A Quixotic Proof of Fermat’s Two Squares Theorem for Prime Numbers

Roland Bacher

Abstract. Every odd prime number $p$ has exactly $(p + 1)/2$ different expressions as a sum $ab + cd$ of two ordered products $ab$ and $cd$ such that $\min(a, b) > \max(c, d)$. An easy corollary is a proof of Fermat’s Theorem expressing primes in $1 + 4\mathbb{N}$ as sums of two squares.

1. INTRODUCTION.

Theorem 1. For every odd prime number $p$ there exist exactly $(p + 1)/2$ sequences $(a, b, c, d)$ of four elements in the set $\mathbb{N} = \{0, 1, 2, \ldots\}$ of nonnegative integers such that $p = ab + cd$ and $\min(a, b) > \max(c, d)$.

As a consequence of this theorem we obtain a new proof of an old result first observed by Albert Girard (1595–1632) around 1625. He noted that the set of integers which are sums of two squares is the subset of $\mathbb{N}$ which is closed under multiplication, contains all squares, 2, and all primes in $1 + 4\mathbb{N}$. A refined statement including multiplicities was written in 1640 by Pierre Fermat (1607–1665) in a letter addressed to Marin Mersenne (1588–1648). The old rascal did not want to spoil his margins and left the proof to Leonhard Euler (1707–1783) who had no such qualms. Euler laid out the proof in a series of letters and publications dated around 1750. More historical details can be found, for example, in the entry “Fermat’s theorem on sums of two squares” in [12].

Corollary 2. Every prime number in $1 + 4\mathbb{N}$ is a sum of two squares.

Proof of Corollary 2. If $p$ is a prime number congruent to 1 (mod 4), the number $(p + 1)/2$ of solutions $(a, b, c, d)$ defined by Theorem 1 is odd. The involution $(a, b, c, d) \mapsto (b, a, d, c)$ has therefore a fixed point $(a, a, c, c)$ expressing $p$ as a sum of two squares.

Nowadays Corollary 2 is a venerable old hat and has quite a few proofs already. Some are described in [12]. The author enjoyed the presentation of a few “elementary” proofs given in [5].

Zagier (based on unpublished notes of Heath-Brown, [8]) published a one sentence proof based on fixed points in [13]. A. Spivak gave an elementary geometric interpretation of Zagier’s proof, see [11]. A nice variation on Zagier’s proof was given by Dolan in [4]. An interesting discussion on Zagier’s proof and variations can be found in [9] which also contains a description of A. Spivak’s proof.

Grace gave a very elegant constructive proof, see [6] (essentially equivalent to the fourth proof of Theorem 366 in [7]) which we recall in Section 3 for the convenience of the reader.

Christopher, see [2], gave a proof based on the existence of a fixed point of an involution acting on suitable partitions with parts of exactly two different sizes (essentially amounting to solutions of $p = ab + cd$ without requirements of inequalities).

doi.org/10.1080/00029890.2023.2242034
MSC: 11A41
The set \( S_p \) of solutions defined by Theorem 1 is invariant under the action of Klein’s Vierergruppe \( V \) (isomorphic to the two-dimensional vector space over the field of two elements or, equivalently, isomorphic to the unique noncyclic group of four elements) with nontrivial elements acting by

\[
(a, b, c, d) \mapsto (b, a, c, d), (a, b, d, c), (b, a, d, c)
\]

(i.e., by exchanging either the first two elements, or the last two elements, or the first two and the last two elements). The following tables list all \( V \)-orbits represented by elements \((a, b, c, d)\) with \(a, b, c, d\) decreasing together with the orbit-sizes \(\sharp(O)\) occurring in the sets \(S_{29}, S_{31}, S_{37}\):

| \(a\) | \(b\) | \(c\) | \(d\) | \(\sharp(O)\) |
|------|------|------|------|----------|
| 29   | 1    | 0    | 0    | 2        |
| 14   | 2    | 1    | 1    | 2        |
| 7    | 4    | 1    | 1    | 2        |
| 9    | 3    | 2    | 1    | 4        |
| 5    | 5    | 4    | 1    | 2        |
| 5    | 5    | 2    | 2    | 1        |
| 5    | 4    | 3    | 3    | 2        |
|      |      |      |      | 15       |

| \(a\) | \(b\) | \(c\) | \(d\) | \(\sharp(O)\) |
|------|------|------|------|----------|
| 31   | 1    | 0    | 0    | 2        |
| 15   | 2    | 1    | 1    | 2        |
| 10   | 3    | 1    | 1    | 2        |
| 6    | 5    | 1    | 1    | 2        |
| 7    | 4    | 3    | 1    | 4        |
| 9    | 3    | 2    | 2    | 2        |
| 5    | 5    | 3    | 2    | 2        |
|      |      |      |      | 16       |

| \(a\) | \(b\) | \(c\) | \(d\) | \(\sharp(O)\) |
|------|------|------|------|----------|
| 37   | 1    | 0    | 0    | 2        |
| 18   | 2    | 1    | 1    | 2        |
| 12   | 3    | 1    | 1    | 2        |
| 9    | 4    | 1    | 1    | 2        |
| 6    | 6    | 1    | 1    | 1        |
| 7    | 5    | 2    | 1    | 4        |
| 11   | 3    | 2    | 2    | 2        |
| 7    | 4    | 3    | 3    | 2        |
| 5    | 5    | 4    | 3    | 2        |
|      |      |      |      | 19       |

Establishing complete lists \( S_p \) of solutions for small primes is a rather pleasant pastime and rates among the author’s more confessable procrastinations.

A solution \( p = ab + cd \) in \( S_p \) can be visualized as a lattice-tiling with a fundamental domain given by the union of two rectangles of size \(a \times b\) and \(d \times c\), aligned as in Figure 1. The resulting tiling is invariant by translations in \(\mathbb{Z}(a, c) + \mathbb{Z}(-d, b)\). Klein’s Vierergruppe \( V \) acts on the set of all such tilings by quarter-turns on rectangles. Tilings associated to \( V \)-invariant solutions correspond to the case where both rectangles are squares.

