GEOMETRIC SUMS AS SUMS OF TWO SQUARES

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

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

Franz Lemmermeyer
Jagstzell, Germany
franz.lemmermeyer@gmx.de

Received: 8/16/25, Revised: 9/15/25, Accepted: 1/14/26, Published: 2/20/26

Abstract

We consider the geometric sum $1 + p^n + p^{2n} + p^{3n} + \ldots + p^{(p-1)n}$ and show that for odd n and primes p with $p \equiv 3 \pmod 4$, this sum has only Pythagorean prime divisors, *i.e.*, primes q of the form $q \equiv 1 \pmod 4$. Similarly, the geometric sum $1 - p^n + p^{2n} - \ldots + p^{(p-1)n}$ has the same property if n is even and p an odd prime, or if n is an arbitrary positive integer and p a Pythagorean prime. In particular, these geometric sums can be written as the sum of squares of two natural numbers a, b. Explicit formulas for a and b are obtained by results on the representation of the cyclotomic polynomials Φ_{4p} as the sum of two squares.

1. Introduction

In [8], Koopa Tak-Lun Koo proposed the following two problems.

(a) Show that when n is an odd positive integer, $1+7^n+7^{2n}+7^{3n}+7^{4n}+7^{5n}+7^{6n}$ is a sum of two squares.

(b) Show that when n is even, the expression in part (a) is not a sum of two squares.

Recall that an integer $n > 1$ can be written as a sum of two squares if and only if the prime decomposition of n contains no factor p^k, where $p \equiv 3 \pmod 4$ and k is odd (see [6, Section 182]). Moreover, an odd integer n can be written as $n = a^2 + b^2$ where a, b can be chosen to be relatively prime, if and only if n is the product of

DOI: 10.5281/zenodo.18714425

Pythagorean primes, *i.e.*, primes p with $p \equiv 1 \pmod 4$ (see [5, p. 22–34,156–163], [7, Chapter 2] or [2]).

If n is even, then $1+7^n+\ldots+7^{6n} \equiv 3 \pmod 4$, *i.e.*, Problem (b) follows directly from Gauss's sum of two squares theorem mentioned above. However, one can ask whether Problem (a) can be generalized to prime numbers different from 7. In particular, a natural generalization is to ask whether for each positive odd integer n and for each (prime) integer p, the expression $1+p^n+p^{2n}+p^{3n}+\ldots+p^{(p-1)n}$ is the sum of two squares. Using Gauss's characterization one can easily verify that for $n=1$ and for *non-primes* p or for primes $p \equiv 1 \pmod 4$, $1+p+p^2+p^3+\ldots+p^{p-1}$ is in general *not* the sum of two squares. The aim of this article is to investigate the conditions under which geometric sums—similar to the above form—have only Pythagorean prime divisors and are therefore the sum of the squares of two natural numbers. In particular, it follows from Theorem 10 that for all odd integers n, $1+7^n+7^{2n}+7^{3n}+7^{4n}+7^{5n}+7^{6n}$ is a sum of two squares.

The article is organized as follows. In Section 2 we show that for p an odd prime the cyclotomic polynomial Φ_{4p} is the sum of squares of two polynomials. The precise statements are given in Propositions 1 and 2, with a generalization in Corollary 3 and an explicit formula for the general case when p is not a prime number. In Section 3, we consider the conditions under which $1-p^n+p^{2n}-\ldots+p^{(p-1)n}$ has only Pythagorean prime divisors. It turns out that this is the case if n is even and p an odd prime (Theorem 5), and if n is an arbitrary natural number and p a Pythagorean prime (Theorem 7). In particular, the results from Section 2 yield an explicit formula for the two squares. Theorem 6 is about geometric sums of the form $x^{4n}-x^{4n-2}y^2+\ldots+x^4y^{4n-4}-x^2y^{4n-2}+y^{4n}$ with $(x,y)=1$. In Corollary 8 we consider the case when p is replaced by the power of a Pythagorean prime in the above alternating sum. The methods which we apply lead to a proof of the Aurifeuillian factorization of $\frac{p^p+1}{p+1}$ in Proposition 9 and of $\frac{p^p-1}{p-1}$ in Proposition 12. In Section 4, we consider the geometric sum $1+p^n+p^{2n}+\ldots+p^{(p-1)n}$. The main result, which is Theorem 10, states that this sum has only Pythagorean prime divisors if n is odd and p is a non-Pythagorean prime. Again, by considering the cyclotomic polynomial Φ_{4p}, an explicit formula for the two squares can be given. Corollary 11 extends the result to powers of non-Pythagorean primes.

2. On Cyclotomic Polynomials

In order to investigate geometric sums of the form $1+p^n+p^{2n}+p^{3n}+\ldots+p^{(p-1)n}$ we set $n=1$ and replace the odd prime p by a variable x. This way, we obtain the cyclotomic polynomial $\Phi_p(x) := 1+x+x^2+\ldots+x^{p-1}$.

In general, for any positive integer n, let ζ_n be a primitive n-th root of unity and

let

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ (k,n)=1}} (x - \zeta_n^k)$$

denote the n-th cyclotomic polynomial. Then, for odd primes p we have

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 \qquad \text{and}$$
$$\Phi_{4p}(x) = x^{2(p-1)} - x^{2(p-2)} + \ldots - x^2 + 1.$$

In particular, since p is odd, we have

$$\Phi_{4p}(i\sqrt{x}) = (-x)^{p-1} - (-x)^{p-2} + \ldots - (-x) + 1 = \Phi_p(x).$$

Let p be an odd prime and let L be the splitting field of Φ_{4p} over $\mathbb{Q}$. Then the Galois group of $L/\mathbb{Q}$ is isomorphic to the group of coprime residue classes $G := (\mathbb{Z}/4p\mathbb{Z})^\times$, where a residue class $a \pmod{4p}$ represents the automorphism defined by $\sigma_a : \zeta_{4p} \mapsto \zeta_{4p}^a$ (see Washington [21, Thm. 2.5]). Observe that σ_{-1} is complex conjugation. Since the group G is abelian, every subgroup of G is a normal subgroup, which implies that all intermediate fields of the field extension $L/\mathbb{Q}$ are *normal* field extension of $\mathbb{Q}$. Furthermore, since $G \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ and the multiplicative group of $(\mathbb{Z}/p\mathbb{Z})$ is cyclic of order $p-1$, we have $G \cong C_2 \times C_{p-1}$, where C_n denotes the cyclic group of order n. Thus, there are three subgroups of index 2 in G. Two of these three subgroups are isomorphic to C_{p-1} and one is isomorphic to $C_2 \times C_{(p-1)/2}$, which implies that in the case when $p \equiv 3 \pmod 4$, all three subgroups are cyclic.

