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 nˆ2+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 $x = n$ 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, setting $c_0 = b$, any polynomial integer function $f(n)$ can be written:

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

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

2.2. **Definition of polynomial primes.** Polynomial primes $q(f, n)$ (hereafter abbreviated as q_n) are the primes generated by polynomial integer functions $f(n)$ by a special 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 $c_0 = b$:

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

3. Proof of Bunyakovsky's conjecture

3.1. **Bunyakovsky's conjecture.** This conjecture states that, under two conditions mentioned hereafter, a polynomial function of degree $m > 1$ generates infinitely many primes.

The two conditions come from the fact that the considered polynomial has to be indivisible, this word being taken with the sense given to it by Bunyakovsky in its article [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 $d = 0$.

3.2. **A useful congruence for polynomial primes.** In the present proof, we will consider only odd prime values $p > 3$ of n and so, only the values:

$$q_p = p.g(p) + b = p.g_p + b$$

We thus get:

$$3^{q_p} = 3^{p \cdot g_p + b}$$
$$3^{q_p} = 3^b (3^p)^{g_p}$$

and as according to Fermat's little theorem we have for $p > 3$:

$$3^p \equiv 3 \mod p$$

we also get for $p > 3$:

$$(1) \qquad 3^{q_p} = 3^{g_p + b} \mod p$$

3.3. **Proof of Bunyakovsky's conjecture.**

Proof. According to Fermat's little theorem, for an existing prime number q_p, we have:

$$(2) \qquad 3^{q_p} \equiv 3 \mod q_p$$

With congruences (1) and (2), and still for an existing prime number q_p, we get the system of two verified congruences:

$$3^{q_p} \equiv 3^{g_p + b} \mod p$$
$$3^{q_p} \equiv 3 \mod q_p$$

Now, in order to generalize the problem by including the possibility of non existing primes q_n, let's replace 3^{q_n} by x. This gives the system:

$$x \equiv 3^{g_p + b} \mod p$$
$$x \equiv 3 \mod q_p$$

and we know from the chinese theorem that this system has always a solution:

$$x \equiv x_0 \mod m$$
with:
$$m = m_1 m_2 = pq_p$$
$$x_0 = 3^{g_p+b} b_1 q_p + 3b_2 p$$
b_j being determined by:
$$\frac{m}{m_j} b_j \equiv 1 \mod m_j$$

As with:

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

$x = 3^{q_p}$ verifies the system, it proves that these numbers q_p always exist as a solution of this system and, as the primes p are infinitely many, they are also infinitely many.

Moreover, as $x = 3^{q_p}$ verifies the second congruence which is Fermat's test of primality for q_p, it proves that these numbers q_p are generally prime, except those q_p's that are pseudoprimes in base 3.

These two last points prove that polynomial primes are infinitely many, which is exactly Bunyakovsky's conjecture. □

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 conjecture is now proven, 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 $m = 1$. These ones, according to the same 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:

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

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:

$q_p = 2p + 1$ (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 the proven conjecture of Bunyakovsky 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:

$$q - p_2 = p_1 + p_2 \tag{3}$$

But, as from Table 1 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 we can symbolically write:

$$q = p_2 + 2n$$

or:

$$q - p_2 = 2n$$

for any $n \geqslant 1$ and we symbolically get from (3):

$$2n = p_1 + p_2$$

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:

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

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:

$$g(n) = p_{n-1}\# = p_n\#/p_n$$

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 $p_n > 3$:

$$3^{q_n} \equiv 27 \mod p_n \tag{4}$$

8.3. **Proof of primorial primes conjecture.**

Proof. According to Fermat's little theorem, for an existing prime number q_n, we have:

$$3^{q_n} \equiv 3 \mod q_n \tag{5}$$

With congruence (4), and still for an existing prime number q_n, we get the system of two verified congruences:

$$3^{q_n} \equiv 27 \mod p_n$$
$$3^{q_n} \equiv 3 \mod q_n$$

Now, in order to generalize the problem by including the possibility of non existing primes q_n, let's replace 3^{q_n} by x. This gives the system:

