Research Article

Chris Busenhart, Lorenz Halbeisen, Norbert Hungerbühler*, and Oliver Riesen

On primitive solutions of the Diophantine equation $x^2 + y^2 = M$

https://doi.org/10.1515/math-2021-0087
received March 19, 2021; accepted August 5, 2021

Abstract: We provide explicit formulae for primitive, integral solutions to the Diophantine equation $x^2 + y^2 = M$, where M is a product of powers of Pythagorean primes, i.e., of primes of the form $4n + 1$. It turns out that this is a nice application of the theory of Gaussian integers.

Keywords: Pythagorean primes, Diophantine equation

MSC 2020: 11D45, 11D09, 11A41

1 Introduction

The history of the Diophantine equation $x^2 + y^2 = M$ has its roots in the study of Pythagorean triples. The oldest known source is Plimpton 322, a Babylonian clay tablet from around 1800 BC: This table lists two of the three numbers of Pythagorean triples, i.e., integers x, y, z which satisfy $x^2 + y^2 = z^2$. Euclid's formula $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, where m and n are coprime and not both odd, generates all primitive Pythagorean triples, i.e., triples where x, y, z are coprime.

In 1625 Albert Girard, a French-born mathematician working in Leiden, the Netherlands, who coined the abbreviations sin, cos, and tan for the trigonometric functions and who was one of the first to use brackets in formulas, stated that every prime of the form $4n + 1$ is the sum of two squares (see [1]). Pierre de Fermat [2, tome premier, p. 293, tome troisiéme, pp. 243–246] claimed that each such *Pythagorean prime* and its square is the sum of two squares in a single way, its cube and biquadratic in two ways, its fifth and sixth powers in three ways, and so on. It is easy to see that, if an odd prime is a sum of two squares, it must be of the form $4n + 1$. The reverse implication, called Fermat's theorem on sums of two squares, or Girard's theorem, is much more difficult to prove. However, Fermat stated in a letter to Carcavi from August 1659 that he had a proof by the method of infinite descent for the fact that each Pythagorean prime is the sum of two squares, but he gave no details (see, [2, tome deuxième, p. 432]). Recall that by the Dirichlet prime number theorem (see [3]), there are infinitely many Pythagorean primes.

Bernard Frénicle de Bessy who lived 1604–1674 was an advocate of experimental mathematics: By his *Méthode des exclusions* he concluded from looking at numerical tables that, if $p_1, p_2, \ldots$ are distinct Pythagorean primes, then the number $N = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ is the hypotenuse of exactly 2^{n-1} primitive right triangles (see [4, pp. 22–34, 156–163]). The theory was finally put on a solid footing by Leonhard Euler who

* **Corresponding author: Norbert Hungerbühler,** Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland, e-mail: norbert.hungerbuehler@math.ethz.ch
Chris Busenhart: Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland, e-mail: chris.busenhart@math.ethz.ch
Lorenz Halbeisen: Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland, e-mail: lorenz.halbeisen@math.ethz.ch
Oliver Riesen: Kantonsschule Zug, Lüssiweg 24, 6300 Zug, Switzerland, e-mail: oliver.riesen@ksz.ch

proved Girard's theorem in two papers (see [5] and [6]). In the sequel, 1775, Joseph-Louis Lagrange gave a proof based on his general theory of integral quadratic forms (see [7, p. 351]). The theory of quadratic forms came to a full understanding with Gauss' *Disquisitiones arithmeticae* [8]. Gauss showed that for odd integers $M > 2$ of the form $M = P \cdot Q$, where P and Q are products of powers of primes of the form $4n + 1$ and $4n + 3$, respectively, the Diophantine equation $x^2 + y^2 = M$ is solvable in positive integers if and only if Q is a perfect square (see Gauss [9, p. 149 f]). Richard Dedekind contributed two more proofs for Girard's theorem: see [10, §27, p. 240] and [11, Supplement XI, Ueber die Theorie der ganzen algebraischen Zahlen, p. 444]. Another beautiful proof uses Minkowski's theorem on convex sets and lattices (see, e.g., [12, §7.2]). The shortest argument is Don Zagier's famous one-sentence proof [13] of Girard's theorem.