We illustrate these three subgroups for $p = 13$. Let $\overline{g}_p \in \mathbb{Z}/p\mathbb{Z}$ be a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. For example, for $g_{13} = 2$ we have

$$\langle \overline{g}_{13} \rangle = \left(\{\overline{2}, \overline{4}, \overline{8}, \overline{3}, \overline{6}, \overline{12}, \overline{11}, \overline{9}, \overline{5}, \overline{10}, \overline{7}, \overline{1}\}, \cdot \right).$$

By the Chinese Remainder Theorem, there exists a $\overline{h}_p \in \mathbb{Z}/4p\mathbb{Z}$, such that $h_p \equiv g_p \pmod p$ and $h_p \equiv 1 \pmod 4$, *e.g.*, $h_{13} = 41$ has this property for $p = 13$. Then $\langle \overline{h}_p \rangle$ and $\langle \overline{2}\overline{p} + \overline{h}_p \rangle$ are two different subgroups of index 2 in G. For example we have

$$\begin{aligned} \langle \overline{41} \rangle &= \left(\{\overline{41}, \overline{17}, \overline{21}, \overline{29}, \overline{45}, \overline{25}, \overline{37}, \overline{9}, \overline{5}, \overline{49}, \overline{33}, \overline{1}\}, \cdot \right), \\ \langle \overline{26} + \overline{41} \rangle &= \left(\{\overline{15}, \overline{17}, \overline{47}, \overline{29}, \overline{19}, \overline{25}, \overline{11}, \overline{9}, \overline{31}, \overline{49}, \overline{7}, \overline{1}\}, \cdot \right). \end{aligned}$$

For the third subgroup of index 2 in G, let $\overline{k}_p \in \mathbb{Z}/4p\mathbb{Z}$ be such that $k_p \equiv g_p^2 \pmod p$ and $k_p \equiv 3 \pmod 4$, *e.g.*, $k_{13} = 43$ has this property for $p = 13$ and $g_{13} = 2$. Then

$$\left(\left\{ \overline{k}_p^{\,i} : 1 \le i \le \tfrac{p-1}{2} \right\} \cup \left\{ \overline{2}\overline{p} + \overline{k}_p^{\,i} : 1 \le i \le \tfrac{p-1}{2} \right\}, \cdot \right)$$

is a subgroup of index 2 in G, where for $p \equiv 3 \pmod 4$, this subgroup is isomorphic to $\langle \overline{k}_p \rangle$. For example, for $p = 13$ and $k_{13} = 43$ we obtain the group

$$\left(\left\{ \overline{43}, \overline{29}, \overline{51}, \overline{9}, \overline{23}, \overline{1} \right\} \cup \left\{ \overline{17}, \overline{3}, \overline{25}, \overline{35}, \overline{49}, \overline{27} \right\}, \cdot \right).$$

The quadratic subextensions of the field extension $L/\mathbb{Q}$ are the fixed fields of the three subgroups of index 2 in G. To find the three quadratic intermediate fields, let p be an odd prime and let ζ_p be a primitive p-th root of unity. First notice that $\zeta_{4p} = i\zeta_p$ is a primitive $4p$-th root of unity. So, we have that $\zeta_{4p} + \zeta_{4p}^{-1} = i\zeta_p - i\zeta_p^{-1} = i(\zeta_p - \zeta_p^{-1})$. In particular, $i \in L$, which gives us the quadratic subextension $\mathbb{Q}(i)$. Furthermore (see, for example, [11, Prp. 3.21, p. 96]), we have

$$\sum_{k=1}^{p-1} \left(\frac{k}{p} \right) \zeta_p^k = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where $\left(\frac{k}{p} \right)$ is the Legendre symbol. Thus, since $i \in L$, for odd primes p we obtain the two quadratic subextensions $\mathbb{Q}(\sqrt{-p}\,) = \mathbb{Q}(i\sqrt{p}\,)$ and $\mathbb{Q}(\sqrt{p}\,)$.

So, the fixed fields of the three subgroups of index 2 in G are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-p}\,)$, and $\mathbb{Q}(\sqrt{p}\,)$. For $\widetilde{H}_1 := \mathrm{Gal}\big(L/\mathbb{Q}(i)\big)$, $\widetilde{H}_2 := \mathrm{Gal}\big(L/\mathbb{Q}(\sqrt{-p}\,)\big)$, and for $\widetilde{H}_3 := \mathrm{Gal}\big(L/\mathbb{Q}(\sqrt{p}\,)\big)$, we have that these groups are isomorphic to the multiplicative groups

$$\begin{aligned} H_1 &= \{a \pmod{4p} : (a, 4p) = 1 \text{ and } (\tfrac{-4}{a}) = +1\}, \\ H_2 &= \{a \pmod{4p} : (a, 4p) = 1 \text{ and } (\tfrac{-4p}{a}) = +1\}, \\ H_3 &= \{a \pmod{4p} : (a, 4p) = 1 \text{ and } (\tfrac{4p}{a}) = +1\}, \end{aligned}$$

where $(\frac{m}{n})$ is the Jacobi symbol.

In order to see this, fix a primitive p-th root of unity ζ_p and let $\zeta_{4p} := i\zeta_p$. Then ζ_{4p} is a primitive $4p$-th root of unity, $L = \mathbb{Q}(\zeta_{4p})$, and $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/4p\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$. For $(r, s) \in (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ define the element $\sigma_{(r,s)} \in \mathrm{Gal}(L/\mathbb{Q})$ by stipulating

$$\sigma_{(r,s)}(\zeta_{4p}) := i^r \zeta_p^s.$$

Clearly the elements $(1, s)$ fix $\mathbb{Q}(i)$, and these correspond to residue classes a mod $4p$ that satisfy $a \equiv 1 \pmod 4$, *i.e.*, $(\frac{-4}{a}) = +1$.

Now, for odd primes p, let p^* be either $+p$ or $-p$, so that $p^* \equiv 1 \pmod 4$. Then, since the automorphisms $\sigma_s : \zeta_p \mapsto \zeta_p^s$ with $(\frac{s}{p}) = (\frac{p^*}{s}) = +1$ fix the quadratic subfield of $\mathbb{Q}(\zeta_p)$, which is $\mathbb{Q}(\sqrt{p^*}\,)$, the automorphisms $\sigma_{(r,s)}$ with $(\frac{p}{s}) = +1$ fix the subfield $\mathbb{Q}(\sqrt{p^*}\,)$ of $\mathbb{Q}(\zeta_{4p})$.

For the other intermediate fields of $L/\mathbb{Q}$, let ζ_p be again a primitive p-th root of unity. Then, the maximal real subfield of L is $\mathbb{Q}\left(i(\zeta_p - \zeta_p^{-1})\right)$. To see this, recall

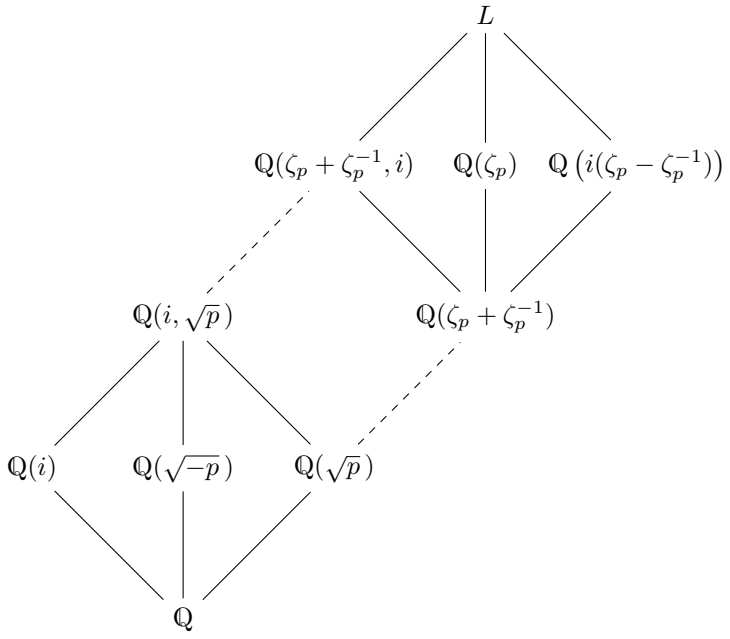

Figure 1: Subfield Diagram of $L = \mathbb{Q}(\zeta_{4p})$.

that $\zeta_{4p} = i\zeta_p$ is a primitive $4p$-th root of unity and that $\zeta_{4p} + \zeta_{4p}^{-1} = i(\zeta_p - \zeta_p^{-1})$. Figure 1 shows some of the intermediate fields of the field extension $L/\mathbb{Q}$.