A rough sketch for proving Theorem 1 goes along the following lines: Every solution \( p = ab + cd \) in \( S_p \) can be encoded by two vectors \( u = (a, c) \), \( v = (-d, b) \) generating a sublattice \( \mathbb{Z}u + \mathbb{Z}v \) of index \( p \) in \( \mathbb{Z}^2 \), see above and Figure 1. It is therefore enough to understand the number of solutions encoded by every sublattice of index \( p \) in \( \mathbb{Z}^2 \). Sublattices of index \( p \) in \( \mathbb{Z}^2 \) are in one-to-one correspondence with all \( p + 1 \) elements of the projective line \( \mathbb{P}_p \cup \{\infty\} \) over the finite field \( \mathbb{F}_p \). An element \( \mu \) encoding the slope \( \mu = \frac{b}{a} \) of \([a : b]\) (using the obvious convention for \( \mu = \infty \))
defines the sublattice $\Lambda_\mu(p) = \{(x, y) \in \mathbb{Z}^2 \mid ax + by \equiv 0 \pmod{p}\}$ of index $p$ in $\mathbb{Z}^2$. The two lattices $\Lambda_0(p) = \mathbb{Z}(p, 0) + \mathbb{Z}(0, 1)$ and $\Lambda_\infty(p) = \mathbb{Z}(1, 0) + \mathbb{Z}(0, p)$ with singular slopes $0, \infty \notin \mathbb{F}_p^*$ give rise to the two degenerate solutions $p \cdot 1 + 0 \cdot 0$ and $1 \cdot p + 0 \cdot 0$. All other solutions $p = ab + cd$ correspond to sublattices of index $p$ in $\mathbb{Z}^2$ generated by $u = (a, c)$ in the open cone delimited by $y = 0$ and $x = y$ (opening up in E-NE directions) and by $v = (-d, c)$ in the open cone delimited by $x = 0$ and $y = -x$ (opening up in N-NW directions). The two lattices $\Lambda_1(p)$ and $\Lambda_{-1}(p)$ with self-inverse slopes 1 and $-1$ have no such bases and thus do not correspond to a solution. Exactly one lattice in every pair of distinct lattices $\Lambda_\mu(p), \Lambda_{-\mu}(p)$ with mutually inverse slopes $\mu, \mu^{-1} \in \mathbb{F}_p^* \setminus \{1, -1\}$ has bases with generators in the two open E-NE and N-NW cones. We show then that exactly one of these bases corresponds to a solution in $S_p$. **Theorem 1** follows now easily.

Coloring the set $\{(x, y) \mid xy(x - y)(x + y) > 0\}$ consisting of the four open E-NE, N-NW, W-SW and S-SE cones and their opposites in black, we get a picture of the four sails of an old windmill, see Figure 2. We therefore prove **Theorem 1** by following in Don Quixote’s heroic footsteps (see the beginning of Chapter 8 in [1]). Cervantes forgot of course the explicit statement of **Theorem 1** and botched the proof by sweeping all those bloody details under the rug.

The author’s serendipitous encounter with Don Quixote happened as follows: Euclid’s algorithm applied to square-matrices of size 2 (replacing iteratively a row/column by itself minus the other row/column) with entries in the set $\{0, 1, \ldots\}$ of nonnegative integers yields a set

$$\left\{ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \mid ad - bc = n, \min(a, d) > \max(b, c), \ a, b, c, d \in \{0, 1, 2, \ldots\}\right\}$$

of

$$\sum_{d|n, d^2 \geq n} \left(d + 1 - \frac{n}{d}\right)$$

"irreducible"matrices of given determinant $n \geq 1$, see [10].

A sign-change made out of curiosity in a naive program checking Formula (1) for small values of $n$ suggested **Theorem 1**.

A final additional Section links solutions occurring in **Theorem 1** with geometric properties of the corresponding lattices.

2. A FEW REMINDERS ON LATTICES IN $\mathbb{R}^2$. This short Section contains a few well-known results on lattices in $\mathbb{R}^2$, recalled for the convenience of the reader.

Henceforth a lattice denotes a discrete additive group $\mathbb{Z}e + \mathbb{Z}f$ generated by an arbitrary basis $e, f$ of the Euclidean vector-space $\mathbb{R}^2$ endowed with the standard scalar product $(u_x, u_y), (v_x, v_y) = u_x v_x + u_y v_y$ of two vectors in $\mathbb{R}^2$. We will mainly work with sublattices of the integral lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$.

A minimal element of a lattice $\Lambda$ is a shortest element in $\Lambda \setminus \{(0, 0)\}$.

An element $v$ of $\Lambda$ is primitive if it is not contained in $k\Lambda$ for some natural integer $k > 1$.

A basis of a lattice $\Lambda$ of rank (or dimension) 2 is a set $e, f$ of two elements in $\Lambda$ such that $\Lambda = \mathbb{Z}e + \mathbb{Z}f$.

The following result is a special case of Pick’s theorem\(^1\):

---

\(^1\)Pick’s theorem gives the area $\frac{1}{2}b + i - 1$ of a closed lattice polygon $P$ (with vertices in $\mathbb{Z}^2$) containing $b$ lattice points $\partial P \cap \mathbb{Z}^2$ in its boundary and $i$ lattice points in its interior.
**Lemma 3.** Two linearly independent elements \( e, f \) of a two-dimensional lattice \( \Lambda \) form a basis of the lattice \( \Lambda \) if and only if the triangle with vertices \((0,0), e, f\) contains no other elements of \( \Lambda \).

**Proof.** The parallelogram \( \mathcal{P} \) with vertices \((0,0), e, f, e+f\) is a fundamental domain for the sublattice \( \mathbb{Z}e + \mathbb{Z}f \) of \( \Lambda \) generated by \( e \) and \( f \). Therefore the two elements \( e, f \) generate \( \Lambda \) if and only if \( \Lambda \) intersects \( \mathcal{P} \) only in its four vertices.

Since \( \mathcal{P} \) and \( \Lambda \) are invariant under the affine involution \( x \mapsto -x + e + f \) exchanging the two triangles with vertices \((0,0), e, f, e+f\), the parallelogram \( \mathcal{P} \) intersects \( \Lambda \) exactly in its vertices if and only if the triangle defined by \((0,0), e, f\) intersects \( \Lambda \) exactly in its vertices.

**Proposition 4.** A lattice \( M \) in \( \mathbb{R}^2 \) has exactly \( p + 1 \) different sublattices of index a prime number \( p \). These sublattices are in one-to-one correspondence with the set of lines in \( M/pM \) representing all elements of the projective line over the finite field \( \mathbb{F}_p \).

