)p_{n-1}\#+1} \equiv 27 \mod p_n \\ 3 \times 3^{(A+6k)p_{n-1}\#} \equiv 27 \mod p_n \\ 3 \times (3^A)^{p_{n-1}\#}(3^k)^{6p_{n-1}\#} \equiv 27 \mod p_n \\ 3 \times (3^A)^{p_{n-1}\#}(3^{\alpha+j10^u})^{6p_{n-1}\#} \equiv 27 \mod p_n \end{gathered}$$

$$3 \times (3^A)^{p_{n-1}\#}(3^\alpha)^{6p_{n-1}\#}(3^{10^u})^{6jp_{n-1}\#} \equiv 27 \mod p_n \tag{7}$$

and we notice, as $u > 1$, $A = 1$ or 5 and $1 \leqslant \alpha \leqslant 10^u$, that the explicit constants 3, 3^A, 3^α and 3^{10^u} of (7) will not change modulo p_n when we consider a modulus $p_n > L = 3^{10^u}$.

Proof. **Hypothesis.** If primorial primes $q_n = (A+6k)p_{n-1}\#+1$ were infinitely many, there would not exist a limit L beyond which there would be no more of them.

This also means that for $q_n > L = 3^{10^u}$, choosing with the integer $u > 1$ one covering system of $\mathbb{N}$, with $k = \alpha + j10^u$ relations (6) and (7) should be verified for infinitely many q_n's.

But, we have on one hand, for the left side of (6), with a direct calculus for all odd prime q_n:

$$\begin{array}{rcc} \text{As: } 3^{\{1,2,3,4\} \mod 4} & \equiv & \{3,9,7,1\} \mod 10 \\ \text{and, as } q_n \text{ is odd: } 3^{q_n} & \equiv & \{3 \text{ or } 7\} \mod 10 \\ 3^{q_n} \mod p_n & \equiv & (\{3 \text{ or } 7\} \mod 10) \mod p_n \end{array}$$

and, on the other hand, for the right side, for any odd prime p_n:

$$\begin{array}{rcc} p_n + 27 & \equiv & even \mod 10 \\ 27 \mod p_n & \equiv & (even \mod 10) \mod p_n \end{array}$$

and (6) is impossible for any $u > 1$, as we always have:

$$(\{3, \text{ or } 7\} \mod 10) \mod p_n \neq (even \mod 10) \mod p_n.$$

So, with this impossibility, we get the (weird but fortunately temporary) result that for any $u > 1$ and any $k > 0$, there exist a limit $L_u = 3^{10^u}$ beyond which there is no more primorial primes q_n. As the smallest limit is obtained for $u = 2$, we can even conclude that there are no primorial primes q_n beyond:

$$L_2 = 3^{10^2} = 515377520732011331036461129765621272702107522001$$

which has 48 digits. But this is a wrong contradiction of the reality because we know that bigger primorial primes exist. The biggest of them, found in 2001 by the PrimeGrid project [4], has 169,966 digits:

$$q_{392113} = 392113\# + 1$$

Then, how do we get out of this wrong contradiction?

As we have the above contradiction for any fixed $u > 1$, the only solution to get out of it is to symbolically choose one covering system of $\mathbb{N}$ based on $u = \infty$ so that $L_\infty = 3^{10^\infty} = \infty$.

Thus, as the contradiction now occurs for $q > L_\infty = \infty$ (which looks like a nonsense), there is no more contradiction for $q < \infty$.

It indeed proves that no fixed limit $L < \infty$ exists beyond which there are no more primorial primes, and this, in turn, proves that primorial primes $q = p\# + 1$ are infinitely many. □

8.4. **List of primorial primes p up to 2657.** In less than 2 minutes on a laptop computer, the following GP/PARI program [2] gives the list of primorial primes $p \leqslant 2,657$:

3, 5, 7, 11, 31, 379, 1019, 1021, 2657, ...

Bigger lists can be found in [4] and [5]. The GP/PARI program for primorial primes follows:

```
# /* to start the timer */
pmax=2659;b=1;oldprim=2;
forprime(p=3,pmax,oldprim=oldprim*p;q=oldprim+b;\
  if(isprime(q)==1,print1(n,", "));)
# /* to stop the timer */
```

9. Extension to factorial primes conjecture

We now mimic the proof of last section to apply it to factorial primes with appropriate adjustments for constants and expressions.

