

Albertas Zinevičius

Sums of two integer squares in a certain quartic extension

Archivum Mathematicum, Vol. 62 (2026), No. 2, 69–73

Persistent URL: <http://dml.cz/dmlcz/153667>

Terms of use:

© Masaryk University, 2026

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

SUMS OF TWO INTEGER SQUARES IN A CERTAIN QUARTIC EXTENSION

ALBERTAS ZINEVIČIUS

ABSTRACT. An example of a quartic extension of the rational number field that does not have quadratic subfields and there exists a set of rational prime numbers $p \equiv 3 \pmod{4}$ of positive Dirichlet density such that either p or $31p$ is a sum of two squares of integers of the extension is given.

1. INTRODUCTION

In [11] it was proved that, given a number field K , there is a set of rational prime numbers of positive Dirichlet density that are not sums of two cubes of integers of K . In comparison, every rational integer is a sum of two squares of Gaussian integers (sums of two integer squares in quadratic extensions have been studied, for example, in [7] and [9]). In fact if $K = \mathbb{Q}(\sqrt{-D})$ (where D is a square-free positive integer) is any other imaginary quadratic extension there exists a nonzero constant a such that the set of rational prime numbers $p \equiv 3 \pmod{4}$ for which ap is a sum of two squares of integers of K has positive upper Dirichlet density. Indeed consider the Galois group $\text{Gal}(H(K(i))/\mathbb{Q})$ of the Hilbert class field $H(K(i))$ of $K(i)$. If the Frobenius automorphism of some prime ideal in $H(K(i))$ above the rational prime ideal (p) is in the division of the complex conjugation automorphism then (p) is inert in extensions $K, \mathbb{Q}(i)$ and has a principal prime ideal factor $(x + yi)$ of degree 2 in $K(i)$ where $2x, 2y$ are some integers of K . Therefore the ideal (p) is equal to $(x^2 + y^2)$ and since the only roots of unity in K are ± 1 (or the sixth roots of unity in the case $D = 3$), either $4p$ or $4Dp$ is a sum of two integer squares. It is therefore interesting to find an example of an extension K that has the aforementioned property and does not contain any quadratic subfield.

Theorem 1.1. *The quartic extension generated by a root of the polynomial $x^4 - 3x^3 + 3x^2 + 2x + 1$ does not have quadratic subfields. There exists a set of rational prime numbers $p \equiv 3 \pmod{4}$ of positive Dirichlet density such that either p or $31p$ is a sum of two squares of integers of the extension.*

Notice that a related question was discussed in [1].

The following theorems will be used in the proof:

2020 *Mathematics Subject Classification*: primary 11R37; secondary 11D09.

Key words and phrases: Sums of two integer squares, quartic number field.

Received October 22, 2025. Editor R. Kučera.

DOI: 10.5817/AM2026-2-69

Lemma 1.2 (Existence of Hilbert class field). [2, p. 153] *If K is a number field, there exists a unique abelian extension $H(K)$ of K with the Galois group isomorphic to the class group of K such that no prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ ramifies in $H(K)/K$ and no injective ring homomorphism $\sigma: K \rightarrow \mathbb{R}$ extends to an injective ring homomorphism $\sigma: H(K) \rightarrow \mathbb{C}$ with $\sigma(H(K)) \not\subset \mathbb{R}$. It has the property that a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ splits completely in $H(K)/K$ if and only if it is principal.*

Definition 1.3. If G is a finite group and $\sigma \in G$, the *division* of σ is the set of all elements of G that are conjugate to σ^m for some $m \in \mathbb{N}$ that is coprime to the order of σ .

Lemma 1.4 (Frobenius density theorem). [3, p. 134] *If L/K is a Galois extension of number fields and $\sigma \in \text{Gal}(L/K)$, the Dirichlet density of the set of prime ideals of $\mathcal{O}_K$ that are divisible by a prime ideal of $\mathcal{O}_L$ such that its Frobenius automorphism is in the division of σ , is equal to the number of elements in the division of σ divided by the number of elements of $\text{Gal}(L/K)$.*

Lemma 1.5. [3, p. 101] *If $K \subset L \subset M$ are number fields such that M/K is Galois, the decomposition type of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ in L that is not ramified in M/K is the same as the cycle structure of the permutation of (left) cosets of $\text{Gal}(M/K) \setminus \text{Gal}(M/L)$ induced by the Frobenius automorphism of any prime ideal $\mathfrak{q} \subset \mathcal{O}_M$ above $\mathfrak{p}$.*

