PROOF OF BUNYAKOVSKY'S CONJECTURE

ROBERT DELOIN

Abstract. In 1857, twenty years after Dirichlet's theorem on arithmetic progressions, the conjecture of the Ukrainian mathematician Victor Y. Bunyakovsky (1804-1889) is already a try to generalize this theorem to polynomial integer functions of degree $m > 1$. This conjecture states that under three conditions a polynomial integer function of degree $m > 1$ generates infinitely many primes.

The main contribution of this paper is to introduce a new approach to this conjecture. The key ideas of this new approach is to relate the conjecture to a general theory (here arithmetic progressions) and use the active constraint of this theory (Dirichlet's theorem) to achieve the proof.

Mathematics Subject Classification : 11A41, 11A51, 11B25, 11C08
Keywords: polynomials, arithmetic progression, prime, conjecture

Contents

1. Introduction

In 1837, the German mathematician P. G. L. Dirichlet (1805-1859) [1][2] proved that an arithmetic progression $a+bd$ of modulus d (a polynomial integer function of degree 1 in d where d, a and b are integers with $gcd(a, d) = 1$), generates infinitely many primes.

In 1857, twenty years after Dirichlet's theorem, the conjecture of the Ukrainian mathematician Victor Y. Bunyakovsky (1804-1889) mentioned in [3] is already a try to generalize this theorem to polynomial integer functions of degree $m > 1$. This conjecture states that, under three conditions mentioned hereafter, a polynomial function of degree $m > 1$ generates infinitely many primes.

As of year 2020, this conjecture was still open.

2. Preliminary notes

General functions are said to be *polynomial integer functions* if their expression is a polynomial of degree $d = m$:

$$f(n) = a_m n^m + a_{m-1} n^{m-1} + a_{m-2} n^{m-2} + \ldots + a_2 n^2 + a_1 n + a_0$$

with n, a_i and $m \in \mathbb{N}$ so that all values $f(n)$ are also in $\mathbb{N}$.

Bunyakovsky's conjecture states that, under three conditions mentioned hereafter, a polynomial integer function of degree $m > 1$ generates infinitely many primes. The three conditions come from the fact that the considered polynomial moreover has to be irreducible, this word being taken with the sense given to it by Bunyakovsky's in its article:

(A) the leading coefficient must be positive;

(B) the polynomial coefficients have to verify $gcd(coefficients) = 1$;

(C) the polynomial has to be irreducible, that is to say, not divisible by any other polynomial of degree d with $0 \leq d < m$.

Note. The integer function $f(n) = 5n^2 + 15n + 125$ is not irreducible because $gcd(a_i) = 5$; $f(n) = n^2 + n + 2$ is also not irreducible but for a different reason: an hidden constant factor 2 appears when $f(n)$ is written as

$$f(n) = n^2 + n + 2 = 2\left(\frac{n(n+1)}{2} + 1\right)$$

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

3. Proof of Bunyakovsky's conjecture

The proof will be given in two steps.

1- the polynomial integer function has to be related to a general theory from which it gets constraints;

2- the constraints are applied to reach the proof.

3.1. Relating the conjecture to the theory of arithmetic progressions.

Let's consider the infinitely many arithmetical progressions

$$A(n, k, \delta) = n + k\delta \tag{1}$$

where n and k are general integers and $\delta \neq 0$ is the integer common difference between numbers A. Let's add the relation $gcd(n, \delta) = 1$ so that not all combinations of n, k and δ are allowed but for the remaining ones Dirichlet's theorem applies. We thus can say that each of these remaining infinitely many arithmetic progressions contains infinitely many primes.

