EasyChair Preprint

№ 8203

Existence of a Quadratic Polynomial, Which Represents Infinitely Many Prime Numbers

Valerii Sopin

November 20, 2023

Existence of a quadratic polynomial, which represents infinitely many prime numbers

Valerii Sopin
email: VvS@myself.com

November 20, 2023

Abstract

No single case of Bunyakovsky's conjecture for degree greater than one has been proved, although numerical evidence in higher degree is consistent with the conjecture. In this paper we overcome such misfortune (using Friedlander–Iwaniec theorem, Fermat's theorem on sums of two squares and Brahmagupta–Fibonacci Identity, Bezout's lemma and a connection to SL(2, Z) and Hyperbolic Prime Number Theorem).

Keywords: *Bunyakovsky's conjecture, Landau's problems, complete and subcomplete sequences, prime numbers, p-adic analysis, Fermat's theorem on sums of two squares, Goldbach's conjecture, Dickson's conjecture, Bateman–Horn conjecture, primes represented by polynomials, Sieve theory.*

1 Introduction

Since the number of all primes is infinite we have the question of whether the number of primes, which for example are contained in the form n^2+1 (the 4th Landau problem, the 5th Hardy-Littlewood conjecture), is also infinite. As the 4th Landau problem (it goes back to Euler, who observed in a letter to Goldbach in 1752 that n^2+1 is often prime for n up to 1500) demonstrates, particular problems of this type have long been of interest; however, the first formulation of a precise conjecture had to wait until Viktor Bunyakovsky in 1857 [1]:

Suppose $f(x)$ is a non-constant polynomial with integer coefficients and positive leading coefficient. Moreover, suppose that $f(x)$ is irreducible in $\mathbb{Z}[x]$ ($\mathbb{Z}$ is for integers) and that there is no prime q which divides $f(n)$ for every positive integer value of n (the numbers $f(n)$ should be relatively prime). Then $f(n)$ is prime for infinitely many positive integer values of n.

Bunyakovsky's conjecture was later generalized to a finite family of polynomials by Schinzel, who with Sierpinski [2] gave several applications to elementary number theory.

In the case of a single linear polynomial, Bunyakovsky's conjecture amounts to Dirichlet's 1837 theorem on primes in progressions. But Dirichlet's theorem has remained the only proven case of it.

Probably the main problem with the conjecture is the lack of good reformulations of its conditions in case of degree higher than 1. This leads to the idea of consideration not one polynomial, but aggregation of polynomials in the following way:

Conjecture. *If the leading coefficient of a polynomial $f(x)$ with integer coefficients is positive, then there exists integer c such that $f(\mathbb{N})+c$ contains infinitely many primes.*

It is helpful to keep in mind next picture: every integer point (x,y) on coordinate plane represents tuple $\{x, f(x)+y\}$. Notice that for any fixed n $f(n)+c$ (c is any integer) contains all prime numbers, as it covers range of arithmetic progression $x+1$. Moreover, Hilbert's irreducibility theorem guarantees that the polynomial $f(x)+c$ is irreducible for almost every c. In addition, it is worthy to highlight that the Conjecture is obvious for a linear polynomial and it can be used to give a simple proof of Dirichlet's theorem on arithmetic progressions.

In this paper we show existence of a quadratic polynomial, range of which contains infinitely many prime numbers. On the whole, we prove the first case of Bunyakovsky's conjecture for degree greater than 1.

2 Main result

To obtain the pronouncement we are going to use Fermat's Theorem on sums of two squares.