For a Pythagorean prime $p = 4n + 1$, Gauss provided an explicit formula for the unique positive, primitive solution $\{x, y\}$ of the Diophantine equation $x^2 + y^2 = p$. Namely, with

$$z \coloneqq \left| \left\langle \frac{1}{2}\binom{2n}{n} \right\rangle \right|$$

we have

$$\{x, y\} = \{z, |\langle z(2n)!\rangle|\},$$

where $\langle u \rangle \in \left(-\frac{p}{2}, \frac{p}{2}\right)$ denotes the residue of u mod p (see [14, Chapter 5] for a proof). Another explicit formula was found by Jacobsthal in his dissertation [15]: The odd number in $\{x, y\}$ is given by

$$\left| \frac{1}{2} \sum_{n=1}^{p} \left(\frac{x}{p}\right)\left(\frac{x^2 - 1}{p}\right) \right|,$$

where $\left(\frac{a}{p}\right)$ denotes the Legendre symbol. Both formulae are of more theoretical interest. For an efficient algorithm to compute the primitive solution we refer to [16].

Hardy and Wright [17, Theorem 278] gave a formula which can be used to calculate the number of all integer solutions of equations of the form $x^2 + y^2 = M$ for any given natural number M. The purpose of this paper is to provide explicit formulae for *positive*, *primitive*, integral solutions to the same Diophantine equation.

2 Combining solutions

A recurring phenomenon in the theory of Diophantine equations is that solutions may be combined to generate new solutions of a given equation. For the equation

$$a^2 + b^2 = M, \tag{1}$$

this is shown in Lemma 1. To keep the notation short we write $(a, b)_M$ for an integer solution of (1). Trivially, we have $(a, b)_M \Rightarrow (b, a)_M$ and $(a, b)_M \Rightarrow (-a, b)_M$. Now, for two pairs of integers (a, b) and (c, d), we define

$$(a, b) * (c, d) \coloneqq (ac - bd, ad + bc). \tag{2}$$

The following result is similar to [18, Lemma 4].

Lemma 1. *Let $a, b, \tilde{a}, \tilde{b}$ be integers and let M, N be positive integers such that $(a, b)_M$ and $(\tilde{a}, \tilde{b})_N$. Then*

$$((a, b) * (\tilde{a}, \tilde{b}))_{M \cdot N}.$$

Proof. We have to verify that $(a\tilde{a} - b\tilde{b})^2 + (a\tilde{b} + b\tilde{a})^2 = M \cdot N$. Indeed, we have

$$(a\tilde{a} - b\tilde{b})^2 + (a\tilde{b} + b\tilde{a})^2 = \underbrace{(a^2 + b^2)}_{=M} \cdot \underbrace{(\tilde{a}^2 + \tilde{b}^2)}_{=N} = M \cdot N. \qquad \square$$

The operation (2) reminds of the product of complex numbers, and, as we shall see below, the Gaussian integers $\mathbb{Z}[i]$ are the adequate language to discuss equation (1). In fact, Gaussian integers are a standard tool in the treatment of this sort of Diophantine equation, see, e.g., Hardy-Wright [17, §12.6, §16.9], or Rosen [19, §14].

3 Primitive solutions for $M = p^k$

The formulae of Gauss and Jacobsthal yield explicit primitive solutions of (1) if M is a Pythagorean prime p. Now we want to see how the *positive*, *primitive* solutions for $M = p^k$, k a positive integer, can be generated from this. Note that in [17, Theorem 278], Hardy and Wright constructed all solutions (not just the primitive ones) of the Diophantine equation using Gaussian integers. This has first been done by Jacobi, it seems, who used generating functions rather than Gaussian integers, see [20, Bd. 2, §7]. Another reference is Grosswald [21, §2.6].