The next result follows in part from the formulas of Gauss (see [6, Sections 356–357], [4, Chapter 5 and Supplement 7], [9, pp. 93–129], and [10, pp. 1–5]), and Lucas, Aurifeuille and Le Lasseur (see [9, pp. 87–88], [13, p. 276], [14, p. 785], [15, 18, 1], and [17, pp. 436–456]). However, since the theory is quite widely scattered in the literature, we give a direct proof here so that the text is self-contained.

Proposition 1. *Let p be an odd prime. Then the cyclotomic polynomial $\Phi_{4p}(x)$ can be written in the form*

$$\Phi_{4p}(x) = X_1^2 + Y_1^2 = X_2^2 + pY_2^2 = X_3^2 - pY_3^2,$$

where $X_1, Y_1,\ 2X_2, 2Y_2,\ 2X_3, 2Y_3 \in \mathbb{Z}[x]$. Moreover, if $p \equiv 1 \pmod 4$, then $X_2, Y_2 \in \mathbb{Z}[x]$, and if $p \equiv 3 \pmod 4$, then $X_3, Y_3 \in \mathbb{Z}[x]$. In addition, the polynomials X_1, X_2 and X_3 are even and the polynomial Y_1 is odd; for $p \equiv 1 \pmod 4$, Y_2 is odd and Y_3 is even; and for $p \equiv 3 \pmod 4$, Y_2 is even and Y_3 is odd.

For proving our main result concerning the representation of certain geometric sums as sums of two squares, it is sufficient that the polynomials X_j have rational

coefficients. This is because an integer that is the sum of two rational squares is always the sum of two integral squares.

Proof of Proposition 1. We have $\Phi_{4p}(x) = \prod(x - \zeta^k)$, where ζ is a primitive $4p$-th root of unity and k runs through the coprime residue classes modulo $4p$. With respect to the three multiplicative groups $H_j \le (\mathbb{Z}/4p\mathbb{Z})^\times$ $(1 \le j \le 3)$ defined above, we define three polynomials f_j of degree $p-1$ and their conjugates g_j by stipulating

$$f_j(x) = \prod_{k \in H_j} (x - \zeta^k), \qquad g_j(x) = \prod_{k \in G \setminus H_j} (x - \zeta^k). \tag{1}$$

Since f_j is fixed by the automorphisms $\sigma_a : \zeta \mapsto \zeta^a$ with $a \in H_j$, we see that the polynomials f_j have coefficients that lie in the rings of integers of the three quadratic subfields of $L = \mathbb{Q}(\zeta_{4p})$, namely

$$K_1 := \mathbb{Q}(i), \quad K_2 := \mathbb{Q}(\sqrt{-p}\,), \quad \text{and} \quad K_3 := \mathbb{Q}(\sqrt{p}\,).$$

Thus, we can write $f_1(x) = X_1(x) + iY_1(x)$ and $g_1(x) = X_1(x) - iY_1(x)$, where $X_1, Y_1 \in \mathbb{Q}[x]$, and obtain

$$\Phi_{4p}(x) = \prod_{k \in G} (x - \zeta^k) = f_1(x)\, g_1(x) = X_1^2(x) + Y_1^2(x).$$

Similarly, there are $X_2, Y_2 \in \mathbb{Q}[x]$ such that $f_2(x) = X_2(x) + \sqrt{-p}\, Y_2(x)$ and $g_2(x) = X_2(x) - \sqrt{-p}\, Y_2(x)$, which implies $\Phi_{4p}(x) = X_2^2(x) + pY_2^2(x)$, and finally, there are $X_3, Y_3 \in \mathbb{Q}[x]$ such that $f_3(x) = X_3(x) + \sqrt{p}\, Y_3(x)$ and $g_3(x) = X_3(x) - \sqrt{p}\, Y_3(x)$, which implies $\Phi_{4p}(x) = X_3^2(x) - pY_3^2(x)$.

Notice that we have

$$\begin{aligned}
X_1(x) &= \tfrac{1}{2}\big(f_1(x) + g_1(x)\big), & Y_1(x) &= \tfrac{1}{2i}\big(f_1(x) - g_1(x)\big), \\
X_2(x) &= \tfrac{1}{2}\big(f_2(x) + g_2(x)\big), & Y_2(x) &= \tfrac{1}{2\sqrt{-p}}\big(f_2(x) - g_2(x)\big), \\
X_3(x) &= \tfrac{1}{2}\big(f_3(x) + g_3(x)\big), & Y_3(x) &= \tfrac{1}{2\sqrt{p}}\big(f_3(x) - g_3(x)\big).
\end{aligned}$$

Concerning the parity of these polynomials we first show that X_1 is even and Y_1 is odd. For this, we show that $f_1 + g_1$ is even. Recall that

$$H_1 = \big\{k : \ 1 \le k \le 4p-1, \ (\tfrac{-4}{k}) = +1, \ (k, 4p) = 1\big\}$$

and that $|H_1| = p - 1$. Now,

$$f_1(-x) = \prod_{k \in H_1} (-x - \zeta^k) = (-1)^{p-1} \prod_{k \in H_1} (x + \zeta^k) = \prod_{k \in H_1} (x + \zeta^k).$$

By definition of H_1 we have that if $k \in H_1$, then $k \equiv 1 \pmod 4$, which implies that $2p + k \equiv 3 \pmod 4$, and since $(k, 4p) = 1$, we have $(2p + k, 4p) = 1$. Thus, we obtain

$$f_1(-x) = \prod_{k \in H_1} (x + \zeta^k) = \prod_{k \in H_1} (x - \zeta^{2p+k}) = g_1(x)\,,$$

which implies that

$$X_1(x) = \frac{1}{2}\big(f_1(x) + g_1(x)\big) = \frac{1}{2}\big(f_1(x) + f_1(-x)\big)$$

is even as claimed. Furthermore,

$$Y_1(x) = \frac{1}{2i}\big(f_1(x) - g_1(x)\big) = \frac{1}{2i}\big(f_1(x) - f_1(-x)\big)$$

and hence, Y_1 is odd, as claimed.