Lemma 1.6. [8, p. 202] *If $K \subset L \subset M$ are number fields, then the discriminant ideals are related by*

$$\mathfrak{d}_{M/K} = \mathfrak{d}_{L/K}^{[M:L]} \text{Nm}_{L/K} \mathfrak{d}_{M/L}.$$

Lemma 1.7. [8, p. 202] *A prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ ramifies in the extension L/K of number fields if and only if it divides the discriminant ideal $\mathfrak{d}_{L/K}$.*

Lemma 1.8. [6, p. 68] *A prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ divides the discriminant ideal $\mathfrak{d}_{L/K}$ if and only if it divides the discriminant ideal of the Galois closure of L over K .*

2. AUXILIARY CALCULATIONS

Denote $f(x) = x^4 - 3x^3 + 3x^2 + 2x + 1 \in \mathbb{Q}[x]$. Notice that

$$f(x) \equiv (x-1)(x^3+x+1) \pmod{2},$$

$$(2.1) \quad f(x) \equiv (x^2+x+1)^2 \pmod{5}.$$

Therefore $f(x)$ is irreducible. The discriminant of f is $\text{disc}(f) = 5^2 13^2$. Denote by u a root of $f(x)$ and denote by K the field extension $\mathbb{Q}(u)$.

Notice that u is a unit. Further, $(u^2 + u + 1)^2 = 5u^3$, therefore the ideal (5) ramifies in the ring of integers $\mathcal{O}_K$. It follows that 5^2 divides the discriminant $d_{K/\mathbb{Q}}$ of the extension $K/\mathbb{Q}$. 13^2 must also divide $d_{K/\mathbb{Q}}$ since otherwise [4, p. 63] Minkowski bound would be less than 1. Therefore $\text{disc}(f) = d_{K/\mathbb{Q}}$. Consequently, $1, u, u^2, u^3$ is a basis of $\mathcal{O}_K$ as a $\mathbb{Z}$ -module.

Since 2 does not divide $\text{disc}(f)$, it follows from [4, p. 55] that the ideal (2) factorizes as $(2, u-1)(2, u^3+u+1)$ in $\mathcal{O}_K$. Therefore the extension $K/\mathbb{Q}$ is not Galois and the degree of its Galois closure is divisible by 3. On the other hand, $\text{disc}(f)$ is a square, therefore the Galois group of f must be a subgroup of the alternating group A_4 [5, p. 47]. Consequently, it must be A_4 . Therefore K does not have nontrivial subfields. In particular, the only roots of unity in K are ± 1 . Since the polynomial f does not have real roots, the unit group of $\mathcal{O}_K$ has rank 1, as follows from the Dirichlet unit theorem.

Lemma 2.1. *$u, -u$ are not squares in $\mathcal{O}_K$.*

Proof. If $u = \beta^2$ for some $\beta \in \mathcal{O}_K$, then $f(\beta^2) = 0$. Therefore $f(x^2)$ must be divisible by the minimal polynomial of β of degree 4. However

$$f(x^2) \equiv (x^6 - x^4 + x^2 + 1)(x^2 + 1) \pmod{3}$$

and the polynomial $x^6 - x^4 + x^2 + 1 \in \mathbb{F}_3[x]$ is irreducible. Contradiction. Therefore u is not a square in $\mathcal{O}_K$.

If $-u = \beta^2$ for some $\beta \in \mathcal{O}_K$, then $f(-\beta^2) = 0$. Therefore $f(-x^2)$ must be divisible by the minimal polynomial of β of degree 4. However

$$f(-x^2) \equiv (x^6 - x^4 - 4x^2 + 3)(x^2 + 4) \pmod{11}$$

and the polynomial $x^6 - x^4 - 4x^2 + 3 \in \mathbb{F}_{11}[x]$ is irreducible. Contradiction. Therefore $-u$ is not a square in $\mathcal{O}_K$. $\square$

