On Primitive Solutions of the Diophantine Equation $x^2 + y^2 = M$

Chris Busenhart
Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland
chris.busenhart@math.ethz.ch

Lorenz Halbeisen
Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland
lorenz.halbeisen@math.ethz.ch

Norbert Hungerbühler
Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland
norbert.hungerbuehler@math.ethz.ch

Oliver Riesen
Department of Mathematics, ETH Zentrum, Kantonsschule Zug, Lüssiweg 24, 6300 Zug, Switzerland
oliver.riesen@ksz.ch

key-words: Pythagorean primes, Diophantine equation

2020 Mathematics Subject Classification: **11D45** 11D09 11A41

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.

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 $a = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, 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 [24]). Pierre de Fermat [19, tome premier, p. 293, tome troisième, p. 243–246] claimed that each such *Pythagorean prime* and its square is the sums 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, communicated to Huygens (August 14, 1659, see [19, tome deuxième, p. 432]) 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. Recall that by the Dirichlet Prime Number Theorem (see [11]), 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 [9, p. 22–34,156–163]). The theory was finally put on a solid footing by Leonhard Euler who proved Girard's Theorem in two papers (see [14] and [13]). In the sequel, 1775, Joseph-Louis Lagrange gave a proof based on his general theory of integral quadratic forms (see [21, p. 351]). The theory of quadratic forms came to a full understanding with Gauss' *Disquisitiones arithmeticae* [16]. 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 [17, p. 149 f]). Richard Dedekind contributed two more proofs for Girard's Theorem: see [10, §27, p. 240] and [12, 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., [25, §7.2]). The shortest argument is Don Zagier's famous one-sentence proof [27] of Girard's Theorem.

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

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

we have

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

where $\langle u \rangle \in (-\frac{p}{2}, \frac{p}{2})$ denotes the residue of u mod p (see [8, Chapter 5] for a proof). Another explicit formula was found by Jacobsthal in his dissertation [20]: 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 $(\frac{a}{p})$ denotes the Legendre symbol. Both formulae are of more theoretical interest. For an efficient algorithm to compute the primitive solution we refer to [26].

The purpose of this paper is to 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.

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 interger solution of (1). Trivially, we have $(a, b)_M \implies (b, a)_M$ and $(a, b)_M \implies (-a, b)_M$. Now, for two pairs of integers (a, b) and (c, d), we define

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

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*

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

in other words, we have

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

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

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

q.e.d.

The operation (2) reminds of the product of complex numbers. Indeed, as we shall see below, the Gaussian integers $\mathbb{Z}[i]$ are the adequate language to discuss equation (1).

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 solutions for $M = p^k$, k a positive integer, can be generated from this.

As mentioned above, the product (2) from Section 2 corresponds to the complex multiplication if we consider the first and second entry as real and imaginary part, 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*

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

So, from now on we will work with Gaussian integers $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ (see, e.g., [15] 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 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 primitive solution to $x^2 + y^2 = p^k$.*

Proof. By observing that $p^k = \alpha^k\overline{\alpha}^k$, we see that the above equation is satisfied by $|\mathrm{Re}(\alpha^k)|, |\mathrm{Im}(\alpha^k)|$. Thus, it only remains 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. In particular, $\frac{\arg(\alpha)}{\pi} \in \mathbb{Q}$ which is a contradiction to Niven's Theorem. *q.e.d.*

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 we have:

- $p = 5$: $x_k = \min\{a_k, b_k\}$ and $y_k = \max\{a_k, b_k\}$ for $M = 5^k$ are explicit formulas for the integer sequences [1, A230710] and [2, A230711], respectively.
- $p = 13$: $x_k = \min\{a_k, b_k\}$ and $y_k = \max\{a_k, b_k\}$ for $M = 13^k$ are explicit formulas for the integer sequences [22, A188948], and [23, A188949], respectively.
- $p = 17$: $x_k = \min\{a_k, b_k\}$ and $y_k = \max\{a_k, b_k\}$ for $M = 17^k$ are explicit formulas for the integer sequences [3, A230622], and [4, A230623], respectively.
- $p = 73$: $x_k = \min\{a_k, b_k\}$ and $y_k = \max\{a_k, b_k\}$ for $M = 73^k$ are explicit formulas for the integer sequences [5, A230962] and [6, A230963], respectively.

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

In this section we show how one can find the primitive solution to the Diophantine equation $x^2+y^2 = M$, where M is a product of powers of Pythagorean primes. Also strongly related with the following part is [7, 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*

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

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

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 $\lambda = \overline{\lambda} = \prod_{l=1}^{n} \overline{\alpha_l}^{k_l'}$. 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 $\mathbb{Z}[i]$. *q.e.d.*

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

Proposition 5. *Let* $p_1, \ldots, p_n$, $k_1, \ldots, k_n$, *and* M *be as in Theorem 4. Then there are* 2^{n-1} *primitive solutions to* $x^2 + y^2 = M$.

Proof. Let I, I' be a partition of the set $\{1, 2, \ldots, n\}$ and

$$\begin{aligned} M = \prod_{l=1}^{n} p_l^{k_l} &= \Big(\prod_{l=1}^{n} \alpha_l^{k_l}\Big)\overline{\Big(\prod_{l=1}^{n} \alpha_l^{k_l}\Big)} \\ &= \underbrace{\Big(\prod_{l\in I} \alpha_l^{k_l} \overline{\prod_{l\in I'} \alpha_l^{k_l}}\Big)}_{=:\alpha_I} \underbrace{\overline{\Big(\prod_{l\in I} \alpha_l^{k_l} \overline{\prod_{l\in I'} \alpha_l^{k_l}}\Big)}}_{=:\overline{\alpha_I}} \end{aligned}$$

be factorised in $\mathbb{Z}[i]$. Then each I gives us a primitive solution of $M = \mathrm{Re}(\alpha_I)^2 + \mathrm{Im}(\alpha_I)^2$.