Now, we investigate the parity of the polynomials X_2 and Y_2. For this, we consider f_2. Recall that

$$H_2 := \big\{k :\ 1 \le k \le 4p-1,\ (\tfrac{-4p}{k}) = +1,\ (k, 4p) = 1\ \big\}$$

and that $|H_2| = p - 1$. We find again that

$$f_2(-x) = \prod_{k \in H_2} (x - \zeta^{2p+k}).$$

Assume first that $p \equiv 1 \pmod 4$. Then

$$\begin{aligned}\Big(\frac{-4p}{2p+k}\Big) &= \Big(\frac{-4}{2p+k}\Big)\Big(\frac{p}{2p+k}\Big) = -\Big(\frac{-1}{k}\Big)\Big(\frac{p}{2p+k}\Big) \\ &= -\Big(\frac{-1}{k}\Big)\Big(\frac{2p+k}{p}\Big) = -\Big(\frac{-1}{k}\Big)\Big(\frac{k}{p}\Big) = -\Big(\frac{-1}{k}\Big)\Big(\frac{p}{k}\Big) = -\Big(\frac{-4p}{k}\Big). \quad (2)\end{aligned}$$

Here, we have used that $2p + k \equiv 2 + k \pmod 4$ and the quadratic reciprocity law $(\frac{-1}{m}) = (-1)^{\frac{m-1}{2}}$, which implies

$$\Big(\frac{-1}{2p+k}\Big) = (-1)^{\frac{(2p+k)-1}{2}} = (-1)^{\frac{(k+2)-1}{2}} = (-1)^{\frac{2+(k-1)}{2}} = -\Big(\frac{-1}{k}\Big).$$

Furthermore, we have used that $2p + k \equiv k \pmod p$ and the quadratic reciprocity law $(\frac{m}{q}) = (\frac{q^*}{m})$, where in our case we have $p^* = p$.

We give a second, shorter proof of Equation (2) which uses the fact, that the Legendre symbol $(\frac{a}{\cdot})$ is a Dirichlet character (see [12, Chapter 3] or [19, Section 22]). Using this we have directly

$$\Big(\frac{-4p}{2p+k}\Big) = \Big(\frac{-1}{2p+k}\Big)\Big(\frac{p}{2p+k}\Big) = -\Big(\frac{-1}{k}\Big)\Big(\frac{p}{k}\Big)$$

where p is the conductor of the character.

Thus, we get again $f_2(-x) = g_2(x)$, which implies that X_2 is even and Y_2 is odd.

Assume now that $p \equiv 3 \pmod 4$. Then, using again the conductor p, we have

$$\Big(\frac{-4p}{2p+k}\Big) = \Big(\frac{-p}{2p+k}\Big) = \Big(\frac{-p}{k}\Big) = \Big(\frac{-4p}{k}\Big).$$

Thus, f_2 and g_2 are even, which implies that X_2 and Y_2 are both even.

Finally, we investigate the parity of the polynomials X_3 and Y_3. For this, we consider f_3. Recall that

$$H_3 := \big\{k:\ 1 \le k \le 4p-1,\ (\frac{4p}{k}) = +1,\ (k,4p) = 1\ \big\}$$

and that $|H_3| = p-1$. Again, we have

$$f_3(-x) = \prod_{k\in H_3} (x - \zeta^{2p+k}).$$

For $p \equiv 1 \pmod 4$ we have as above

$$\Big(\frac{4p}{2p+k}\Big) = \Big(\frac{p}{2p+k}\Big) = \Big(\frac{p}{k}\Big) = \Big(\frac{4p}{k}\Big).$$

Thus, f_3 and g_3 are even, which implies that X_3 and Y_3 are both even.

Now, assume that $p \equiv 3 \pmod 4$. Then

$$\begin{aligned}\Big(\frac{4p}{2p+k}\Big) = \Big(\frac{p}{2p+k}\Big) = \Big(\frac{(-1)(-p)}{2p+k}\Big) &= \Big(\frac{-1}{2p+k}\Big)\Big(\frac{-p}{2p+k}\Big)\\ = -\Big(\frac{-1}{k}\Big)\Big(\frac{-p}{k}\Big) = -\Big(\frac{p}{k}\Big) &= -\Big(\frac{4p}{k}\Big).\end{aligned}$$

Thus, we get again $f_3(-x) = g_3(x)$, which implies that X_3 is even and Y_3 is odd.

Next we show that $X_1, Y_1 \in \mathbb{Z}[x]$, that $X_2, Y_2 \in \mathbb{Z}[x]$ for $p \equiv 1 \pmod 4$, and that $X_3, Y_3 \in \mathbb{Z}[x]$ for $p \equiv 3 \pmod 4$. For this, we first show that the coefficients of the polynomials f_j and g_j (for $1 \le j \le 3$) are algebraic integers which belong to K_j, *i.e.*, the coefficients of f_j and g_j are roots of monic polynomials with coefficients in $\mathbb{Z}$. To see this, recall that the roots of Φ_{4p} are algebraic integers and notice that the coefficients of f_j and g_j are sums of products of roots of Φ_{4p}. Hence, the coefficients of f_j and g_j are algebraic integers (see Marcus [16, Cor. 1 on p. 12]). Furthermore, since $H_j \cong \mathrm{Gal}(L/K_j)$, the coefficients of f_j and g_j are in K_j. Now, by Marcus [16, Cor. 2 on p. 11] we have that for squarefree integers m, the set of algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{m})$ is

$$\begin{cases} \big\{a + b\sqrt{m} : a, b \in \mathbb{Z}\big\} & \text{if } m \equiv 2 \text{ or } 3 \pmod 4\,,\\ \big\{\frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z},\ a \equiv b \pmod 2\big\} & \text{if } m \equiv 1 \pmod 4\,. \end{cases}$$

In particular, for $m = -1$ we find that the algebraic integers in $\mathbb{Q}(i)$ are of the form $a + b\sqrt{m}$ where $a, b \in \mathbb{Z}$, which implies that $X_1, Y_1 \in \mathbb{Z}[x]$, and for odd primes p we see that for $p \equiv 1 \pmod 4$ the algebraic integers in $\mathbb{Q}(\sqrt{-p})$ have the form $a + b\sqrt{-p}$ where $a, b \in \mathbb{Z}$, and for $p \equiv 3 \pmod 4$ the algebraic integers in $\mathbb{Q}(\sqrt{p})$ have the form $a + b\sqrt{p}$ where $a, b \in \mathbb{Z}$. Therefore, we obtain that $X_2, Y_2 \in \mathbb{Z}[x]$ for $p \equiv 1 \pmod 4$ and that $X_3, Y_3 \in \mathbb{Z}[x]$ for $p \equiv 3 \pmod 4$. □

Example. For $p = 11$ and $p = 13$, we obtain the following polynomials. Notice that for $p = 11$, $X_3, Y_3 \in \mathbb{Z}[x]$.

$p = 11$

$$\begin{aligned} X_1(x) &= x^{10} - x^8 + x^6 - x^4 + x^2 - 1 & Y_1(x) &= x^9 - x^7 + x^5 - x^3 + x \\ 2X_2(x) &= 2x^{10} - x^8 - 2x^6 - 2x^4 - x^2 + 2 & 2Y_2(x) &= x^8 - x^2 \\ X_3(x) &= x^{10} + 5x^8 - x^6 - x^4 + 5x^2 + 1 & Y_3(x) &= x^9 + x^7 - x^5 + x^3 + x \end{aligned}$$

$p = 13$

$$\begin{aligned} X_1(x) &= x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1 \\ Y_1(x) &= x^{11} - x^9 + x^7 - x^5 + x^3 - x \\ X_2(x) &= x^{12} - 7x^{10} + 15x^8 - 19x^6 + 15x^4 - 7x^2 + 1 \\ Y_2(x) &= x^{11} - 3x^9 + 5x^7 - 5x^5 + 3x^3 - x \\ 2X_3(x) &= 2x^{12} - x^{10} + 4x^8 + x^6 + 4x^4 - x^2 + 2 \\ 2Y_3(x) &= x^{10} + x^6 + x^2 \end{aligned}$$

We now show that the polynomials X_1 and Y_1 can always be given explicitly.