Lemma 2.2. *The ring of integers of $K(i)$ is $\mathcal{O}_K[i]$.*

Proof. $\mathfrak{d}_{K(i)/K}$ divides $(d_{K(i)/K}(1, i)) = (-4)$. Therefore from lemma 1.6,

$$\mathfrak{d}_{K(i)/\mathbb{Q}} = \mathfrak{d}_{K/\mathbb{Q}}^{[K(i):K]} \text{Nm}_{K/\mathbb{Q}} \mathfrak{d}_{K(i)/K} = (5^4 13^4 2^e)$$

for some nonnegative integer $e \leq 8$. On the other hand,

$$\mathfrak{d}_{K(i)/\mathbb{Q}} = \mathfrak{d}_{\mathbb{Q}(i)/\mathbb{Q}}^{[K(i):\mathbb{Q}(i)]} \text{Nm}_{\mathbb{Q}(i)/\mathbb{Q}} \mathfrak{d}_{K(i)/\mathbb{Q}(i)} = (-4)^4 \text{Nm}_{\mathbb{Q}(i)/\mathbb{Q}} \mathfrak{d}_{K(i)/\mathbb{Q}(i)}.$$

Therefore $e = 8$. Since $5^4 13^4 2^8 = d_{K(i)/\mathbb{Q}}(1, u, u^2, u^3, i, ui, u^2i, u^3i)$, the ring of integers of $K(i)$ must be $\mathbb{Z} + \mathbb{Z}u + \mathbb{Z}u^2 + \mathbb{Z}u^3 + \mathbb{Z}i + \mathbb{Z}ui + \mathbb{Z}u^2i + \mathbb{Z}u^3i = \mathcal{O}_K[i]$. $\square$

3. PROOF OF THE THEOREM

From lemma 1.7 it follows that the prime ideal $(31) \subset \mathbb{Z}$ does not ramify in the Hilbert class field $H(K(i))$ of $K(i)$. From lemma 1.8, the ideal (31) does not ramify in the Galois closure M (with respect to the base field $\mathbb{Q}$) of $H(K(i))$.

The polynomial $f(x)$ has no root modulo 31. On the other hand,

$$(3.1) \quad -31u = (2u^2 - 6u - 3)(2u^3 - 6u^2 + 9u + 4)$$

and $\text{Nm}_{K/\mathbb{Q}}(2u^2 - 6u - 3) = 31^2$. Consequently the ideals $\mathfrak{p}_1 = (2u^2 - 6u - 3)$, $\mathfrak{p}_2 = (2u^3 - 6u^2 + 9u + 4)$ are prime, of degree 2. Since

$$(3.2) \quad 2u^3 - 6u^2 + 9u + 4 = (u^3 - 3u^2 + 2u + 2)^2 + 1^2,$$

$$(3.3) \quad 2u^3 - 6u^2 - 3u = (2u^2 - 1)^2 + (u^3 - u^2 - 2u)^2,$$

the prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ split completely into a product of principal ideals in the extension $K(i)/K$. From lemma 1.2 it follows that the factors split completely in the extension $H(K(i))/K(i)$. Therefore (31) splits into a product of ideals of degree 2 in $H(K(i))$.

Denote by $\mathfrak{q}$ any prime factor of (31) in $\mathcal{O}_M$ and denote by $\sigma \in \text{Gal}(M/\mathbb{Q})$ the Frobenius automorphism of $\mathfrak{q}$. It follows from lemma 1.5 that the permutation of $\text{Gal}(M/\mathbb{Q}) \setminus \text{Gal}(M/L)$ induced by σ is a product of disjoint 2-cycles when L is $\mathbb{Q}(i), K, K(i), H(K(i))$. Since the restriction of σ to $\mathbb{Q}(i)$ is the Frobenius automorphism of $\mathfrak{q} \cap \mathcal{O}_{\mathbb{Q}(i)}$, and since (31) is inert in $\mathbb{Q}(i)$, the order of $\sigma|_{\mathbb{Q}(i)}$ is 2. Therefore the order of σ in $\text{Gal}(M/\mathbb{Q})$ is even. Denote by m any positive integer that is coprime to the order of σ . Then m is odd.