**Proof.** A sublattice \( \Lambda \) of prime index \( p \) in a two-dimensional lattice \( M \) gives rise to a quotient group \( M/\Lambda \) isomorphic to the additive group \( \mathbb{Z}/p\mathbb{Z} \). Since \( pM \) is contained in the kernel of the quotient map \( M \mapsto M/\Lambda \), subgroups of index \( p \) in \( M \) are in bijection with kernels of linear surjections from the two-dimensional vector-space \( M/pM \) over \( \mathbb{F}_p \) onto \( \mathbb{F}_p \) considered as a one-dimensional vector-space. The set of all subgroups of index \( p \) in \( M \) is therefore in bijection with the set of one-dimensional subspaces in \( \mathbb{F}_p^2 \) representing all possible kernels. Such subspaces represent all \( p + 1 \) points of the projective line over \( \mathbb{F}_p \).

The Euclidean algorithm computes the positive generator of the cyclic subgroup \( \mathbb{Z}a + \mathbb{Z}b \) of \( \mathbb{Z} \) generated by two integers \( a \) and \( b \). Gaussian lattice reduction does essentially the same for lattices in the Euclidean space \( \mathbb{R}^2 \): Given two linearly independent vectors \( e, f \) in \( \mathbb{R}^2 \), the Gaussian algorithm produces a **reduced basis** \( r, s \) of the lattice \( \mathbb{Z}e + \mathbb{Z}f = \mathbb{Z}r + \mathbb{Z}s \) defining two (not necessarily unique) distinct shortest pairs \( \pm r, \pm s \) of primitive vectors. The Gaussian algorithm starts with a basis \( e, f \) of \( \Lambda = \mathbb{Z}e + \mathbb{Z}f \) and iterates the following two steps until stabilization:

- Exchange \( e \) and \( f \) if \( f \) is strictly longer than \( e \).
- Replace \( e \) by \( e + kf \) if \( e + kf \) (for \( k \) an integer) is strictly shorter than \( e \) (the optimal choice for \( k \) is given by \( k \in \mathbb{Z} \) such that \( \left| k + \frac{e}{f} \frac{f}{e} \right| \) is at most equal to \( \frac{1}{2} \)).

Finally, the following (obvious) result will also be needed a few times:

**Proposition 5.** The sublattice \( \mathbb{Z}(ae + bf) + \mathbb{Z}(ye + df) \) of a lattice \( \Lambda = \mathbb{Z}e + \mathbb{Z}f \) generated by two linearly independent vectors \( ae + bf \) and \( ye + df \) (with \( a, b, y, d \) in \( \mathbb{Z} \)) has index \( |a\delta - b\gamma| \) in \( \Lambda \).

**Proof.** The result is obvious if \( a\beta\gamma\delta = 0 \). The general case can be reduced by elementary operations on the generators \( u = ae + bf \) and \( v = ye + df \) to the obvious case.

---

\(^2\)Gaussian lattice reduction applied to two linearly dependent vectors boils down to the Euclidean algorithm.
3. GRACE’S PROOF. For the convenience of the reader, we recall Grace’s proof (of Corollary 2), as given in [7] (see the fourth proof of Theorem 366 in [7] or [6])3.

Proof. Given an odd prime number \( p \equiv 1 \pmod{4} \) we have \( ((\frac{p-1}{2})!)^2 (-1)^{(p-1)/2} \equiv (p-1)! \pmod{p} \) which equals \(-1 \pmod{p}\) by Wilson’s Theorem. For \( p \) a prime number congruent to 1 \pmod{4}, the integer \( \iota = (\frac{p-1}{2})! \) (and its opposite) is a square root of \(-1\) in the finite field \( \mathbb{F}_p \). The kernel of the homomorphism \( \mathbb{Z}^2 \ni (x, y) \mapsto x + \iota y \pmod{p} \) is a sublattice \( \Lambda \) of index \( p \) in \( \mathbb{Z}^2 \). Since \( \iota(x + \iota y) \equiv -y + \iota x \pmod{p} \), we have \( (x, y) \in \Lambda \) if and only if \((-y, x) \in \Lambda\). The lattice \( \Lambda \) is therefore invariant under quarter-turns (rotations of order 4 by \( \pm 90 \) degrees). Let \((a, b)\) be a nonzero element of minimal length in \( \Lambda \). Invariance under quarter-turns of \( \Lambda \) implies that \((-b, a)\) is also an element of \( \Lambda \). Length-minimality of \((a, b)\) and \((-b, a)\) implies that the triangle with vertices \((0, 0), (a, b), (-b, a)\) contains no other element of \( \Lambda \). Lemma 3 shows that the two vectors \((a, b)\) and \((-b, a)\) generate \( \Lambda \). Proposition 5 implies now that \(a^2 + b^2\) is equal to the index \( p \) of the sublattice \( \Lambda \) in \( \mathbb{Z}^2 \).

Grace’s proof is effective: Given a prime \( p \equiv 1 \pmod{4} \), we can use quadratic reciprocity to find a non-square \( n \pmod{p} \). We obtain a square root \( \iota \) of \(-1 \pmod{4} \) in \( \mathbb{F}_p \) by computing \( \iota \equiv n^{(p-1)/4} \pmod{p} \) using fast exponentiation. We now obtain a solution by considering an element \((a, b)\) of a reduced basis (obtained by Gaussian lattice reduction) of the lattice generated by \((p, 0)\) and \((-\iota, 1)\).

4. INTERLACEDNESS.

Definition 6. Two unordered bases \( f_1, f_2 \) and \( g_1, g_2 \) of \( \mathbb{R}^2 \) are interlaced if the vectors \( f_1, f_2, g_1, g_2 \) represent four distinct points of the real projective line such that the two projective points represented by \( f_1, f_2 \) separate the two projective points represented by \( g_1, g_2 \).

Interlacedness can be defined equivalently as follows: Color the two lines \( \mathbb{R}f_1 \) associated to the first basis \( f_1, f_2 \) fuchsia and color the two lines \( \mathbb{R}g_1 \) green. Then the set \( \mathbb{R}f_1 \cup \mathbb{R}f_2 \cup \mathbb{R}g_1 \cup \mathbb{R}g_2 \) should contain four different lines and the colors should alternate.

Example 7. The standard basis \((1, 0), (0, 1)\) of \( \mathbb{R}^2 \) is interlaced with the basis \((-1, 2), (6, 1)\). The standard basis \((1, 0), (0, 1)\) is however not interlaced with the basis \((2, 3), (-1, -1)\).

Lemma 8. Two bases \( f_1, f_2 \) and \( g_1, g_2 \) of a two-dimensional lattice \( \Lambda = \mathbb{Z}f_1 + \mathbb{Z}f_2 = \mathbb{Z}g_1 + \mathbb{Z}g_2 \) are never interlaced.