2.1 Fermat's Theorem on sums of two squares

Fermat's Theorem on sums of two squares states that if $p = 4k + 1$ is a prime number, it can be expressed as the sum of two squares. Euler succeeded in proving Fermat's theorem on sums of two squares in 1749 with such propositions:

(i) *if a number which is a sum of two squares is divisible by a prime which is a sum of two squares, then the quotient is a sum of two squares*;

(ii) *if a number which can be written as a sum of two squares is divisible by a number which is not a sum of two squares, then the quotient has a factor which is not a sum of two squares.*

In addition, formula (Sum of Squares Function, see [3]) for number of representations of a natural

$$t = 2^{a_0} q_1^{2a_1} \dots q_r^{2a_r} p_1^{b_1} \dots p_s^{b_s},$$

where the q_i are primes of the form $4k + 3$ and the p_j are primes of the form $4k + 1$, as the sum of two squares, ignoring order and signs, is

$$r_2(t) = \begin{cases} 0 & \text{if any } a_i \text{ is a half-integer} \\ \frac{1}{2}B & \text{if all } a_i \text{ are integer and } B \text{ is even} \\ \frac{1}{2}(B - (-1)^{a_0}) & \text{if all } a_i \text{ are integer and } B \text{ is odd} \end{cases}$$

$$B = (b_1 + 1)(b_2 + 1) \dots (b_s + 1)$$

Accordingly, representation as sum of two squares is unique for any prime $4k+1$ and any prime $4k+3$ is not sum of two squares.

Remark 1. *B. M. Bredihin proved the infinitude of primes of the form $x^2 + y^2 + 1$.*

2.2 Theorem

Theorem. *There exists a quadratic polynomial, which represents infinitely many prime numbers.*

Proof. If range of $x^2 + 1$ or $x^2 + (x - 1)^2$ contains infinitely many primes, we have done. Otherwise, assume the contrary: there exists natural N that for any natural number $n > N$ none of the numbers $n^2 + 1, n^2 + (n - 1)^2$ are primes.

If $p = 4k+1$ is a prime number, then there must be natural m such that m^2+1 is divisible by p (we can see this by Euler's criterion or via Lagrange's approach with quadratic forms). Thus, for $p = 4k+1 > N$ we have that

$$p = t^2 + l^2,$$
$$m^2 + 1 = (v^2 + w^2)(t^2 + l^2),$$

where $t, l > 1$, $t - l > 1$ and $v^2 + w^2 > 1$ by the assumption.

Diophantus/Brahmagupta–Fibonacci Identity says that the product of two sums of two squares is itself a sum of two squares. Namely,

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2,$$

where, without loss of generality, $a \geq b \geq 0$, $c \geq d \geq 0$.

Observe:

(1) If $c, d > 1$, then $ad + bc, ac + bd > 1$.
(2) If $c, d > 1$ and $b = 0$, then $ac - bd = ac, ad - bc = ad > 1$.
(3) If $b \neq 0$, $c, d > 1$ and $(c - d) > 1$, then $ac - bd = b(c - d) + (a - b)c > 1$.
(4) If $b \neq 0$, then $|ad - bc| = |b(d - c) + (a - b)d|$ *can possibly be one*.

Notice that c, d is relatively prime. Given relatively prime integers c, d, there are integers a, b such that $ad - bc = 1$, as there are integers s, t that $1 = sc + td$ (the Euclidean algorithm). Thus, $a := t, b := -s$.

It is well-known that there exist infinitely many integers m such that m^2+1 is either prime or the product of two primes. Thus, by the assumption it is the product of two primes (Sum of two squares theorem is notable here and the case $(4k+3)^2 = m^2+1$ is impossible). We notice that conditions $a,b,c,d>1$ with $c-d>1$ and $a-b>1$ for $p_1 = a^2+b^2$ and $p_2 = c^2+d^2$, where $m^2+1 = p_1p_2$, mean that, according to the observations on the previous page, $ad-bc=1$. Note here that $r_2(m^2+1 = p_1p_2) = 2$ then and Brahmagupta–Fibonacci Identity yields all cases for Sum of Squares Function.

If one of the primes is always bounded, then from Bezout's lemma we know that all solutions of $ad-bc=1$ for fixed natural a,b can be represented in the form $(d+kb, c+ka)$, where k is an arbitrary integer, i.e. infinite number of primes under consideration satisfy finitely many certain linear patterns. In particular, there exist a,b with corresponding c,d that

$$(d+kb)^2+(c+ka)^2 = (c^2+d^2)+(2ac+2db)k+(a^2+b^2)k^2$$

are primes for infinitely many k.