As mentioned above, the product (2) from Section 2 corresponds to the complex multiplication if we consider the first and second entries as real and imaginary parts, respectively. In particular, Lemma 1 can be formulated as follows:

Fact 2. Let $a, b, \tilde{a}, \tilde{b}$ be integers and let M, N be positive integers such that $(a, b)_M$ and $(\tilde{a}, \tilde{b})_N$. Then, for $z := (a + ib)(\tilde{a} + i\tilde{b})$, we have

$$(\mathrm{Re}(z), \mathrm{Im}(z))_{M \cdot N}.$$

So, from now on we will work with Gaussian integers $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ (see, e.g., [22] as a general reference): Gaussian integers are a factorial ring, i.e., each element in $\mathbb{Z}[i]$ has a unique factorisation up to the units $\pm 1, \pm i$. Every Pythagorean prime p can be decomposed by two Gaussian primes, which are the complex conjugate of each other, i.e., Pythagorean primes are of the form $p = \alpha\overline{\alpha}$ for some $\alpha \in \mathbb{Z}[i]$, and this represents the corresponding unique positive, primitive solution of (1). As an example, 5 can be factorised by $1 + 2i, 1 - 2i$. This is also true for $2 = (1 + i)(1 - i)$. On the other hand, all non-Pythagorean primes in $\mathbb{Z}$, different from 2, are also primes in $\mathbb{Z}[i]$.

Proposition 3. *Let $p = \alpha\overline{\alpha}$ be a Pythagorean prime and let k be a positive integer. Then $\{|\mathrm{Re}(\alpha^k)|, |\mathrm{Im}(\alpha^k)|\}$ is the unique positive, primitive solution to $x^2 + y^2 = p^k$.*

Proof. At first, we will show the existence of a primitive solution to the above equation. By observing that $p^k = \alpha^k\overline{\alpha}^k$, we see that this equation is satisfied by $\{|\mathrm{Re}(\alpha^k)|, |\mathrm{Im}(\alpha^k)|\}$. Thus, we need to show that these numbers are relatively prime. Assume not then there exist integers u, v, λ where $\lambda > 1$ such that $\alpha^k = \lambda(u + iv)$. By the uniqueness of prime factorisation in $\mathbb{Z}[i]$ we get $\lambda = \alpha^l$ for some positive integer l. For $\theta = \arg(\alpha)$, we get that $\frac{\theta}{\pi}$ and $\tan(\theta)$ are both rational, a contradiction to Niven's theorem (see [23, Cor. 3.12]).

To show uniqueness, let us assume that $a, b \in \mathbb{Z}$ are relatively prime and satisfy $a^2 + b^2 = p^k$. Then we also have

$$(a + bi)(a - bi) = \alpha^k\overline{\alpha}^k,$$

which implies that α divides either one of the factors on the left-hand side. Hence, without loss of generality, we have that α divides $(a + bi)$ and by complex conjugation, $\overline{\alpha}$ divides $(a - bi)$. However, neither α divides $(a - bi)$ nor $\overline{\alpha}$ divides $(a + bi)$. Otherwise, α or $\overline{\alpha}$ would divide a and b (observe that α and $\overline{\alpha}$ do not divide 2 because p is a Pythagorean prime), so both would then divide both because $a, b \in \mathbb{Z}$. By considering $\alpha \neq \overline{\alpha}$, we get that p divides a and b, which is a contradiction to the coprimality of them. Hence, we conclude that α^k divides $(a + bi)$ and $\overline{\alpha}^k$ divides $(a - bi)$ in the Gaussian integers. Therefore, both Gaussian integers on the left-hand side of the equation

$$\frac{a+bi}{\alpha^k}\frac{a-bi}{\overline{\alpha}^k}=1,$$

are units, which implies the existence of $s \in \{0, 1, 2, 3\}$ such that $i^s\alpha^k = a + bi$ and we get our desired result

$$\{a, b\} = \{|\mathrm{Re}(\alpha^k)|,\ |\mathrm{Im}(\alpha^k)|\}. \qquad \square$$

Although the formula in Proposition 3 is practically trivial in the context of Gaussian integers, it does not seem to be very widely known. Indeed, the formulas we now have at hand are missing for the corresponding sequences in the *On-Line Encyclopedia of Integer Sequences* OEIS. A few examples: Let $p = \alpha\overline{\alpha}$ be a factorised Pythagorean prime, $a_k = |\mathrm{Re}(\alpha^k)|$ and $b_k = |\mathrm{Im}(\alpha^k)|$. Then $x_k = \min\{a_k, b_k\}$ and $y_k = \max\{a_k, b_k\}$ for $M = 5^k, 17^k, 73^k$ and $M = 13^k$ are explicit formulas for the integer sequences [24, A230710, A230711, A230622, A230623, A230962, A230963] and [25, A188948, A188949].