Proof. Suppose that a lattice \( \Lambda = \mathbb{Z}f_1 + \mathbb{Z}f_2 = \mathbb{Z}g_1 + \mathbb{Z}g_2 \) has two bases \( f_1, f_2 \) and \( g_1, g_2 \) which are interlaced. After replacing \( f_1 \) and \( f_2 \) by their negatives if necessary, and perhaps after exchanging \( f_1 \) with \( f_2 \), we can suppose that \( f_1 \) belongs to the open cone spanned by \( g_1 \) and \(-g_2\) and \( f_2 \) belongs to the open cone spanned by \( g_1 \) and \( g_2 \). Since we are working with bases of a lattice \( \Lambda \), there exist strictly positive integers \( \alpha, \beta, \gamma, \delta \) such that \( f_1 = \alpha g_1 - \beta g_2 \) and \( f_2 = \gamma g_1 + \delta g_2 \) which can be

3The only difference is the fact that Grace admits the existence of square roots of \(-1 \pmod{4} \) modulo primes congruent to 1 \pmod{4}. The author succumbed to the siren song of a well-known explicit construction (based on Wilson’s Theorem) for such a square-root.
rewritten as \[
\begin{pmatrix}
    f_1 \\
    f_2
\end{pmatrix} =
\begin{pmatrix}
    \alpha & -\beta \\
    \gamma & \delta
\end{pmatrix}
\begin{pmatrix}
    g_1 \\
    g_2
\end{pmatrix}.
\]
Proposition 5 applied to the inequality \[
\det \begin{pmatrix}
    \alpha & -\beta \\
    \gamma & \delta
\end{pmatrix} = \alpha \delta + \beta \gamma \geq 2
\]
now implies that \(\mathbb{Z}f_1 + \mathbb{Z}f_2\) is a strict sublattice of index at least 2 in \(\Lambda = \mathbb{Z}g_1 + \mathbb{Z}g_2\).

5. PROOF OF THEOREM 1. We consider the eight open cones of \(\mathbb{R}^2\) delimited by the four lines \(x = 0, y = 0, x = y\) and \(x = -y\). We call these eight open cones windmill cones and we color them alternately black and white, starting with a black E-NE windmill cone \((x, y) \mid 0 < y < x\) (using the conventions of wind-roses), as illustrated in Figure 2.

Definition 9. A basis \(e, f\) of \(\mathbb{R}^2\) is a black windmill basis if \(e\) and \(f\) are contained in the open upper half-plane and if one element in \(\{e, f\}\) belongs to the open black E-NE windmill cone and the other element in \(\{e, f\}\) belongs to the open black N-NW windmill cone. Similarly, a white windmill basis contains an element in the open white N-NE windmill cone and an element in the open white W-NW windmill cone.

A 2-dimensional lattice \(\Lambda\) in \(\mathbb{R}^2\) has a black (respectively white) windmill basis if \(\Lambda = \mathbb{Z}e + \mathbb{Z}f\) is generated by a black (respectively white) windmill basis \(e, f\).
We illustrate the notion of windmill bases with the following example, henceforth used as a running example: Consider the lattice
\[ \Lambda = \{(x, y) \in \mathbb{Z}^2 | x + 7y \equiv 0 \pmod{13}\} \tag{2} \]
depicted in Figure 3 with shaded black windmill cones. The lattice \( \Lambda \) has two black windmill bases given by \((-1, 2), (5, 3)\) and by \((-1, 2), (6, 1)\).

The basis \((-1, 2), (-6, -1)\) is not a black windmill basis: \((-6, -1)\) does not belong to the upper half-plane.

The basis \((5, 3), (6, 1)\) is not a windmill basis since both basis vectors are contained in the open black E-NE windmill cone.

The basis \((-1, 2), (4, 5)\) is not a windmill basis since \((4, 5)\) belongs to the open white N-NE windmill cone and \((-1, 2)\) belongs to the open black N-NW windmill cone.

**Lemma 10.** All windmill bases of a lattice have the same color.

**Proof.** Otherwise we get a contradiction with Lemma 8 since windmill bases of different colors are obviously interlaced.

An odd prime number \(p\) and an element \(\mu\) of \(\mathbb{F}_p\) (henceforth often identified with \(\{0, \ldots, p-1\}\)) define a sub-lattice
\[ \Lambda_\mu(p) = \{(x, y) \in \mathbb{Z}_p, | x + \mu y \equiv 0 \pmod{p}\} \tag{3} \]
of index \(p\) in \(\mathbb{Z}_p^2\). We set \(\Lambda_\infty(p) = \{(x, y) \in \mathbb{Z}_p, | y \equiv 0 \pmod{p}\}\). We therefore have \(\Lambda = \Lambda_7(13)\) for our running example given by (2). All \(p + 1\) lattices \(\Lambda_\mu(p)\) with \(\mu\) in \(\{0, \ldots, p-1, \infty\}\) are distinct and \(\mathbb{Z}_p^2\) contains no other sublattices of prime index \(p\), see Proposition 4.

**Proposition 11.** The four lattices \(\Lambda_0(p), \Lambda_\infty(p), \Lambda_1(p), \Lambda_{p-1}(p)\) have no windmill basis.

**Proof.** Each of these four lattices is invariant under an orthogonal reflection with respect to a line separating black and white windmill cones. Such orthogonal reflections, followed by obvious sign changes, exchange white and black windmill bases. Lemma 10 shows therefore the nonexistence of (black or white) windmill bases for these lattices.

**Proposition 11** is optimal by the following result:

**Proposition 12.** Every lattice \(\Lambda_\mu(p)\) with \(2 \leq \mu \leq p - 2\) has a windmill basis.

**Proof.** \(\Lambda_\mu(p)\) obviously contains no elements of the form \((\pm m, 0)\) or \((\pm m, \pm p)\) with \(m\) in \(\{1, 2, \ldots, p-1\}\). Since \(p\) is prime, \(\Lambda_\mu(p)\) contains no elements of the form \((0, \pm m), (\pm p, \pm m)\) with \(m\) in \(\{1, \ldots, p-1\}\). Moreover, for \(\mu\) in \(\{2, \ldots, p-2\}\) considered as a subset of the finite field \(\mathbb{F}_p\), the elements \(1 + \mu\) and \(1 - \mu\) are invertible in \(\mathbb{F}_p\). This implies that \(\Lambda_\mu(p)\) has no elements of the form \(\pm(m, m), \pm(m, -m)\) for \(m\) in \(\{1, \ldots, p-1\}\). The intersection of a (black or white) windmill cone with \([-p, p]^2\) defines a triangle of area \(p^2/2 > p/2\) whose boundary contains no lattice-points of...
Lemma 3 implies now that every open (black or white) windmill cone contains a nonzero element \((x, y)\) of \(\Lambda_\mu(p)\) with coordinates \(x, y \in \{\pm 1, \pm 2, \ldots, \pm (p-1)\}\).