$$x \equiv 27 \mod p_n$$
$$x \equiv 3 \mod q_n$$

and we know from the chinese theorem that this system has always a solution:

$$x \equiv x_0 \mod m$$
with:
$$m = m_1 m_2 = p_n q_n$$
$$x_0 = 27 b_1 q_n + 3 b_2 p_n$$

$$b_j \text{ being determined by:}$$
$$\frac{m}{m_j} b_j \equiv 1 \mod m_j$$

As with:

$$q_p = p_n\# + 1$$

$x = 3^{q_p}$ verifies the system, it proves that these numbers q_p always exist as a solution of this system and, as the primes p are infinitely many, they are also infinitely many.

Moreover, as $x = 3^{q_p}$ verifies the second congruence which is Fermat's test of primality for q_p, it proves that these numbers q_p are generally prime, except those q_p's that are pseudoprimes in base 3.

These two last points prove that primorial primes $q_n = p_n\# + 1$ are infinitely many, which is exactly the primorial primes conjecture. □

8.4. **List of primes p generating primorial primes q.** In less than 2 minutes on a laptop computer, the following GP/PARI program [2] gives the list of primes $p \leqslant 2,657$ that generate primorial primes $q_p = p\# + 1$:

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:

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

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:

$$\begin{array}{ccc}
3^{q_n} = 3^{n(n-1)!+1} & \equiv & 3 \times 3^{n(n-1)!} \\
 & \equiv & 3 \times (3^{(n-1)!})^n \\
 & \equiv & 3 \times 3^{(n-1)!}(3^{(n-1)!})^{(n-1)} \\
\text{and with prime } n = p > 3\text{:} & & \\
 & \equiv & 3 \times 3^{(p-1)!}(3^{(p-1)!})^{(p-1)} \\
\text{Now, as from Fermat's little theorem} & & \text{for primes } p > 3\text{, we have:} \\
(3^{(p-1)!})^{(p-1)} & \equiv & 1 \mod p \\
\text{we get: } 3^{q_p} \equiv 3 \times 3^{(p-1)!} & \equiv & 3^{(p-1)!+1} \mod p \\
3^{q_p} & \equiv & 3^{q_{p-1}} \mod p
\end{array}$$

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 $n = p > 3$:

$$3^{q_p} \equiv 27 \mod p \tag{6}$$

9.3. **Proof of factorial primes conjecture.**

Proof. According to Fermat's little theorem, for an existing prime number q_n, we have:

$$3^{q_n} \equiv 3 \mod q_n \tag{7}$$

With congruence (6) and still for an existing prime number q_n, we get the system of two verified congruences:

$$\begin{array}{c}
3^{q_n} \equiv 27 \mod p_n \\
3^{q_n} \equiv 3 \mod q_n
\end{array}$$

Now, in order to generalize the problem by including the possibility of non existing primes q_n, let's replace 3^{q_n} by x. This gives the system:

$$\begin{array}{c}
x \equiv 27 \mod p_n \\
x \equiv 3 \mod q_n
\end{array}$$

and we know from the chinese theorem that this system has always a solution:

$$\begin{array}{c}
x \equiv x_0 \mod m \\
\text{with:} \\
m = m_1 m_2 = p_n q_n \\
x_0 = 27 b_1 q_n + 3 b_2 p_n \\
b_j \text{ being determined by:} \\
\frac{m}{m_j} b_j \equiv 1 \mod m_j
\end{array}$$

As with:

$$q_p = p_n! + 1$$

$x = 3^{q_p}$ verifies the system, it proves that these numbers q_p always exist as a solution of this system and, as the primes p are infinitely many, they are also infinitely many.

Moreover, as $x = 3^{q_p}$ verifies the second congruence which is Fermat's test of primality for q_p, it proves that these numbers q_p are generally prime, except those q_p's that are pseudoprimes in base 3.

These two last points prove that factorial primes $q_n = p_n! + 1$ are infinitely many, which is exactly the factorial primes conjecture. □

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