Proposition 2. *For each odd prime p there are polynomials $X_1, Y_1 \in \mathbb{Z}[x]$ such that*

$$\Phi_{4p}(x) = X_1^2 + Y_1^2,$$

where

$$\begin{aligned} X_1 &= x^{p-1} - x^{p-3} \pm \ldots - (-1)^{(p-1)/2}x^2 + (-1)^{(p-1)/2} \quad \textit{and} \\ Y_1 &= x^{p-2} - x^{p-4} \pm \ldots + (-1)^{(p-1)/2}x^3 - (-1)^{(p-1)/2}x. \end{aligned}$$

Proof. It is sufficient to show that $X_1^2 + Y_1^2 = 0$ for all primitive $4p$-th roots of unity ζ_{4p}. Choose $\zeta_{4p} = i\zeta_p$. Then

$$\begin{aligned} X_1(\zeta_{4p}) &= \zeta_p^{p-1} + \zeta_p^{p-3} + \ldots + \zeta_p^2 + 1, \\ Y_1(\zeta_{4p}) &= i\zeta_p(\zeta_p^{p-3} + \ldots + \zeta_p^2 + 1), \end{aligned}$$

and hence we have

$$\begin{aligned}
X_1(\zeta_{4p})^2 + Y_1(\zeta_{4p})^2 &= \left(\zeta_p^{p-1} + \zeta_p^{p-3} + \ldots + \zeta_p^2 + 1\right)^2 - \zeta_p^2 \left(\zeta_p^{p-3} + \ldots + \zeta_p^2 + 1\right)^2 \\
&= \left(\zeta_p^{p-1} + \zeta_p^{p-3} + \ldots + \zeta_p^2 + 1 - \zeta_p(\zeta_p^{p-3} + \ldots + \zeta_p^2 + 1)\right) \cdot \\
&\qquad \left(\zeta_p^{p-1} + \zeta_p^{p-3} + \ldots + \zeta_p^2 + 1 + \zeta_p(\zeta_p^{p-3} + \ldots + \zeta_p^2 + 1)\right) \\
&= \left(\zeta_p^{p-1} - \zeta_p^{p-2} + \ldots - \zeta_p + 1\right) \cdot \underbrace{\left(\zeta_p^{p-1} + \zeta_p^{p-2} + \ldots + \zeta_p + 1\right)}_{=0} \\
&= 0,
\end{aligned}$$

as claimed. □

The formulas in Proposition 2 can easily be generalized to powers of primes if we use a well-known identity for cyclotomic polynomials.

Corollary 3. *Let p be an odd prime and k a natural number. Then we have*

$$\Phi_{4p^k}(x) = X_1^2(x^{p^{k-1}}) + Y_1^2(x^{p^{k-1}}),$$

where X_1 and Y_1 are the polynomials from Proposition 2.

Proof. Recall that for $n = p^k r$, with r relatively prime to p, we have

$$\Phi_n(x) = \Phi_{pr}(x^{p^{k-1}}).$$

Using this general identity for $r = 4$, we get

$$\Phi_{4p^k}(x) = \Phi_{4p}(x^{p^{k-1}}) = X_1^2(x^{p^{k-1}}) + Y_1^2(x^{p^{k-1}})$$

by Proposition 2, as claimed. □

Proposition 2 expresses the cyclotomic polynomial $\Phi_{4p}(x)$ for an odd prime number p as the sum of two explicitly given squares, and with the help of a known relation for cyclotomic polynomials, this also applies for Φ_{4p^k} in Corollary 3 . In fact, this is also possible for Φ_{4q} for general composite numbers $q \geq 1$ instead of odd prime numbers p and their powers. To see this, we note that the calculation of the polynomials X_1 and Y_1 in the proof of Proposition 1 also works for such numbers q. However, in this case, we cannot expect such an explicit form of the squares as in Proposition 2 and Corollary 3. In general, the following holds.

Proposition 4. *Let $q \geq 1$ be a natural number, and define*

$$F(x) = \prod_{\substack{1 \leq k \leq 4q \\ (k,4q)=1 \\ k \equiv 1 \bmod 4}} (x - e^{2k\pi i/(4q)}). \tag{3}$$

Then we have $\Phi_{4q}(x) = A^2 + B^2$*, where* $A, B \in \mathbb{Z}[x]$ *are given by* $A(x) = (F(x) + \overline{F}(x))/2$ *and* $B(x) = (F(x) - \overline{F}(x))/(2i)$*, where* $\overline{F}(x)$ *is the complex conjugate of* $F(x)$*.*

Proof. Let

$$G(x) \;=\; \prod_{\substack{1\le k\le 4q\\(k,4q)=1\\k\equiv 3 \bmod 4}} (x - e^{2k\pi i/(4q)}) \;=\; \prod_{\substack{-1\ge k\ge -4q\\(k,4q)=1\\k\equiv 1 \bmod 4}} (x - e^{2k\pi i/(4q)})\,.$$

Then we have $\Phi_{4q}(x) = F(x)G(x)$, since all factors of $\Phi_{4q}(x)$ appear either in $F(x)$ or in $G(x)$. Observe also that $G(x) = \overline{F}(x)$, *i.e.*, $F(x) = A(x) + iB(x)$ and $G(x) = A(x) - iB(x)$. Thus, we have

$$\Phi_{4q}(x) = F(x)G(x) = (A(x) + iB(x))(A(x) - iB(x)) = A(x)^2 + B(x)^2.$$

Notice that for odd k we have

$$\Big(\frac{-4}{k}\Big) = 1 \text{ if and only if } k \equiv 1 \bmod 4. \tag{4}$$

Indeed, $k \equiv 1 \bmod 4$ implies $(\frac{-1}{k}) = 1$. Hence, by the general relation

$$\Big(\frac{2a}{k}\Big) = \Big(\frac{2}{k}\Big)\Big(\frac{a}{k}\Big) = \begin{cases} (\frac{a}{k}) & \text{if } k \equiv 1 \text{ or } 7 \bmod 8 \\ -(\frac{a}{k}) & \text{if } k \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$$

it follows with $a = -1$ that

$$\Big(\frac{-2}{k}\Big) = \begin{cases} 1 & \text{if } k \equiv 1 \text{ or } 7 \bmod 8 \\ -1 & \text{if } k \equiv 3 \text{ or } 5 \bmod 8, \end{cases}$$

and from this with $a = -2$ that $(\frac{-4}{k}) = 1$ in both cases, $k \equiv 1$ or $7 \bmod 8$, and $k \equiv 3$ or $5 \bmod 8$. Similarly, if $k \equiv 3 \bmod 4$, we find that $(\frac{-1}{k}) = -1$. Hence, because of Equation (4), the polynomial $f_1(x)$ in Equation (1) coincides with the polynomial $F(x)$ in Equation (3). In particular, $F(x)$ has coefficients in $\mathbb{Z}[i]$, and we are done. □

3. On $1 - p^n + p^{2n} - \ldots + p^{(p-1)n} = a^2 + b^2$

Theorem 5. *Let* n *be a positive even integer, and* p *an odd prime. Then the geometric sum*

$$1 - p^n + p^{2n} - p^{3n} + \ldots - p^{(p-2)n} + p^{(p-1)n}$$

is the product of Pythagorean primes; in fact it is the sum of the squares of two natural numbers a, b *which are relatively prime.*