Thus there exists a parallelogram \(P\) of minimal area with vertices \(\pm e, \pm f\) in \(\Lambda_\mu(p) \cap (-p+1, \ldots, p-1)^2\) such that the set \(\{\pm e, \pm f\}\) intersects either all four open black windmill cones or all four open white windmill cones.

Suppose for simplicity that all elements of \(\{\pm e, \pm f\}\) are black (i.e., belong to open black windmill cones). (The case where both pairs \(\pm e\) and \(\pm f\) are white is analogous.)

Since \(\Lambda_\mu(p)\) intersects the diagonal \(\mathbb{R}(1, 1)\) and the antidiagonal \(\mathbb{R}(1, -1)\) in \(\mathbb{Z}(p, p)\) and in \(\mathbb{Z}(p, -p)\), and since \(\Lambda_\mu(p)\) contains obviously no elements of the form \((\pm a, 0), (0, \pm a)\) with \(a\) in \(\{1, \ldots, p-1\}\), all nonzero elements of \(P \cap \Lambda_\mu(p)\) belong to open windmill cones. Suppose that \(P \setminus \{\pm e, \pm f\}\) contains a nonzero element \(g\) of \(\Lambda_\mu(p)\). Area-minimality of \(P\) and the absence of nonzero elements in \(\Lambda_\mu(p) \cap (\mathbb{Z}(1, 1) \cup \mathbb{Z}(1, -1)) \cap (-p+1, \ldots, p-1)^2\) shows that \(g\) is contained in a white windmill cone (under the assumption that \(e\) and \(f\) are black). After replacing \(g\) by \(-g\) if necessary, the element \(g\) belongs either to the triangle with vertices \((0, 0), e, f\) or to the triangle with vertices \((0, 0), e, -f\). Lemma 3 applied to the two bases \(e, f\) and \(e, -f\) generating the same sublattice \(\mathbb{Z}e + \mathbb{Z}f\) of \(\Lambda_\mu(p)\) implies therefore the existence of a nonzero element \(h\) in \(P \cap \Lambda_\mu(p)\) such that the set \(\{\pm g, \pm h\}\) intersects all four open white windmill cones. The parallelogram with vertices \(\pm g, \pm h\) in all four open white windmill cones is therefore strictly included in \(P\) in contradiction with area-minimality of \(P\).

After replacing each of \(e\) and \(f\) by its negative if necessary, we get that \(e, f\) is a windmill basis of \(\Lambda_\mu(p)\) by Lemma 3.

**Lemma 13.** Let \(\Lambda\) be a lattice with two distinct windmill bases \(e, f\) and \(e, g\) sharing a common element \(e\). Then \(\Lambda\) has a unique pair of minimal elements given by \(\pm e\).

**Proof.** Since both ordered bases \(e, f\), and \(e, g\) start with \(e\) and are windmill bases, they induce the same orientation and we have \(g = f + ke\) for some nonzero integer \(k\) in \(\mathbb{Z}\). The affine line \(L = f + \mathbb{R}e\) intersects the open windmill cone \(C_f\) containing \(f\) and \(g\) in an open segment of length \(l > \sqrt{\langle e, e \rangle}\). Denoting by \(d\) the distance of \(L\) to the origin \((0,0)\) and by \(\alpha\) the angle in \((0, \pi/4)\) between the normal line \((\mathbb{R}e)^\perp\) \((\text{with } (\mathbb{R}e)^\perp \setminus \{(0,0)\})\) contained in \(C_f \cup (-C_f)\) of \(L\) and a boundary line of \(C_f\) (separating \(C_f\) from a windmill cone of the opposite color) we have the inequalities

\[
\sqrt{\langle e, e \rangle} < l = d \tan \alpha + \tan(\pi/4 - \alpha) = (1 - \tan \alpha \tan(\pi/4 - \alpha))d \tan(\pi/4) < d
\]

where we have used the addition formula \(\tan(x + y) = \frac{\tan x + \tan y}{1 - \tan x \tan y}\) of the tangent function.

The open strip delimited by the two parallel affine lines \(L\) and \(-L\) consisting of all points at distance \(< d\) from \(\mathbb{R}e\) intersects \(\Lambda\) in \(\mathbb{Z}e\). All elements of \(\Lambda \setminus \mathbb{Z}e\) are therefore at least at distance \(d > \sqrt{\langle e, e \rangle}\) from the origin. This shows that \(\pm e\) is the unique pair of minimal vectors in \(\Lambda\).
Figure 4. A schematic figure with $e + f$ in the E-NE windmill cone.

Lemma 14. Two windmill bases of a lattice are never disjoint.

Proof. Lemma 10 shows that two disjoint windmill bases of a lattice $\Lambda$ have the same color. If they are both white, we replace $\Lambda$ with the lattice $\sigma(\Lambda)$ having two black windmill bases given by $e, f$ and $g, h$ with $e, g$ in the open black E-NE windmill cone and $f, h$ in the open black N-NW windmill cone. Since the two bases are not interlaced by Lemma 8, we can moreover assume that $g$ and $h$ both belong to the open cone spanned by $e, f$. If the sum $e + f$ belongs to the open cone spanned by $g$ and $h$ we get two interlaced bases $e, e + f$ and $g, h$ in contradiction with Lemma 8. The nonzero lattice element $e + f$ therefore belongs either to the closed cone spanned by $e, g$ or to the closed cone spanned by $f, h$.

In the first case ($e + f$ in the closed cone spanned by $e, g$) the element $e + f$ belongs to the open black E-NE windmill cone containing $f$ and $g$, see Figure 4 for a schematic illustration.

Since the affine line $L = e + \mathbb{R}f$ has a downward slope strictly steeper than $-1$, the intersection of $L$ with the open white N-NE windmill cone is strictly longer than the intersection of $L$ with the open black E-NE windmill cone. Since the intersection of $L$ with the open black E-NE windmill cone contains at least the two elements $e$ and $e + f$ of $\Lambda$, there exists a natural integer $k > 1$ such that the element $e + kf$ of $\Lambda$ belongs to the open white N-NE windmill cone. This leads to two interlaced bases $f, e + kf$ and $g, h$ in contradiction with Lemma 8.