4 Primitive solutions for $M = \prod_{l=1}^{n} p_l^{k_l}$

In this section, we show how one can find the positive, primitive solution to the Diophantine equation $x^2 + y^2 = M$, where M is a product of powers of Pythagorean primes. The following part is strongly related to [26, Lemma 3.30].

Theorem 4. *Let n and k_l be positive integers, $p_l = \alpha_l\overline{\alpha}_l$ be pairwise distinct Pythagorean primes for $1 \le l \le n$ and let $M = \prod_{l=1}^{n} p_l^{k_l}$. Then*

$$\left\{\left|\mathrm{Re}\left(\prod_{l=1}^{n}\alpha_l^{k_l}\right)\right|,\ \left|\mathrm{Im}\left(\prod_{l=1}^{n}\alpha_l^{k_l}\right)\right|\right\}$$

is a primitive solution for $x^2 + y^2 = M$.

Proof. Obviously, we have $M = \prod_{l=1}^{n}\alpha_l^{k_l}\overline{\prod_{l=1}^{n}\alpha_l^{k_l}}$. Therefore, $x^2 + y^2 = M$ is clearly satisfied by $|\mathrm{Re}(\prod_{l=1}^{n}\alpha_l^{k_l})|$, $|\mathrm{Im}(\prod_{l=1}^{n}\alpha_l^{k_l})|$.

It remains to show that our solution is relatively prime. If not, then there exists integers u, v, λ where $\lambda > 1$ such that $\prod_{l=1}^{n}\alpha_l^{k_l} = \lambda(u + iv)$. In this case, we must have $\lambda = \prod_{l=1}^{n}\alpha_l^{k_l'}$ with $0 \le k_l' \le k_l$. Additionally, it holds true that $\lambda = \overline{\lambda} = \prod_{l=1}^{n}\overline{\alpha}_l^{k_l'}$. Observe that all prime factors of λ are different from $\pm 1, \pm i$. Thus, we have a contradiction to the unique prime factorisation in $\mathbb{Z}[i]$. $\square$

The following proposition was stated by Frénicle without a proof, as we mentioned in the introduction.

Proposition 5. *Let an arbitrary $M = 2^r\prod_{l=1}^{n} p_l^{k_l} \in \mathbb{N}_{>2}$ be factorised and $r, n \in \mathbb{N}$. If all the primes $p_l \neq 2$ are Pythagorean and $r \in \{0, 1\}$, then there are 2^{n-1} positive, primitive solutions to $x^2 + y^2 = M$. Otherwise, there is no primitive solution.*

Proof. At first assume that all the p_l's are Pythagorean primes and $r \in \{0, 1\}$. Let I, I' be a partition of the set $\{1, 2, \ldots, n\}$ and

$$M = 2^r\prod_{l=1}^{n} p_l^{k_l} = \left((1+i)^r\prod_{l=1}^{n}\alpha_l^{k_l}\right)\overline{\left((1+i)^r\prod_{l=1}^{n}\alpha_l^{k_l}\right)} = \underbrace{((1+i)^r\prod_{l\in I}\alpha_l^{k_l}\overline{\prod_{l\in I'}\alpha_l^{k_l}})}_{=\alpha_I}\underbrace{\overline{((1+i)^r\prod_{l\in I}\alpha_l^{k_l}\overline{\prod_{l\in I'}\alpha_l^{k_l}})}}_{=\overline{\alpha_I}}$$

be factorised in $\mathbb{Z}[i]$. Then each I gives us a primitive solution of $M = \mathrm{Re}(\alpha_I)^2 + \mathrm{Im}(\alpha_I)^2$ for $r = 0$ by Theorem 4. If $r = 1$, then the solution clearly remains primitive.