9.1. **The factorial primes conjecture.** Factorial primes are primes of the form: $q_n = n! + 1$ where $n!$ is the factorial of n defined by $n! = 1 \times 2 \times 3 \times 4 \times 5 \times \ldots \times n$. As we have:

$$q_n = n! + 1 = n.(n-1)! + 1$$

we see that q_n is also of the form $g(n).n + b$ where g(n) is the fully factorized polynomial function:

$$g(n) = (n-1)! = (1)(2)(3)...(n-2)(n-1)$$

The factorial primes conjecture is the question: are there infinitely many primes $q_n = n! + 1$?

9.2. **A useful congruence for factorial primes.** As $q_n = n(n-1)! + 1$, we also have:

$$\begin{aligned} 3^{q_n} = 3^{n(n-1)!+1} &\equiv 3 \times 3^{n(n-1)!} \\ &\equiv 3 \times (3^{(n-1)!})^n \\ &\equiv 3 \times 3^{(n-1)!}(3^{(n-1)!})^{(n-1)} \end{aligned}$$

Now, with prime $n > 3$ replaced by $p > 3$:

$$\equiv 3 \times 3^{(p-1)!}(3^{(p-1)!})^{(p-1)}$$

and from Fermat's little theorem for primes $p > 3$:

$$\begin{aligned} (3^{(p-1)!})^{(p-1)} &\equiv 1 \mod p \\ \text{we get: } 3^{q_p} \equiv 3 \times 3^{(p-1)!} &\equiv 3^{(p-1)!+1} \mod p \\ 3^{q_p} &\equiv 3^{q_{p-1}} \mod p \end{aligned}$$

As this congruence defines a recurrence on 3^{q_p} that begins with $3^{q_{p-1}} = 3^{q_1} = 3^{p_1!+1} = 3^{2!+1} = 3^3$, we finally have for any odd prime $n = p > 3$:

$$3^{q_p} \equiv 3^3 \mod p \tag{8}$$

9.3. **Proof of factorial primes conjecture.** Even if generally n can be odd or even, during the proof it will be supposed that $n > 3$ is a prime $p > 3$ in order to be able to use congruence (8). As primes $p > 3$ always belong to the arithmetic progressions $A + 6k$ with $A = \{1, 5\}$, we have:

$$q_p = q_{p,k} = (A + 6k)(p - 1)! + 1$$

As set $\mathbb{N}$ is completely covered by the system of congruences $\{1, ..., 10^u\} \mod 10^u$, we can choose, with the integer $u > 1$, one of these covering systems.

For $k = \alpha + j10^u$ with $1 \leqslant \alpha \leqslant 10^u$ and for b such that $\gcd(A + 6k,\, b) = 1$, we get that for any prime $q_p = (A + 6k).g(n) + b$, we have from (8):

$$\begin{gathered}
3^{(A+6k)(p-1)!+1} \equiv 27 \mod p \\
3 \times 3^{(A+6k)(p-1)!} \equiv 27 \mod p \\
3 \times 3^{A(p-1)!}3^{6k(p-1)!} \equiv 27 \mod p \\
3 \times (3^A)^{(p-1)!}(3^k)^{6(p-1)!} \equiv 27 \mod p \\
3 \times (3^A)^{(p-1)!}(3^{\alpha+j10^u})^{6(p-1)!} \equiv 27 \mod p
\end{gathered}$$

$$3 \times (3^A)^{(p-1)!}(3^\alpha)^{6(p-1)!}(3^{10^u})^{6j(p-1)!} \equiv 27 \mod p \tag{9}$$

and we notice, with $u > 1$, $A = 1$ or 5 and $1 \leqslant \alpha \leqslant 10^u$, that the explicit constants 3, 3^A, 3^α and 3^{10^u} of (9) will not change modulo p when we consider a modulus $p > L = 3^{10^u}$.

Proof. **Hypothesis.** If factorial primes $q_p = (A+6k)(p-1)!+1$ were infinitely many, there would not exist a limit L beyond which there would be no more of them.

This also means that for a factorial prime $q_p > L = 3^{10^u}$, choosing with the integer $u > 1$ one of the covering systems of $\mathbb{N}$, with $k = \alpha + j10^u$ relations (8) and (9) should be verified for infinitely many q_p's.