The second case where $e + f$ belongs to the closed cone spanned by $f$ and $h$ can be handled similarly. We also can reduce it to the first case by replacing $\Lambda$ with $\rho(\Lambda)$ where $\rho(x, y) = (y, -x)$ is a quarter-turn in clockwise direction.

Proposition 15. The following assertions hold if a lattice $\Lambda$ has at least two windmill bases:

- $\Lambda$ has a unique pair $\pm m$ of minimal vectors with $m$ contained in all windmill bases of $\Lambda$.
- $\Lambda$ has only finitely many windmill bases. More precisely, there exists a windmill basis $m, f$ of $\Lambda$ such that all windmill bases of $\Lambda$ are given by $m, f + sm$ for $s$ in $\{0, 1, \ldots, k - 1\}$ where $k$ is the number of windmill bases of $\Lambda$. 

© THE MATHEMATICAL ASSOCIATION OF AMERICA
Minimal vectors do not necessarily intersect the set \(\{e, f\}\) in the case of a lattice \(\Lambda\) with a unique windmill basis \(e, f\).

Both black windmill bases \((-1, 2), (5, 3)\) and \((-1, 2), (6, 1)\) of our running example \(\Lambda\) defined by (2) contain the minimal element \(m = (-1, 2)\) of \(\Lambda\). The running example gives \(f = (6, 1)\) and \(k = 2\) in the last assertion.

**Proof of Proposition 15.** Lemma 14 shows that two windmill bases of \(\Lambda\) intersect in a common element \(m\) defining the unique pair \(\pm m\) of minimal vectors of \(\Lambda\) by Lemma 13. Thus all windmill bases of \(\Lambda\) are all pairs \(m, g\) with \(g\) in the set \((f + \mathbb{R}m) \cap C_m^\perp \cap \Lambda\) where \(m, f\) is an arbitrary windmill basis and where \(C_m^\perp\) is the open windmill cone containing \(f\) perpendicular to the open windmill cone \(C_m\) containing \(m\).

Since the vector \(m\) does not belong to \(C_m^\perp\), the intersection of the affine line \(L = f + \mathbb{R}m\) with \(C_m^\perp\) is an open interval of bounded length and the set \(G = L \cap C_m^\perp \cap \Lambda\) is finite. We replace \(f\) by the element \(g\) of \(G\) minimizing the scalar product with \(m\) in order to get the result.

**Definition 16.** We call a black windmill basis \(u, v\) of a lattice \(\Lambda_\mu(p)\) (with \(\mu\) in \(\{2, \ldots, p - 2\}\)) standard if \(u = (a, c), v = (-d, b)\) with \(a, b, c, d \in \mathbb{N}\) such that \(\min(a, b) > \max(c, d)\).

The basis \(u = (6, 1), v = (-1, 2)\) of our running example (2) is a standard black windmill basis. The inequality \(3 \geq 2\) implies that its second black windmill basis \((5, 3), (-1, 2)\) is not standard.

**Proposition 17.** Given an odd prime number \(p\) and an integer \(\mu\) in \(\{2, \ldots, p - 2\}\), the lattice \(\Lambda_\mu(p)\) has either only white windmill bases or it has a unique standard black windmill basis.

**Proof.** Proposition 12 shows that such a lattice \(\Lambda = \Lambda_\mu(p)\) has windmill bases. They are all of the same color by Lemma 10. We assume now that all windmill bases of \(\Lambda\) are black. A vector \(w\) in \(\Lambda\) is of windmill type if there exists a windmill basis containing \(w\).

We denote by \(u = (a, c) \in \Lambda\) the lowest vector of windmill type in the open black E-NE windmill cone and we denote by \(v = (-d, b) \in \Lambda\) the rightmost vector of windmill type in the open black N-NE windmill cone. The vectors \(u, v\) form a black windmill basis of \(\Lambda\): This is obvious if \(\Lambda\) has a unique windmill basis and it follows from the description of all windmill bases given by Proposition 15 otherwise.

For our running example (2) we get \(u = (6, 1)\) and \(v = (-1, 2)\).

We claim that \(u, v\) is a standard black windmill basis of \(\Lambda\): We have \(a > c\) since \(u = (a, c)\) belongs to the open black E-NE windmill cone and \(b > d\) since \(v = (-d, b)\) belongs to the open black N-NW windmill cone.

Since \(u - v = (a + d, c - b)\) is lower than \(u\), the basis of \(\Lambda\) given by \(u - v = (a + d, c - b), v = (-d, b)\) is not a windmill basis and we have therefore \(b \geq c\). If \(b = c\), the vectors \(u - v = (a + d, 0), v = (-d, b)\) are a basis of \(\Lambda\). Since \(\Lambda\) intersects \(\mathbb{Z}(1, 0)\) in \(\mathbb{Z}(p, 0)\) we have \(a + d = p\) which implies \(u - v = (p, 0)\). Since \(u - v = (p, 0)\) and \(v = (-d, b)\) is a basis of \(\Lambda\), we get \(b = 1\) in contradiction with the inequalities \(1 \leq d < b\). We have thus \(b > c\).

Similarly, since \(v + u = (a - d, b + c)\) is at the right of \(v\), the basis of \(\Lambda\) given by \(u = (a, c), v + u = (a - d, b + c)\) is not a windmill basis and we have \(a \geq d\). If \(a = d\), the vectors \(u = (a, c), v + u = (0, b + c)\) are a basis of \(\Lambda\). This implies \(b + c = p\) and \(a = 1\) contradicting the inequalities \(1 \leq c < a\). This shows \(a > d\).
Uniqueness of the standard basis for a lattice with black windmill bases follows easily from the description of all windmill bases given by the last assertion of Proposition 15.

Proof of Theorem 1. Given an odd prime number \( p \), we denote by \( S_p \) the set of all solutions \((a, b, c, d)\) as defined by Theorem 1.

We associate to a solution \((a, b, c, d)\) in \( S_p \) the two vectors \( u = (a, c) \), \( v = (-d, b) \) and we consider the sublattice \( \Lambda = \mathbb{Z}u + \mathbb{Z}v \) of index \( p = ab - c(-d) \) in \( \mathbb{Z}^2 \) generated by \( u \) and \( v \). Since \( p \) is prime, there are exactly two solutions with \( cd = 0 \), given by \((p, 1, 0, 0)\) and \((1, p, 0, 0)\) corresponding to the lattices \( \mathbb{Z}(p, 0) + \mathbb{Z}(0, 1) \) and \( \mathbb{Z}(1, 0) + \mathbb{Z}(0, p) \).