Otherwise, according to the first lines of the page we always have relation $ad-bc=1$ between two primes $p_1 = a^2+b^2$ and $p_2 = c^2+d^2$ in all sufficiently big $m^2+1 = p_1p_2$, i.e. we have come to an analogy of the so-called Hyperbolic Prime Number Theorem, which established upper and lower bounds for the number of primes $p = a^2+b^2+c^2+d^2$ up to x with the hyperbolic condition $ad-bc=1$.$_\bigtriangledown$

Remark 2. *Semisubgroups of $SL_2(\mathbb{Z})$?*

$$SL_2(\mathbb{Z}) = \{2-by-2 \text{ integer matrices with determinant } 1\}$$

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}^n = \begin{pmatrix}1&0\\n&1\end{pmatrix}$$

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}^{n-1}\begin{pmatrix}1&1\\0&1\end{pmatrix} = \begin{pmatrix}1&1\\n-1&n\end{pmatrix}$$

$$Matrices \begin{pmatrix}1&0\\1&1\end{pmatrix} and \begin{pmatrix}1&1\\0&1\end{pmatrix} have infinite order$$

For any $p = c^2+d^2$ there exist pair of integers a,b such that $ad-bc=1$, i.e.

$$p \Rightarrow \begin{pmatrix}a&b\\c&d\end{pmatrix}$$

On the other hand, a matrix $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ corresponds to $(ac+bd)^2+(ad-bc)^2 = (ac+bd)^2+1$.

Notice that the Semigroup Membership problem is decidable for 2-by-2 integer matrices with non-zero determinant (I. Potapov and P. Semukhin).

Remark 3. *Euler's $6k+1$ theorem states that every prime of the form $6k+1$ can be written in the form x^2+3y^2 with x and y positive integers (every prime number other than 2 and 3 is of the form $6k\pm1$). A prime dividing n^2+n+1 can only be 3 or of the form $6k+1$.*

Remark 4. *All primes appear as factor on the three polynomials: $x^2+1, 2x^2+1, 2x^2-1$. All primes of $2x^2-1$ are of the form $8k+1$ or $8k+7$.*

2.3 Generalization

2.3.1 Waring's problem

Waring's problem asks whether each natural number k has an associated positive integer s such that every natural number is the sum of at most s natural numbers raised to the power k. For every k let $g(k)$ denote the minimum number s of kth powers of naturals needed to represent all positive integers. It has been determined that $g(k) < \infty$. For example, every natural is sum of at most 4 squares, 9 cubes, or 19 fourth powers.

Remark 5. *From* [4] *it is known that for each odd natural* n *there exist non-negative integers* x, y, z *such that* $n = x^2 + y^2 + 2z^2$. *Moreover, it is not possible to represent any natural number in the manner* $ax^2 + by^2$ *with* $1 \leq a \leq b$.

Remark 6. *Notice that all numbers of the form* $2(4^m), 6(4^m)$ *or* $14(4^m)$ *cannot be represented as a sum of four non-zero squares. Moreover,* $2(4^m), 6(4^m)$ *and* $14(4^m)$ *have only one representation as a sum of four squares. Is* $2(4^m) + 2$ *a sum of two primes in the form* $4k + 1$*?*

2.3.2 Goldbach–Linnik type and Waring–Goldbach type problems

Goldbach's conjecture is one of the oldest and best-known unsolved problems in number theory and all of mathematics. It states that every even natural number greater than 2 is the sum of two prime numbers, as Goldbach was following the now-abandoned convention of considering 1 to be a prime number.

It is known that the set of even integers that are not the sum of two primes has density zero. Olivier Ramare showed that every even number is sum of at most six primes and Terence Tao indicated that every odd integer is a sum of at most five primes. Moreover, it was exhibited by Yuri Linnik that every sufficiently large integer can be represented as the sum of two primes and K powers of two, where K is an absolute number ($K = 13$ is acceptable).