Proof. Let p be an odd prime and let $n = 2k$ be even. Write

$$\Phi_{4p}(x) = X_1^2 + Y_1^2$$

for X_1 and Y_1 as in Proposition 2. So, for all x we have

$$x^{2(p-1)} - x^{2(p-2)} + \ldots - x^2 + 1 = \\ \left(x^{p-1} - x^{p-3} + \ldots + x^2 - 1\right)^2 + x^2\left(x^{p-3} - x^{p-5} + \ldots - x^2 + 1\right)^2.$$

If we replace x by $\sqrt{p^n} = \sqrt{p^{2k}} = p^k$, then we obtain

$$p^{(p-1)n} - p^{(p-2)n} + \ldots - p^n + 1 = \\ \Big(\underbrace{p^{k(p-1)} - p^{k(p-3)} + \ldots + p^{2k} - 1}_{=:a}\Big)^2 + p^{2k}\Big(\underbrace{p^{k(p-3)} - p^{k(p-5)} \pm \ldots - p^{2k} + 1}_{=:b'}\Big)^2.$$

Hence,

$$1 - p^n + p^{2n} - \ldots + p^{(p-1)n} = a^2 + (\underbrace{p^k \cdot b'}_{=:b})^2 = a^2 + b^2.$$

Since $a = p^{k(p-1)} - b'$ and $b = p^k b'$, we conclude that a and b are relatively prime. □

The previous proof suggests the following generalization.

Theorem 6. *Let x, y be integers with $(x, y) = 1$, and $n > 0$ a natural number. Then*

$$x^{4n} - x^{4n-2}y^2 + \ldots + x^4y^{4n-4} - x^2y^{4n-2} + y^{4n}$$

is the product of Pythagorean primes, or equivalently, the sum of the squares of two natural numbers a, b which are relatively prime.

Proof. We have

$$x^{4n} - x^{4n-2}y^2 + x^{4n-4}y^4 - \ldots + y^{4n} = \frac{x^{4n+2} + y^{4n+2}}{x^2 + y^2} =: A,$$

$$x^{2n} - x^{2(n-1)}y^2 + x^{2(n-2)}y^4 - \ldots + (-1)^n y^{2n} = \frac{x^{2n+2} + (-1)^n y^{2n+2}}{x^2 + y^2} =: B,$$

$$x^{2(n-1)} - x^{2(n-2)}y^2 + x^{2(n-3)}y^4 - \ldots - (-1)^n y^{2(n-1)} = \frac{x^{2n} - (-1)^n y^{2n}}{x^2 + y^2} =: C.$$

It follows that

$$\begin{aligned} B^2 + (xyC)^2 &= \\ &= \frac{x^{4n+4} + 2(-1)^n x^{2n+2}y^{2n+2} + y^{4n+4} + x^{4n+2}y^2 - 2(-1)^n x^{2n+2}y^{2n+2} + x^2y^{4n+2}}{(x^2+y^2)^2} \\ &= \frac{(x^2+y^2)(x^{4n+2} + y^{4n+2})}{(x^2+y^2)^2} = A. \end{aligned}$$

Observe that for $(x, y) = 1$, we have $(x, C) = 1$ and $(y, C) = 1$. Hence, if d is a divisor of xyC, then d is a divisor of either x, or y or C. In all three cases, we conclude that d does not divide $B = x^{2n} - Cy^2$, and hence $(B, xyC) = 1$. □

Theorem 7. *Let n be an integer and $p \equiv 1 \pmod 4$ a prime number. Then the geometric sum*

$$1 - p^n + p^{2n} - p^{3n} + \ldots - p^{(p-2)n} + p^{(p-1)n}$$

is the product of Pythagorean primes, or equivalently, the sum of the squares of two natural numbers a, b.

Proof. Let

$$N_{p,n} := 1 - p^n + p^{2n} - p^{3n} + \ldots - p^{(p-2)n} + p^{(p-1)n} = \frac{p^{np} + 1}{p^n + 1}.$$

Then, $N_{p,n}$ is an odd integer and we need to show that all its prime divisors are of the form $q \equiv 1 \pmod 4$. We assume towards a contradiction, that $q \equiv 3 \pmod 4$ is a prime divisor of $N_{p,n}$.

First, observe that $p^{np} \equiv -1 \pmod q$, and hence $p^{2np} \equiv 1 \pmod q$. Indeed, since $q \mid N_{p,n}$ we have $qk(p^n + 1) = p^{np} + 1$ for an integer k. Next observe that $p^n \not\equiv 1 \pmod q$, since otherwise,

$$N_{p,n} = 1 - p^n + p^{2n} - \ldots + p^{(p-1)n} \equiv 1 - 1 + 1 - \ldots + 1 \equiv 1 \pmod q,$$

which is impossible since $q \mid N_{p,n}$. Similarly we have $p^n \not\equiv -1 \pmod q$. In fact, if $p^n \equiv -1 \pmod q$, then

$$N_{p,n} = 1 + p^n + p^{2n} + \ldots + p^{(p-1)n} \equiv 1 + 1 + 1 + \ldots + 1 \equiv p \pmod q,$$

but because $q \mid N_{p,n}$ and $p \neq q$, this is impossible — recall that $p \equiv 1 \pmod 4$ and by assumption we have $q \equiv 3 \pmod 4$. Thus, since $p^n \not\equiv \pm 1 \pmod q$, we have $p^{2n} \not\equiv 1 \pmod q$. From this together with $p^{np} \not\equiv 1 \pmod q$ and $p^{2np} \equiv 1 \pmod q$, it follows that p^n has order $2p$ mod q.

By Lagrange's theorem we have that $p^{n(q-1)} \equiv 1 \pmod q$, and the order of p^n mod q must divide the power $q - 1$, *i.e.*, $2p \mid q - 1$. Hence, we have $q - 1 = 2hp$ for an integer h. Now, h cannot be even, since in that case, we would have $q - 1 \equiv 0 \pmod 4$. Thus, we have $q = 2hp + 1$ for an odd integer h. Now recall that $p^{np} \equiv -1 \pmod q$ from which it follows that

$$(p^n)^{\frac{q-1}{2}} \equiv p^{nhp} \equiv -1 \pmod q, \tag{5}$$

and since $q \equiv 3 \pmod 4$, -1 is not a square mod q. Therefore, it follows from Equation (5) that p is not a square mod q. Hence, we have $(\frac{p}{q}) = -1$.