We suppose henceforth that \( cd > 0 \). The vectors \( u \) and \( v \) are then contained respectively in the open black E-NE and in the open black N-NW windmill cone and therefore form a standard black windmill basis of the lattice \( \Lambda \).

Sub-lattices of prime-index \( p \) in \( \mathbb{Z}^2 \) are in bijection with the set of all \( p + 1 \) points on the projective line \( \mathbb{P}^1 \mathbb{F}_p \) over the finite field \( \mathbb{F}_p \), see Proposition 4. More precisely, a point \([a : b]\) of the projective line defines the lattice

\[
\Lambda_{[a:b]} = \{(x, y) \in \mathbb{Z}^2 \mid ax + by \equiv 0 \pmod{p}\}
\]

which is equal to the lattice \( \Lambda_{\mu}(p) \) defined by (3) for \( \mu \equiv b/a \pmod{p} \) using obvious conventions. We have already considered lattices associated to the two solutions with \( cd = 0 \). By Proposition 11, the two lattices given by \( \mu \equiv \pm 1 \pmod{p} \) have no windmill basis and thus yield no solutions. All \((p - 3)\) lattices \( \Lambda_{\mu}(p) \) with \( \mu \in \{2, \ldots, p - 2\} \) have windmill bases by Proposition 12.

Since \( \Lambda_{\mu}(p) \) and \( \Lambda_{\mu^{-1} \pmod{p}}(p) \) (respectively \( \Lambda_{\mu^{-1}}(p) \)) differ by a horizontal (respectively diagonal) reflection, they have windmill bases of different colors. Proposition 17 shows that exactly \((p - 3)/2\) values of \( \mu \) in \( \{2, \ldots, p - 2\} \) correspond to lattices \( \Lambda_{\mu}(p) \) with unique standard black windmill bases. These \((p - 3)/2\) lattices are therefore in one-to-one correspondence with solutions in \((a, b, c, d)\) in \( S_p \) such that \( cd > 0 \). Taking into account the two degenerate solutions \( p \cdot 1 + 0 \cdot 0 \) and \( 1 \cdot p + 0 \cdot 0 \), we get a total number of \((p - 3)/2 + 2 = (p + 1)/2\) solutions in \( S_p \).

6. COMPLEMENT: VORONOI CELLS AND WINDMILL BASES. A lattice \( \Lambda \) induces a Voronoi diagram tiling the \( \mathbb{R}^2 \) plane with Voronoi cells bounded by points of \( \mathbb{R}^2 \) having more than a unique closest lattice point. Points at locally maximal distance to \( \Lambda \) are vertices of the Voronoi diagram for \( \Lambda \), see for example the monograph [3] for more on Voronoi cells of lattices and sphere packings.

We denote by \( \mathcal{C}_\Lambda \) the Voronoi cell consisting of all points of \( \mathbb{R}^2 \) with closest lattice-point the trivial element \((0, 0)\) of \( \Lambda \). The plane \( \mathbb{R}^2 \) is tiled by \( \Lambda \)-translates of \( \mathcal{C}_\Lambda \). The Voronoi cell \( \mathcal{C}_\Lambda \) is a rectangle if \( \Lambda \) has a reduced basis of two orthogonal vectors and it is a centrally symmetric hexagon otherwise. A reduced basis \( e, f \) defines normal vectors to two pairs of parallel sides of \( \mathcal{C}_\Lambda \). A normal vector \( g \) to the remaining pair of sides in the hexagonal case is given by \( e - f \epsilon \) where \( \epsilon = \langle e, f \rangle / |\langle e, f \rangle| \) is the sign of the scalar product \( \langle e, f \rangle \) between \( e \) and \( f \). We call the set \( \{\pm e, \pm f, \pm g\} \), respectively \( \{\pm e, \pm f\} \), \{\pm g\} of primitive lattice elements normal to sides of \( \mathcal{C}_\Lambda \) the set of Voronoi vectors. The Voronoi cell \( \mathcal{C}_\Lambda \) is defined by the inequalities \( 2\langle x, v \rangle \leq \langle v, v \rangle \) for all elements \( v \) of the set \( \mathcal{V} \) of Voronoi vectors. Two linearly independent Voronoi vectors \( u, v \) in \( \mathcal{V} \) generate \( \Lambda \).

We illustrate these notions on our running example \( \Lambda = \mathbb{Z}(-1, 2) + \mathbb{Z}(6, 1) \) defined by (3): A reduced basis for \( \Lambda \) is given by the minimal vector \( e = (-1, 2) \) and
Proposition 18. Every lattice $\Lambda$ in $\mathbb{R}^2$ with windmill bases has a windmill basis contained in its set of Voronoi vectors.

Proposition 18 (together with Proposition 15 and Gaussian lattice reduction) gives a fast algorithm (using $O(\log p)$ operations on integers not exceeding $p$) for computing the solution of $\mathcal{S}_p$ associated to $\Lambda_{\pm\mu}(p)$ for $\mu \in \mathbb{F}_p \setminus \{0, \pm 1\}$. Compute a reduced basis of $\Lambda_{\mu}(p)$ and use it to construct the associated set $\mathcal{V}$ of Voronoi vectors which contains a windmill basis by Propositions 12 and 18. If the windmill basis is white, replace $\Lambda_{\mu}(p)$ by $\Lambda_{-\mu}(p)$ (using for example the vertical reflection $\sigma(x, y) = (-x, y)$ of $\mathbb{R}^2$) in order to get a black windmill basis of $\Lambda_{-\mu}(p)$. Now use Proposition 15 for constructing the unique standard basis $(a, c), (-d, b)$ encoding the solution $p = ab + cd$ of $\mathcal{S}_p$.

The main tool for proving Proposition 18 is the following result which is perhaps of independent interest:

Lemma 19. Assume that the set $\mathcal{V}$ of Voronoi vectors of a lattice $\Lambda$ does not intersect the set of boundary lines separating black and white windmill cones. Then $\Lambda$ has a windmill basis contained in $\mathcal{V}$.

Proof of Lemma 19. We suppose first that the Voronoi domain of $\Lambda$ is a rectangle. This implies $\mathcal{V} = \{\pm e, \pm f\}$ with $e$ and $f$ two elements of open windmill cones in the upper half-plane forming a reduced orthogonal basis of $\Lambda$. Since $e$ and $f$ are orthogonal they belong to two distinct open windmill cones of the same color. Therefore they form a windmill basis.