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 $I \subset \{1, 2, \ldots, n\}$ and $k \in \{0, 1, 2, 3\}$ such that $x + iy = i^k \alpha_I$. This shows that each primitive solution to the equation above can be constructed by the right choice of I.

It remains to show that $x^2 + y^2 = M$ has exactly 2^{n-1} solutions. For this let I_1 and I_2 be subsets of $\{1, 2, \ldots, n\}$ and assume that α_{I_1} and α_{I_2} represent the same solution, i.e., we have

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

Then we find θ, θ' in $\mathbb{R}$ such that

$$\arg(\alpha_{I_1}) = \theta + \theta' \qquad \text{and} \qquad \arg(\alpha_{I_2}) = \theta - \theta'$$

and it must hold either

$$\theta + \theta' \equiv \theta - \theta' \pmod{\tfrac{\pi}{2}} \qquad \text{or} \qquad \theta + \theta' \equiv -(\theta - \theta') \pmod{\tfrac{\pi}{2}}$$

which implies $\theta \equiv 0 \mod \frac{\pi}{4}$ or $\theta' \equiv 0 \mod \frac{\pi}{4}$. However, since θ and θ' are either arguments of primitive solutions for equations of the form $x^2 + y^2 = M'$, where M' divides M, or I_1, I_2 must be disjoint or equal, we conclude the latter. Furthermore, if I_1 and I_2 are disjoint or equal, then (**) is clearly satisfied, so we get the same primitive solution. Thus, there are exactly 2^{n-1} different choices for I such that the resulting primitive solutions are different from each other. *q.e.d.*

References

[1] Colin Barker, The On-Line Encyclopedia of Integer Sequences, A230710, Oct 2013.

[2] Colin Barker, The On-Line Encyclopedia of Integer Sequences, A230711, Oct 2013.

[3] Colin Barker, The On-Line Encyclopedia of Integer Sequences, A230622, Oct 2013.

[4] Colin Barker, The On-Line Encyclopedia of Integer Sequences, A230623, Oct 2013.

[5] Colin Barker, The On-Line Encyclopedia of Integer Sequences, A230962, Nov 2013.

[6] Colin Barker, The On-Line Encyclopedia of Integer Sequences, A230963, Nov 2013.

[7] Chris Busenhart, Investigation on rational and integral circular point sets in the plane, Master's thesis, ETH Zürich, November 2019.

[8] S. Chowla, The Riemann hypothesis and Hilbert's tenth problem, *Norske Vid. Selsk. Forh. (Trondheim)* **38** (1965), 62–64.

[9] Bernhard Frénicle de Bessy, *Memoires de l'Academie royale des sciences*, Vol. tome V, La compagnie des libraires, Paris, 1729.

[10] Richard Dedekind, Sur la théorie des nombres entiers algébriques, *Bulletin des Sciences Mathématiques et Astronomiques* **2e série, 1**(1) (1877), 207–248.

[11] P. G. Lejeune 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.

[12] Peter Gustav Lejeune 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)., 1894.

[13] Leonhard 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.

[14] Leonhard Euler, De numeris, qui sunt aggregata duorum quadratorum, *Novi Commentarii academiae scientiarum Petropolitanae* **4** (1758), 3–40.

[15] John B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967.

[16] Carl Friedrich Gauß, *Disquisitiones arithmeticae*, Gerh. Fleischer, Jun., 1801.

[17] Carl Friedrich Gauss, *Untersuchungen über höhere Arithmetik*, Deutsch herausgegeben von H. Maser, Verlag Julius Springer, Berlin, 1889.

[18] Lorenz Halbeisen and Norbert Hungerbühler, A geometric representation of integral solutions of $x^2 + xy + y^2 = m^2$, *Quaestiones Mathematicae* **43** (2020), 425–439.

[19] Charles Henry, Pierre de Fermat, and Paul Tannery, *Œuvres de Fermat*, Gauthier-Villars et Fils, Paris, 1891.

[20] Ernst Jacobsthal, *Anwendungen einer Formel aus der Theorie der quadratischen Reste*, PhD thesis, Humboldt-Universität zu Berlin, 1906.

[21] Joseph-Louis Lagrange, Suite des recherches d'arithmétique, *Nouveaux mémoires de l'Académie Royale des Sciences et Belles-Lettres* (1775), 323–356.

[22] Zak Seidov, The On-Line Encyclopedia of Integer Sequences, A188948, Apr 2011.

[23] Zak Seidov, The On-Line Encyclopedia of Integer Sequences, A188949, Apr 2011.

[24] Simon Stevin, Albert Girard, Abraham Elzevir, and Bonaventura 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, 1625.

[25] Ian Stewart and David Tall, *Algebraic number theory and Fermat's last theorem*, CRC Press, Boca Raton, FL, fourth edition, 2016.

[26] Stan Wagon, Editor's corner: the Euclidean algorithm strikes again, *Amer. Math. Monthly* **97**(2) (1990), 125–129.

[27] D. Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, *Amer. Math. Monthly* **97**(2) (1990), 144.