Furthermore, all sufficiently large odd integers can be represented in the form $n = p_1 + p_2^2 + p_3^3 + p_4^4 + p_5^5$, where $p_i, i = 1, \ldots, 5$ are primes. Additionally, every sufficiently large integer congruent to 14 modulo 240 may be written as the sum of 14 fourth powers of prime numbers. And every sufficiently large odd integer may be written as the sum of 21 fifth powers of prime numbers. Besides, every sufficient large odd integer is a sum of one prime, two squares of primes and 31 powers of two.

Remark 7. *It is worth bringing up here Yitang Zhang and Polymath Project collaborative result: there are infinitely many prime gaps (a prime gap is the difference between two successive prime numbers) that do not exceed some constant (246 can be taken).*

2.3.3 Cubes and Fourth Powers

Which primes are sums of two cubes? The prime 2 and primes of the form $3x^2 - 3x + 1$ for some integer x. However, there are infinitely many primes of the form $x^3 + 2y^3$. Moreover, $\Omega(n^{0.9})$ of the numbers from 1 to n have representations as sums of three cubes of non-negative integers. And it is conjectured that every sufficiently large natural number can be represented as a sum of four cubes of natural numbers. So, is the Conjecture true for $f(x) = x^3$?

It is important problem to determine whether there are infinitely many prime numbers, which are represented in the form $p = a^4 + b^4$. However, we know that $\Omega(n^{0.8})$ of the numbers from 1 to n have representations as sums of four fourth powers.

Remark 8. *Notice that some probabilistic models suggest that the sums of four fourth powers, and more generally sums of* k *perfect* k*th powers for* $k \geq 3$*, should have positive natural density. In particular the gaps between these numbers are conjectured to have bounded average size.*

3 Useful observations

3.1 Complete and subcomplete sequences

Given a sequence S of positive integers, let $P(S)$ be the set of numbers which can be represented as the sum of a finite subsequence of S. Then S is complete if $\mathbb{N} \setminus P(S)$ is finite, and subcomplete if there are positive integers m and n such that $\{mk + n,\ k \in \mathbb{N}\} \subset P(S)$.

Roth & Szekeres [5] and Graham [6] showed that if a polynomial f with real coefficients maps integers to integers, a necessary and sufficient condition for the range of f to be complete is that the leading coefficient is positive and for any prime p there exist an integer n such that p does not divide $f(n)$.

Any integer-valued polynomial $f(x) = a_0 + a_1 x + \cdots + a_d x^d$ can be written in the basis of binomial coefficient polynomials $f(x) = \hat{a}_0 + \hat{a}_1 \binom{x}{1} + \cdots + \hat{a}_d \binom{x}{d}$, where each $\hat{a}_i$ is an integer. As claimed in [5][6] the range of a polynomial f is complete if and only if $\hat{a}_d > 0$ and $gcd(\hat{a}_0, \hat{a}_1, \ldots, \hat{a}_d) = 1$.

Additionally, if a (rational) polynomial maps positive integers to positive integers, its image is subcomplete [5][6][7]. Szemeredi and Vu [8] showed that there is a constant c such that the following holds: any

increasing sequence $A = a_1 < a_2 < a_3 < \ldots$ satisfying $A(n) \geq cn^{1/2}$ (with $A(n) = |\{a_i \in A : a_i \leq n\}|$) for all n is subcomplete. A subcomplete sequence S is complete if and only if for all m $P(S)$ has an element in all residue classes mod m [5].

3.2 The p-adic analysis

Every polynomial with integer coefficients is 1-lipschitz mapping over the ring of p-adic integers $\mathbb{Z}_p$. It turns out that any 1-lipschitz measure-preserving transformation on $\mathbb{Z}_p$ is an isometry which induces permutations on all residue rings $\mathbb{Z}/p^k\mathbb{Z}$, $k = 1, 2, \ldots$, and vice versa. That's why measure-preserving polynomials with integer coefficients on $\mathbb{Z}_p$ are called permutation polynomials. See for details [9][10]. Even more, a polynomial f with integer coefficients induces a measure-preserving transformation on the ring of p-adic integer $\mathbb{Z}_p$ if and only if the mapping $x \to f(x) \mod p^2$ is a bijective transformation on residue ring $\mathbb{Z}/p^2\mathbb{Z}$ [9].