We consider now $\mathcal{V} = \{\pm e, \pm f, \pm g\}$ with $e, f, g$ in open windmill cones of the upper half-plane. We also assume that $e$ is a (perhaps not unique) minimal vector of $\Lambda$. Minimality of $e$ and the inequalities $|\langle e, f \rangle| < \langle e, e \rangle$ and $|\langle e, g \rangle| < \langle e, e \rangle$ imply that the line $\mathbb{R} e$ crosses both lines $\mathbb{R} f$ and $\mathbb{R} g$ with angles strictly larger than $\pi/4$. The open windmill cone $\mathcal{C}_e$ containing $e$ has an opening angle of $\pi/4$ and is therefore distinct from the (not necessarily distinct) open windmill cones $\mathcal{C}_f$ and $\mathcal{C}_g$ containing $f$, respectively $g$. We get a windmill basis $e, h$ for $h \in \{f, g\}$ such that $\mathcal{C}_e$ and $\mathcal{C}_h$ are of the same color. If such an element $h$ does not exist, then $\mathcal{C}_f$ and $\mathcal{C}_h$ have the same color opposite to the color of $\mathcal{C}_e$. Since $f$ and $g$ are either separated by the line $\mathbb{R} e$ or by its orthogonal $(\mathbb{R} e)^\perp$ (with $(\mathbb{R} e)^\perp \setminus \{(0, 0)\}$ contained in the two open windmill cones orthogonal to $\mathcal{C}_e$ and of the same color as $\mathcal{C}_e$), the elements $f$ and $g$ of the upper half-plane belong to different open windmill cones of the same color and therefore form a windmill basis.

Proof of Proposition 18. The result holds by Lemma 19 if $\mathcal{V}$ contains no elements on boundary lines separating black and white windmill cones.

Otherwise, if $\mathcal{V} = \{\pm e, \pm f\}$ is reduced to two pairs of orthogonal elements, then $e, f$ are both elements in the boundary of black and white windmill cones. The reflection $ae + bf \mapsto ae - bf$ induces therefore a lattice isomorphism of $\Lambda$ which exchanges colors of windmill cones. Such a lattice has no windmill bases by Lemma 10.
We suppose now that $\Lambda$ has a windmill basis $u, v$ not contained in the set $\mathcal{V} = \{\pm e, \pm f, \pm g\}$ of Voronoi vectors, with $e, f, g$ in the closed upper half-plane. A sufficiently small rotation $\rho$ (suitably chosen if $\{e, f, g\}$ intersects the horizontal line $y = 0$) sends the windmill basis $u, v$ of $\Lambda$ to a windmill basis (of the same color) $\rho(u), \rho(v)$ of $\rho(\Lambda)$ and sends $\mathcal{V}$ to a set $\rho(\mathcal{V})$ of Voronoi vectors having no elements on boundary lines separating windmill cones. Lemma 19 shows that $\rho(\Lambda)$ has an additional windmill basis contained in $\rho(\mathcal{V})$ distinct from the windmill basis $\rho(u), \rho(v)$ not contained in $\rho(\mathcal{V})$. Proposition 15 therefore implies that $\rho(\Lambda)$ has a unique pair $\pm \rho(m)$ of minimal vectors intersecting every windmill basis of $\rho(\Lambda)$. We can therefore assume (perhaps after a permutation among the elements $e, f, g$) that $e$ is the unique minimal element in the upper half-plane of $\Lambda$ and that $e$ is contained in every windmill basis of $\Lambda$. Since $\pm f$ and $\pm g$ are the elements of $\pm f + \mathbb{Z}e$ which are closest to the line $(\mathbb{Re})^\perp$ orthogonal to $\mathbb{Re}$, the last assertion of Proposition 15 implies that either $e, f$ or $e, g$ is a windmill basis of $\Lambda$. \hfill \blacksquare

ACKNOWLEDGMENTS. I thank M. Decauwert, P. Dehornoy, P. De la Harpe, C. Elsholtz, A. Guilloux, C. Leuridan, C. MacLean, E. Peyre, for comments, remarks or questions. Special thanks to C. Leuridan and to two anonymous referees whose suggestions improved the text tremendously.

REFERENCES

[1] de Cervantes, M. (1605). El ingenioso hidalgo don Quijote de la Mancha, Madrid.
[2] Christopher, D.A. (2016). A partition-theoretic proof of Fermat’s two squares theorem. Discrete Math. 339(4): 1410–1411.
[3] Conway, J. H., Sloane, N. J. A. (1999). Sphere Packings, Lattices and Groups, 3rd ed. New York: Springer.
[4] Dolan, S. (2016). A very simple proof of the two-squares theorem. Math. Gazette. 105(564): 511.
[5] Elsholtz, C. (2010). A combinatorial approach to sums of two squares and related problems. In: Chudnovsky, D., et al., eds. Additive Number Theory. Festschrift in Honor of the Sixtieth Birthday of Melvyn B. Nathanson. New York: Springer, pp. 115–140.
[6] Grace, J. H. (1927). The four square theorem. J. London Math. Soc. 2: 3–8.
[7] Hardy, G. H., Wright, E. M. (1960). An Introduction to the Theory of Numbers, 4th ed. London: Oxford Univ. Press.
[8] Heath-Brown, D. R. Fermat’s Two Squares Theorem. Archived by Oxford Univ. https://ora.ox.ac.uk/
[9] Mathoverflow, MO31113: https://mathoverflow.net/questions/31113
[10] Mathoverflow, MO405035: https://mathoverflow.net/questions/405035
[11] Spivak, A. Крылатые квадраты. Lecture notes for the mathematical circle at Moscow State University: 15th lecture 2007. https://mmmf.msu.ru/lect/spivak/summa_sq.pdf
[12] Wikipedia (June 2022). Fermat’s theorem on sums of two squares, https://en.wikipedia.org/wiki/Fermat’s_theorem_on_sums_of_two_squares
[13] Zagier, D. (1990). A one-sentence proof that every prime $p \equiv 1 \pmod{4}$ is a sum of two squares. Amer. Math. Monthly 97(2): 144.

ROLAND BACHER earned a Ph.D. from the University of Geneva. He holds a position at the University Grenoble-Alpes where he recovers from all those gloriously lost battles against students and administrative windmills by dreaming of quixotic quests in the quadrivium.

Univ. Grenoble Alpes, Institut Fourier, F-38000 Grenoble, France
roland.bacher@univ-grenoble-alpes.fr

836 © THE MATHEMATICAL ASSOCIATION OF AMERICA [Monthly 130