Finally, by quadratic reciprocity, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$$

because $p \equiv 1 \pmod 4$. Thus, we have $-1 = (\frac{p}{q}) = (\frac{q}{p}) = (\frac{2kp+1}{p}) = 1$ since $q = 2kp + 1$ is obviously a square mod p. This is a contradiction and we are done. □

Remark. If n is odd, we can give an explicit formula for two numbers a, b such that $a^2+b^2 = N_{p,n}$. Indeed, let p be a prime with $p \equiv 1 \pmod 4$ and let $n = 2k+1$ be odd. Write

$$\Phi_{4p}(x) = X_2^2 + p\,Y_2^2$$

for X_2 and Y_2 as in Proposition 1. Since $Y_2(x)$ is odd, $Y_2(x) = x\widetilde{Y}_2(x)$, for some even polynomial $\widetilde{Y}_2(x)$. So, for all x we have

$$x^{2(p-1)} - x^{2(p-2)} + \ldots - x^2 + 1 = X_2^2(x) + p\,x^2\,\widetilde{Y}_2^2(x).$$

If we replace x by $\sqrt{p^n} = \sqrt{p^{2k+1}}$, then we obtain

$$p^{(p-1)n} - p^{(p-2)n} + \ldots - p^n + 1 = X_2^2(\sqrt{p^{2k+1}}) + \underbrace{p\cdot p^{2k+1}}_{=(p^{k+1})^2}\cdot \widetilde{Y}_2^2(\sqrt{p^{2k+1}}),$$

and since the polynomials X_2 and $\widetilde{Y}_2$ are even,

$$a := X_2(\sqrt{p^{2k+1}}) \quad \text{and} \quad b := p^{k+1}\cdot\widetilde{Y}_2(\sqrt{p^{2k+1}})$$

are integers and

$$N_{p,n} = 1 - p^n + p^{2n} - \ldots + p^{(p-1)n} = a^2 + b^2.$$

Notice that these values for a and b are relatively prime if $N_{p,n}$ is square free because in this case, the diophantine equation $a^2 + b^2 = N_{p,n}$ has only primitive solutions (see [2] and [7, Chapter 2, Section 4]).

Example 1. For $p = 17$ and $n = 5$ we have

$$\begin{aligned} 1 - p^n + p^{2n} - \ldots + p^{(p-1)n} = {} & 272\,843\,369\,591\,083\,565\,163\,897\,960\,274\,150\backslash \\ & 163\,925\,907\,398\,160\,401\,760\,528\,914\,080\,984\backslash \\ & 723\,578\,982\,308\,965\,034\,129\,183\,153\,705\,601 \end{aligned}$$

which is equal to $a^2 + b^2$ for

$$\begin{aligned} a &= 16\,517\,872\,224\,923\,648\,631\,090\,629\,860\,090\,753\,718\,335\,620\,345\,665, \\ b &= -57\,155\,508\,740\,967\,834\,987\,352\,073\,159\,700\,853\,265\,061\,238\,624. \end{aligned}$$

The statement of Theorem 7 is in general false if $p \equiv 1 \pmod 4$ is not prime. However, it holds for powers of primes of the form $p \equiv 1 \pmod 4$.

Corollary 8. *Let $p \equiv 1 \pmod 4$ be a prime number, n a positive odd integer, and $q = p^k$ for some positive integer k. Then there are integers a and b such that*

$$1 - q^n + q^{2n} - q^{3n} + \ldots - q^{(q-2)n} + q^{(q-1)n} = a^2 + b^2 \,.$$

Proof. Let $F(u,v) := \sum_{j=0}^{v-1} (-1)^j p^{ju}$ for positive integers u, v. Then we have

$$F(kn, p^k) = F(kn, p) F(pkn, p^{k-1}),$$

and by induction we get

$$F(kn, p^k) = \prod_{r=0}^{k-1} F(p^r kn, p). \tag{6}$$

By Theorem 7 we know that all factors of the product in Equation (6) are sums of two squares. Hence, the claim follows from the sum of two squares theorem, or, if an explicit representation is needed, from the Brahmagupta-Fibonacci identity. □

The next result shows that for each positive odd integer n and for each prime $p \equiv 3 \pmod 4$, there are integers a and b such that $1 - p^n + p^{2n} - p^{3n} + \ldots - p^{(p-2)n} + p^{(p-1)n} = a^2 - b^2$. On the one hand, since $1 - p^n + p^{2n} - p^{3n} + \ldots - p^{(p-2)n} + p^{(p-1)n}$ is odd, it is trivial that this number can be written as the difference of two consecutive squares, for arbitrary positive integers p and n. However, our construction in the following proof provides, in particular, the Aurifeuillian factorization $(a-b)(a+b)$ with polynomials of $\frac{p^p+1}{p+1}$ (see [3, 18, 20]).

Proposition 9. *For each positive odd integer n and for each prime $p \equiv 3 \pmod 4$, there are integers a and b such that*

$$1 - p^n + p^{2n} - p^{3n} + \ldots - p^{(p-2)n} + p^{(p-1)n} = a^2 - b^2 \,.$$

Proof. Let p be a prime with $p \equiv 3 \pmod 4$ and let $n = 2k+1$ be odd. Write

$$\Phi_{4p}(x) = X_2^2 - p\, Y_3^2$$

for X_3 and Y_3 as in Proposition 2. Since $Y_3(x)$ is odd, $Y_3(x) = x\widetilde{Y}_3(x)$, for some even polynomial $\widetilde{Y}_3(x)$. So, for all x we have

$$x^{2(p-1)} - x^{2(p-2)} + \ldots - x^2 + 1 = X_3(x)^2 - p\, x^2\, \widetilde{Y}_3(x)^2.$$

If we replace x by $\sqrt{p^n} = \sqrt{p^{2k+1}}$, then we obtain

$$p^{(p-1)n} - p^{(p-2)n} + \ldots - p^n + 1 = X_3(\sqrt{p^{2k+1}})^2 - \underbrace{p \cdot p^{2k+1}}_{=(p^{k+1})^2} \cdot \widetilde{Y}_3(\sqrt{p^{2k+1}})^2,$$

and since the polynomials X_3 and $\widetilde{Y}_3$ are even,

$$a := X_3(\sqrt{p^{2k+1}}) \quad \text{and} \quad b := p^{k+1} \cdot \widetilde{Y}_3(\sqrt{p^{2k+1}})$$

are integers and

$$1 - p^n + p^{2n} - \ldots + p^{(p-1)n} = a^2 - b^2$$

as desired. □

Example 2. For $p = 19$ and $n = 5$ we have

$$\begin{aligned} 1 - p^n + p^{2n} - \ldots + p^{(p-1)n} = {} & 12\,241\,197\,653\,400\,194\,976\,316\,344\,352\,158\,020\,672\backslash \\ & 788\,585\,557\,257\,984\,632\,807\,522\,590\,951\,633\,776\,884\backslash \\ & 227\,612\,141\,191\,585\,621\,087\,559\,109\,580\,423\,076\,919 \end{aligned}$$

which is equal to $a^2 - b^2$ for

$$\begin{aligned} a &= 3\,498\,755\,719\,507\,579\,273\,794\,799\,179\,010\,519\,299\,740\,321\,464\,312\,052\,914\,100, \\ b &= -9\,691\,820\,613\,473\,972\,679\,175\,423\,830\,801\,834\,757\,164\,995\,075\,858\,712\,741. \end{aligned}$$

4. On $1 + p^n + p^{2n} + \ldots + p^{(p-1)n} = a^2 + b^2$

Theorem 10. *Let n be a positive odd integer and p a prime with $p \equiv 3 \pmod 4$. Then the geometric sum*

$$1 + p^n + p^{2n} + p^{3n} + \ldots + p^{(p-1)n}$$

is the product of Pythagorean primes, or equivalently, the sum of the squares of two natural numbers a, b.