Conversely, if $\{x, y\}$ is a primitive solution to the equation $x^2 + y^2 = M$, then $M = (x + iy)(x - iy)$. So, both of these factors can be factorised by the Gaussian primes of M multiplied by a unit of $\mathbb{Z}[i]$. Since these factorisations must be the complex conjugates of each other and $(x, y) = 1$, there exists $I \subset \{1, 2, \dots, n\}$ and $k \in \{0, 1, 2, 3\}$ such that $x + iy = (1 + i)^r i^k \alpha_I$ or $x + iy = \overline{(1 + i)^r i^k \alpha_I}$. This shows that each primitive solution to the equation above can be constructed by the right choice of I.

Now we would like to show that $x^2 + y^2 = M$ has exactly 2^{n-1} positive solutions. Let I_1 and I_2 be subsets of $\{1, 2, \dots, n\}$ and assume that α_{I_1} and α_{I_2} represent the same solution, i.e., we have

$$\{|\mathrm{Re}(\alpha_{I_1})|, |\mathrm{Im}(\alpha_{I_1})|\} = \{|\mathrm{Re}(\alpha_{I_2})|, |\mathrm{Im}(\alpha_{I_2})|\}. \qquad (**)$$

Then we find $k \in \{0, 1, 2, 3\}$ such that

$$\alpha_{I_1} = i^k \alpha_{I_2} \quad \text{or} \quad \alpha_{I_1} = i^k \overline{\alpha_{I_2}}.$$

Since i is a unit, we have that either both α_{I_1} and α_{I_2} have the same prime factors in $\mathbb{Z}[i]$ or they are the complex conjugates of each other. Therefore, $k = 0$ and $\alpha_{I_1} = \alpha_{I_2}$ or $\alpha_{I_1} = \overline{\alpha_{I_2}}$ by definition of α_I. Furthermore, if I_1 and I_2 are disjoint or equal, then $(**)$ is clearly satisfied, so we get the same positive, primitive solution. Thus, there are exactly 2^{n-1} different choices for I such that the resulting positive, primitive solutions are different from each other if all the p_l's are Pythagorean primes and $r \in \{0, 1\}$.

It remains to show the case where one of the primes p_l is odd and non-Pythagorean or $r > 1$. Let $x, y \in \mathbb{Z}$ with $x^2 + y^2 = M$.

Assume that $p_1 \equiv 3 \pmod 4$. Then p_1 is a Gaussian prime and, without loss of generality, p_1 divides $x + iy$ in $\mathbb{Z}[i]$. Then p_1 also divides $x - iy$ because its complex conjugate (which is p_1 itself) must divide the complex conjugate of $x + iy$. Hence, p_1 is also a divisor of the sum and the difference of both terms above. Since p_1 is not a divisor of 2, we get that p_1 divides x and y which let us conclude that our solution cannot be primitive.

Finally, we only have to treat the case $r > 1$. Since 2 can be decomposed by the Gaussian primes $1 + i$ and $1 - i$, we have that $x + iy$ or $x - iy$ must be divisible by the multiplication of at least two of these factors. Hence, $x + iy$ and $x - iy$ have a divisor 2 or $2i$. Thus, by similar arguments to above, you can show that x and y can be divided by 2, which shows us again that our solution cannot be primitive.

Alternative for $r > 1$: (Shorter but not argued by the Gaussian prime theorem) If M is divisible by 4, then either $x^2 \equiv 3 \pmod 4$ and $y^2 \equiv 1 \pmod 4$ or the other way round because our solution is primitive, which implies that x and y must be odd. However, this is a contradiction because an integer square cannot be congruent to 3 (mod 4). □

The result on the number of primitive solutions in Proposition 5 can also be found in [27, Theorem 1, (1.6)]. There, the proof uses generating functions and is not constructive, in contrast to our argument.

Acknowledgements: The authors would like to thank the referees for their careful reading and useful comments and suggestions, which helped to improve the quality of the article. In particular, the authors are grateful for the suggestion regarding the generalisation of the initial version of Proposition 5.

Conflict of interest: Authors state no conflict of interest.

References

[1] S. Stevin, A. Girard, A. Elzevir, and B. Elzevir, *L'arithmetique de Simon Stevin de Bruges, Reveuë, corrigee & augmentee de plusieurs traictez at annotations par Albert Girard Samielois Mathematicien*, L'imprimerie des Elzeviers, Leiden, 1625.