But, we have on one hand, for the left side of (8), with a direct calculus:

$$\begin{array}{rcc}
\text{As: } 3^{\{1,2,3,4\} \mod 4} & \equiv & \{3, 9, 7, 1\} \mod 10 \\
\text{And as } q_p \text{ is odd: } 3^{q_p} & \equiv & \{3 \text{ or } 7\} \mod 10 \\
3^{q_p} \mod p & \equiv & (\{3 \text{ or } 7\} \mod 10) \mod p
\end{array}$$

and, on the other hand, for the right side, as $p > 2$ is odd:

$$\begin{array}{rcc}
p + 27 & \equiv & even \mod 10 \\
27 \mod p & \equiv & (even \mod 10) \mod p
\end{array}$$

and (8) is impossible for any $u > 1$, as we always have:

$$(\{3 \text{ or } 7\} \mod 10) \mod p \neq (even \mod 10) \mod p.$$

So, with this impossibility, we get the (weird but fortunately temporary) result that for any $u > 1$ and any $k > 0$, there exist a limit $L_u = 3^{10^u}$ beyond which there is no more factorial primes q_p. As the smallest limit is obtained for $u = 2$, we can even conclude that there are no factorial primes q_p beyond:

$$L_2 = 3^{10^2} = 515377520732011331036461129765621272702107522001$$

which has 48 digits. But this is a wrong contradiction of the reality because we know that bigger factorial primes q_p exist. The biggest of them, found by the PrimeGrid project [2], has 712,355 digits:

$$q_{150209} = 150209! + 1$$

where 150209 is prime. Then, how do we get out of this wrong contradiction? As the above contradiction holds for any fixed $u > 1$, the only solution to get out of it is to symbolically choose one covering system of $\mathbb{N}$ based on $u = \infty$ so that $L_\infty = 3^{10^\infty} = \infty$.

Thus, as the contradiction now occurs for $q_p > L_\infty = \infty$ (which looks like a nonsense), there is no more contradiction for $q_p < \infty$.

It indeed proves that no fixed limit $L < \infty$ exists beyond which there are no more factorial primes q_p, and this in turn, as all natural numbers n include all odd primes p, proves that factorial primes $q_n = n! + 1$ are infinitely many. □

9.4. **List of n's that generate factorial primes.** In less than 3 minutes on a laptop computer, the following GP/PARI program gives the list of $n \leqslant 427$ (prime or not) that generate factorial primes $q_n = n! + 1$:

$$n = 3,\ 11,\ 27,\ 37,\ 41,\ 73,\ 77,\ 116,\ 154,\ 320,\ 340,\ 399,\ 427,\ ...$$

Bigger lists can be found in [4] and [5]. The GP/PARI program for factorial primes follows:

```
# /* to start the timer */
pmax=427;b=1;oldfact=2;
for(n=3,pmax,oldfact=oldfact*n;q=oldfact+b;\
  if(isprime(q)==1,print1(n,", "));)
# /* to stop the timer */
```

Acknowledgements. This work is dedicated to my family. As I am a hobbyist in mathematics, I also wish to express my gratitude towards the Editors of this journal as well as towards the team of Reviewers for having welcomed, reviewed and accepted my article.

References

[1] Bouniakowsky V., Sur les diviseurs numériques invariables des fonctions rationnelles entières, *Mémoires de l'Académie Impériale des Sciences de Saint-Pétersbourg*, Sixième série Sciences Mathématiques, Physiques et Naturelles **Tome VIII**, Première partie **Tome VI**, 1857, 305-329

[2] GP/PARI program available at University of Bordeaux (France): http://pari.math.u-bordeaux.fr/download.html

[3] Deloin, R., Improved version of: From Sierpinski's conjecture to Legendre's, *Theoretical Mathematics & Applications*, **6**(4), 2016, 13-31 http://www.scienpress.com/journal_focus.asp?main_id=60&Sub_id=IV&Issue=1890

[4] OEIS, The On-line Encyclopedia of Integer Sequences, Primorial primes are at: http://oeis.org/A005234 Factorial primes are at: http://oeis.org/A002981

[5] Caldwell C., Prime Pages,
Primorial primes at: http://primes.utm.edu/top20/page.php?id=5
Factorial primes at: http://primes.utm.edu/top20/page.php?id=30

Robert Deloin, Bouc Bel Air, France
E-mail address: rdeloin@free.fr