Let's now discover the key feature of the proof. Let's build a new polynomial function $X(A)$ by applying the polynomial integer function $f(n) = polynomial(n)$ to these infinitely many arithmetic progressions, $polynomial(n)$ being any irreducible polynomial. We get the polynomial integer function

$$X(A) = polynomial(A)$$

From (1) we then have

$$\begin{aligned} X(A) &= polynomial(n+k\delta) \\ &= polynomial(n) + (polynomial(n+k\delta) - polynomial(n)) \\ &= \sum_{d=0}^{m} a_d(n)^d + \left(\left(\sum_{d=0}^{m} a_d(n+k\delta)^d\right) - \left(\sum_{d=0}^{m} a_d(n)^d\right)\right) \end{aligned}$$

or, noticing that all terms of $polynomial(n)$

disappear in $(polynomial(n+kd) - polynomial(n))$

$$X(A) = X(n,k,\delta) = polynomial(n) + k\delta.h(n,k,\delta)$$

where $h(n,k,\delta)$ is a polynomial.

Let's illustrate this result with the irreducible $polynomial(n) = 5n^2+3n+7$.

$$\begin{aligned} X(A) &= polynomial(n+k\delta) \\ &= polynomial(n) + (polynomial(n+k\delta) - polynomial(n)) \\ &= (5n^2+3n+7) + \big(7+5(n+k\delta)^2+3(n+k\delta)\big) - \big(5n^2+3n+7\big) \\ &= (5n^2+3n+7) + \big(\big(5(2nk\delta+k^2\delta^2)+3(k\delta)\big)\big) \\ &= (5n^2+3n+7) + k\delta\,(5(2n+k\delta)+3) \end{aligned}$$

This result allows us to look at function $X(A)$ as if it were an infinite set of arithmetic progressions $X(n,k,\delta)$ of miscellaneous common differences or moduli. As its second term $k.\delta.h(n,k,\delta)$ is made of three factors, we have several ways to choose a modulus μ from it but only $\mu = \delta.h(n,k,\delta)$ leads simply to the proof of Bunyakovsky's conjecture. We thus choose to write

$$X(A) = X(n,k,\delta) = polynomial(n) + k[\delta.h(n,k,\delta)] \tag{2}$$

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

Proof. According to Dirichlet's theorem, each of the arithmetic progressions of (2) contains infinitely many primes when the condition

$$gcd(polynomial(n), \delta.h(n,k,\delta)) = 1 \tag{3}$$

is verified.

As the second term $\delta.h(n,k,\delta)$ of this gcd is composite, this condition (3) is *almost always* verified when its first term ($polynomial(n)$) is prime. The word *almost* is justified by the two exceptions that create constant divisors $\neq 1$ by

$$divisor = gcd(polynomial(n),\delta) \neq 1$$

or

$$divisor = gcd(polynomial(n), h(n,k,\delta)) \neq 1)$$

Finally, disregarding these two exceptions that do not verify Dirichlet's gcd condition, we have to consider two facts

1- the second term $\delta.h(n,k,\delta)$ of the gcd in (3) is *always* composite and

2- Dirichlet's theorem *always implies* by its *gcd* condition (3) that each of the infinitely many arithmetic progressions $X(n, k, \delta)$ equivalent to any irreducible $polynomial(n + k\delta)$ contains infinitely many primes.

These two facts *always imply* that *the first term of the gcd* in (3) (any irreducible) $polynomial(n)$ *has to be prime infinitely often* in order to be in accordance with the infinitely many primes that have to be present in each corresponding arithmetic progression $X(n, k, \delta)$ according to Dirichlet's theorem. This solves Bunyakovsky's conjecture.

□

ACKNOWLEDGEMENTS. This work is dedicated to my family.

References

[1] P. G. L. Dirichlet, "Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält," [Proof of the theorem that every unbounded arithmetic progression, whose first term and common difference are integers without common factors, contains infinitely many prime numbers], Abhandlungen der Königlichen Preussischen Akademie der Wissenschaften zu Berlin, 8, 1837, pp. 45-81. https://gallica.bnf.fr/ark:/12148/bpt6k99435r/f326 (pdf p. 313)

[2] R. Stephan, "There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime," (English translation of Dirichlet's 1837 publication), 2014. https://arxiv.org/pdf/0808.1408.pdf

[3] V. Y. Bounyakowsky, "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, pp. 305-329.

Robert Deloin, 13320 Bouc Bel Air, France
E-mail address: `rdeloin@free.fr`