If $\tau \text{Gal}(M/L), \sigma\tau \text{Gal}(M/L)$ is a 2-cycle induced by σ , then $\sigma^2\tau \text{Gal}(M/L) = \tau \text{Gal}(M/L)$. Consequently, $\sigma^m\tau \text{Gal}(M/L) = \sigma\tau \text{Gal}(M/L)$ and $(\sigma^m)^2\tau \text{Gal}(M/L) = \tau \text{Gal}(M/L)$. Therefore the permutation of $\text{Gal}(M/\mathbb{Q}) \setminus \text{Gal}(M/L)$ induced by σ^m is the product of the same disjoint 2-cycles as is the permutation induced by σ . Therefore any prime ideal $(p) \subset \mathbb{Z}$ (generated by a prime number $p > 0$) that is not ramified in $M/\mathbb{Q}$ and has a prime ideal factor in $\mathcal{O}_M$ with Frobenius automorphism σ^m is a product of prime ideals of degree 2 in $\mathcal{O}_{\mathbb{Q}(i)}, \mathcal{O}_K, \mathcal{O}_{K(i)}, \mathcal{O}_{H(K(i))}$. If (p) has a prime ideal factor with Frobenius automorphism conjugate to σ^m , then it also has a prime ideal factor with Frobenius automorphism σ^m [4, p. 134]. Therefore every prime ideal $(p) \subset \mathbb{Z}$ that is not ramified in $M/\mathbb{Q}$ and has a prime ideal factor with Frobenius automorphism in the division of σ is a product of prime ideals of degree 2 in $\mathcal{O}_{\mathbb{Q}(i)}, \mathcal{O}_K, \mathcal{O}_{K(i)}, \mathcal{O}_{H(K(i))}$. In particular, (p) is inert in $\mathbb{Q}(i)/\mathbb{Q}$, therefore $p \equiv 3 \pmod{4}$. It follows from lemma 1.4 that the Dirichlet density of such (p) is positive. The prime ideal factors of (p) in $K(i)$ split completely in the extension $H(K(i))/K(i)$ and therefore must be principal ideals. Moreover, they form two pairs of ideals that are conjugate by an element of $\text{Gal}(K(i)/K)$. By lemma 2.2, the ideals of such pair are of the form $(\beta_1 + i\beta_2), (\beta_1 - i\beta_2)$ for some $\beta_1, \beta_2 \in \mathcal{O}_K$. Therefore the prime ideals of $\mathcal{O}_K$ above (p) are of the form $(\beta_1^2 + \beta_2^2)$. Since the product of sums of two squares is a sum of two squares, we must have

$$p = \epsilon(\alpha_1^2 + \alpha_2^2)$$

for some $\alpha_1, \alpha_2 \in \mathcal{O}_K$ and $\epsilon \in \mathcal{O}_K^\times$. Since the unit group of $\mathcal{O}_K$ has rank 1 and the only roots of unity in K are ± 1 , there exists a unit $u_0 \in \mathcal{O}_K$ such that every unit is of the form $\pm u_0^l$ for some integer l . From lemma 2.1,

$$u = \pm u_0^l$$

for some odd integer l . Since

$$(2u)^2 + (1 + u - u^2)^2 = u^3,$$

u is a sum of two squares. Therefore either u_0 or $-u_0$ is a sum of two squares. Consequently either p or $-p$ is a sum of two squares in $\mathcal{O}_K$.

It follows from equations 3.1, 3.2, 3.3 that $-31u$ is a sum of two squares and therefore -31 is a sum of two squares. Therefore if p is not a sum of two squares then $-p \cdot (-31)$ is.

Acknowledgements. We used computer to generate the example. In particular, we are thankful to SageMath [10] for some of the computations. We are also thankful to the anonymous referee for their remarks and the short proof of lemma 2.1.

REFERENCES

- [1] *Sums of two squares in (certain) integral domains*, <https://mathoverflow.net/questions/30998/>, 2010, Last accessed 6 May, 2026.
- [2] Childress, N., *Class field theory*, Springer, 2009.
- [3] Janusz, G. J., *Algebraic number fields*, Academic Press, 1973.
- [4] Milne, J. S., *Algebraic number theory*, Version 3.03, jmilne.org, 2011.
- [5] Milne, J. S., *Fields and galois theory*, Version 4.60, jmilne.org, 2018.
- [6] Murty, R., Esmonde, J., *Problems in algebraic number theory*, 2 ed., Springer, 2005.
- [7] Nagell, T., *On the sum of two integral squares in certain quadratic fields*, Ark. Mat. **4** (1961), 267–286.
- [8] Neukirch, J., *Algebraic number theory*, Springer-Verlag Berlin Heidelberg, 1999.
- [9] Niven, I., *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. **48** (1940), 405–417.
- [10] SageMath, *Version 9.2*, Online, 2020, Available at: <https://www.sagemath.org/>.
- [11] Zinevičius, A., *Non-sums of two cubes of algebraic integers*, Colloq. Math. **163** (2021), 285–293.

FACULTY OF MATHEMATICS AND INFORMATICS, VILNIUS UNIVERSITY,
 NAUGARDUKO 24, VILNIUS, LT – 03225, LITHUANIA
E-mail: albertas.zinevicius@mif.vu.lt