[2] C. Henry, P. de Fermat, and P. Tannery, *Œuvres de Fermat*, Gauthier-Villars et Fils, Paris, 1891.

[3] 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*, Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin **48** (1837), 45–71.

[4] B. F. de Bessy, *Memoires de l'Academie Royale des Sciences*, Tome V, La compagnie des libraires, Paris, 1729.
[5] L. Euler, *De numeris, qui sunt aggregata duorum quadratorum*, Novi Commentarii Academiae Scientiarum Petropolitanae **4** (1758), 3–40.
[6] L. Euler, *Demonstratio theorematis fermatiani omnem numerum primum formae* $4n + 1$ *esse summam duorum quadratorum*, Novi Commentarii Academiae Scientiarum Petropolitanae **5** (1754/5, 1760), 3–13.
[7] J.-L. Lagrange, *Suite des recherches d'arithmétique*, Nouveaux mémoires de l'Académie Royale des Sciences et Belles-Lettres (1775), 323–356.
[8] C. F. Gauß, *Disquisitiones arithmeticae*, Gerh. Fleischer, Leipzig, 1801.
[9] C. F. Gauß, *Untersuchungen über höhere Arithmetik*, Deutsch herausgegeben von H. Maser, Verlag Julius Springer, Berlin, 1889.
[10] R. Dedekind, *Sur la théorie des nombres entiers algébriques*, Bulletin des Sciences Mathématiques et Astronomiques **1** (1877), no. 1, 207–248.
[11] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, Herausgegeben und mit Zusätzen versehen von R. Dedekind. 4. umgearbeitete und vermehrte Auflage, Braunschweig, F. Vieweg u. Sohn. XVII + 657 S. 8° (1894).
[12] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, fourth edition, CRC Press, Boca Raton, FL, 2016.
[13] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990), no. 2, 144.
[14] S. Chowla, *The Riemann hypothesis and Hilbert's tenth problem*, Norske Vid. Selsk. Forh. (Trondheim) **38** (1965), 62–64.
[15] E. Jacobsthal, *Anwendungen einer Formel aus der Theorie der quadratischen Reste*, PhD thesis, Humboldt-Universität zu Berlin, 1906.
[16] S. Wagon, *Editor's corner: the Euclidean algorithm strikes again*, Amer. Math. Monthly **97** (1990), no. 2, 125–129.
[17] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Berlin, 1975.
[18] L. Halbeisen and N. Hungerbühler, *A geometric representation of integral solutions of* $x^2 + xy + y^2 = m^2$, Quaestiones Mathematicae **43** (2020), 425–439.
[19] K. H. Rosen, *Elementary Number Theory and Its Applications*, 4th edition, Addison-Wesley, Reading, MA, 2000.
[20] P. Bachmann, *Niedere Zahlentheorie. Erster Teil; Zweiter Teil: Additive Zahlentheorie*, B. G. Teubner, Leipzig, 1902, 1910.
[21] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer-Verlag, New York, 1985.
[22] J. B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967.
[23] I. Niven, *Irrational numbers*, *The Carus Mathematical Monographs*, No. 11, The Mathematical Association of America, Distributed by John Wiley and Sons, Inc., New York, 1956.
[24] C. Barker, *The On-Line Encyclopedia of Integer Sequences*, http://oeis.org/A230710 A230710, http://oeis.org/A230711 A230711, http://oeis.org/A230622 A230622, http://oeis.org/A230623 A230623, http://oeis.org/A230962 A230962, http://oeis.org/A230963 A230963, Oct, Nov 2013.
[25] Z. Seidov, *The On-Line Encyclopedia of Integer Sequences*, http://oeis.org/A188948 A188948, http://oeis.org/A188949 A188949, Apr 2011.
[26] C. Busenhart, *Investigation on Rational and Integral Circular Point Sets in the Plane*, Master's thesis, ETH Zürich, 2019, 59–60.
[27] S. Cooper and M. Hirschhorn, *On the number of primitive representations of integers as sums of squares*, Ramanujan J. **13** (2007), 7–25.