A permutation polynomial f is called ergodic polynomial on $\mathbb{Z}_p$ if the mapping $x \to f(x) \mod p^k$ is transitive modulo p^k for all $k = 1, 2, \ldots$, where transitivity modulo p^k means that this permutation $x \to f(x) \mod p^k$ on residue ring $\mathbb{Z}/p^k\mathbb{Z}$ has only one cycle of length p^k. It is known that f is ergodic if and only if it is transitive modulo p^3, see [9].

Obviously, if a polynomial f is a permutation polynomial on $\mathbb{Z}_p$, then polynomial $f + c$ is also a permutation polynomial on $\mathbb{Z}_p$ for any integer c. However, a linear polynomial from the Dirichlet's theorem is not always measure-preserving, see [9]. And $gcd(\hat{a}_0, \hat{a}_1, \ldots, \hat{a}_d) = 1$ is not always true for permutation polynomials, see [9].

Additionally, it seems that general case, an ordinary polynomials, can be considered as deviation from permutation polynomials by meaning that not whole $\mathbb{Z}_p$, but some ball of non-zero radius in it is in the range. Paper [11] studies the topological structure of polynomial mappings over the ring of p-adic integers.

3.3 Friedlander–Iwaniec theorem

It states that there are infinitely many prime numbers of the form $a^2 + b^4$, see [12]. Moreover, [13] proves that there exist infinitely many integers n such that $n^2 + 1$ is either prime or the product of two primes. The last implies that one prime factor p of $m^2 + 1$ is strictly smaller than m, and therefore also divisor of (the usually much smaller) $\hat{m}^2 + 1$, where $\hat{m} = m \mod p$.

For an arbitrary polynomial f that is irreducible and doesn't have a fixed prime divisor, one can say that f represents infinitely many elements with at most $1 + deg(f)$ factors.

References

[1] V. Bunyakovsky, *Sur les diviseurs numeriques invariables des fonctions rationnelles entieres*, Mémoires de l'Académie impériale des sciences de St.-Pétersbourg, **6**, 1857, 305–329.

[2] A. Schinzel and W. Sierpinski, *Sur certaines hypotheses concernant les nombres premiers*, Acta Arithmetica, **4**, 1958, 185–208.

[3] A. Beiler, *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains*, New York: Dover, 1966.

[4] L. Panaitopol, *On the Representation of Natural Numbers as Sums of Squares*, The American Mathematical Monthly, **112** : 2, 2005, 168–171.

[5] K. Roth and G. Szekeres, *Some asymptotic formulae in the theory of partitions*, The Quarterly Journal of Mathematics, **5**, 1954, 241–259.

[6] R. Graham, *Complete sequences of polynomial values*, Duke Mathematical Journal, **31**, 1964, 275–285.

[7] S. Burr, *On the completeness of sequences of perturbed polynomial values*, Pacific Journal of Mathematics, **85** : 2, 1979, 355–360.

[8] E. Szemeredi and V. Vu, *Finite and infinite arithmetic progressions in sumsets*, Annals of Mathematics, **163** : 1, 2006, 1–35.

[9] V. Anashin and A. Khrennikov, *Applied algebraic dynamics*, de Gruyter Expositions in Mathematics, Berlin, 2009.

[10] R. Rivest, *Permutation Polynomials Modulo* 2^w, Finite Fields and Their Applications, **4**, 1999, 287–292.

[11] M. Zieve and D. desJardins, *Polynomial Mappings mod* p^n, arXiv:math/0103046, 2001.

[12] J. Friedlander and H. Iwaniec, *Using a parity-sensitive sieve to count prime values of a polynomial*, Proceedings of the National Academy of Sciences of the United States of America, **94** : 4, 1997, 1054–1058.

[13] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Inventiones mathematicae, **47**, 1978, 171–188.