Proof. Let

$$N_{p,n} := 1 + p^n + p^{2n} + p^{3n} + \ldots + p^{(p-1)n} = \frac{p^{np} - 1}{p^n - 1}.$$

Note that $N_{p,n}$ is odd and that $N_{p,n} \equiv 1 \pmod p$. Assume towards a contradiction that for some prime q with $q \equiv 3 \pmod 4$ we have $q \mid N_{p,n}$. Then $p \neq q$, and $p^{np} \equiv 1 \pmod q$. As in the proof of Theorem 7 we find that $p^n \not\equiv 1 \pmod q$. It follows that p^n has order p mod q. Since, by Lagrange, we have $p^{n(q-1)} \equiv 1 \pmod q$, we conclude that $p \mid q - 1$. Observe that n is odd, and hence $-p^{np} = (-p^n)^p \equiv -1 \pmod q$. Therefore, $-p$ cannot be a square mod q. Hence, we have $-1 = \left(\frac{-p}{q}\right) = (\frac{-1}{q})(\frac{p}{q}) = -(\frac{p}{q})$, since $q \equiv 3 \pmod 4$. Thus, we have $(\frac{p}{q}) = 1$. On the other hand, by quadratic reciprocity, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = -1,$$

which implies that $(\frac{q}{p}) = -1$. But because of $p \mid q-1$, we have that q is a square mod p, and hence $(\frac{q}{p}) = 1$ which is a contradiction. □

Remark. We can actually give an explicit formula for the two numbers a, b in Theorem 10. Indeed, assume that $p \equiv 3 \pmod 4$ and write

$$\Phi_{4p}(x) = X_3^2 - pY_3^2.$$

If we set $x = \sqrt{-p^n}$, the left side becomes

$$\Phi_{4p}\big(\sqrt{-p^n}\,\big) = 1 + p^n + p^{2n} + \ldots + p^{(p-1)n}$$

and since X_3 is even and Y_3 is odd, we find that there are integers a and $\widetilde{b}$ with

$$X_3\big(\sqrt{-p^n}\,\big) = a \quad \text{and} \quad Y_3\big(\sqrt{-p^n}\,\big) = \widetilde{b}\sqrt{-p^n}\,.$$

This implies

$$1 + p^n + p^{2n} + \ldots + p^{(p-1)n} = a^2 - p \cdot (-p^n) \cdot \widetilde{b}^2 = a^2 + p^{n+1} \cdot \widetilde{b}^2,$$

and since n is odd, $b := p^{(n+1)/2} \cdot \widetilde{b}$ is an integer and we finally have

$$1 + p^n + p^{2n} + \ldots + p^{(p-1)n} = a^2 + b^2$$

as desired.

Example 3. For $p = 19$ and $n = 5$ we have

$$\begin{aligned} 1 + p^n + p^{2n} + \ldots + p^{(p-1)n} = {} & 12\,241\,207\,540\,890\,636\,307\,955\,864\,529\,747\,398\,926\backslash \\ & 816\,231\,303\,577\,845\,363\,670\,867\,101\,162\,934\,744\,482\backslash \\ & 260\,391\,318\,439\,126\,866\,697\,079\,482\,004\,381\,725\,101 \end{aligned}$$

which is equal to $a^2 + b^2$ for

$$\begin{aligned} a &= -3\,498\,730\,285\,397\,697\,559\,176\,102\,637\,920\,628\,146\,694\,774\,816\,247\,528\,976\,330, \\ b &= -9\,691\,797\,128\,607\,969\,251\,794\,909\,402\,064\,256\,942\,732\,602\,279\,983\,923\,101. \end{aligned}$$

Also the previous result can be extended to powers of primes.

Corollary 11. *Let $p \equiv 3 \pmod 4$ be a prime number, n a positive odd integer, and $q = p^k$ for some positive integer k. Then there are integers a and b such that*

$$1 + q^n + q^{2n} + q^{3n} + \ldots + q^{(q-2)n} + q^{(q-1)n} = a^2 + b^2\,.$$

Proof. We repeat the proof of Corollary 8, this time with $F(u,v) := \sum_{j=0}^{v-1} p^{ju}$. □

The last result shows that for each positive odd integer n and each prime p with $p \equiv 1 \pmod 4$, there are integers a and b such that $1+p^n+p^{2n}+p^{3n}+\ldots+p^{(p-1)n} = a^2 - b^2$. Again, this result is trivial for numbers, however our construction in the following proof yields an Aurifeuillian factorization $(a-b)(a+b)$ with polynomials of $\frac{p^p-1}{p-1}$.

Proposition 12. *For each positive odd integer n and for each prime p with $p \equiv 1 \pmod 4$, there are integers a and b such that*

$$1 + p^n + p^{2n} + p^{3n} + \ldots + p^{(p-1)n} = a^2 - b^2 \,.$$

Proof. Assume that $p \equiv 1 \pmod 4$ and write

$$\Phi_{4p}(x) = X_2^2 + pY_2^2.$$

If we set $x = \sqrt{-p^n}$, the left side becomes

$$\Phi_{4p}\big(\sqrt{-p^n}\,\big) = 1 + p^n + p^{2n} + \ldots + p^{(p-1)n}$$

and since X_2 is even and Y_2 is odd, we find that there are integers a and $\widetilde{b}$ with

$$X_2\big(\sqrt{-p^n}\,\big) = a \quad \text{and} \quad Y_2\big(\sqrt{-p^n}\,\big) = \widetilde{b}\sqrt{-p^n}\,.$$

This implies

$$1 + p^n + p^{2n} + \ldots + p^{(p-1)n} = a^2 + p \cdot (-p^n) \cdot \widetilde{b}^2 = a^2 - p^{n+1} \cdot \widetilde{b}^2,$$

and since n is odd, $b := p^{(n+1)/2} \cdot \widetilde{b}$ is an integer and we finally have

$$1 + p^n + p^{2n} + \ldots + p^{(p-1)n} = a^2 - b^2$$

as desired. □

Acknowledgement. We would like to thank the referees for the careful reading and useful comments and suggestions, which helped to improve the quality of the article.

References

[1] R. P. Brent, On computing factors of cyclotomic polynomials, *Math. Comput.* **61** (203) (1993), 131–149.

[2] C. Busenhart, L. Halbeisen, N. Hungerbühler, and O. Riesen, On primitive solutions of the diophantine equation $x^2 + y^2 = M$, *Open Math.* **19** (1) (2021), 863–868.

[3] A. Cunningham, Factorization of $N = (Y^Y \mp 1)$ and $(X^{XY} \mp Y^{XY})$, *Messenger Math.* **45** (2) (1915), 49–75.

[4] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, Friedr. Vieweg & Sohn, Braunschweig, 1894.

[5] B. Frénicle de Bessy, *Memoires de l'Academie Royale des Sciences, Tome V*, La compagnie des libraires, Paris, 1729.

[6] C. F. Gauss, *Disquisitiones Arithmeticae*, G. Fleischer, Leipzig, 1801.

[7] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer, New York, 1985.

[8] K. T.-L. Koo, Problem 12295, *Amer. Math. Monthly* **129** (1) (2022), 86–95.

[9] M. Kraitchik, *Recherches sur la Théorie des Nombres*, Gauthier-Villars, Paris, 1924.

[10] M. Kraitchik, *Recherches sur la Théorie des Nombres, Tome II, Factorization*, Gauthier-Villars, Paris, 1929.

[11] F. Lemmermeyer, *Reciprocity Laws, from Euler to Eisenstein*, Springer-Verlag, Berlin, 2000.

[12] F. Lemmermeyer, *Quadratic Number Fields*, Springer-Verlag, Cham, 2021.

[13] É. Lucas, Théorèmes d'arithmétique, *Atti. R. Acad. Sc. Torino* **13** (1877/8), 271–284.

[14] É. Lucas, Sur la série récurrente de Fermat, *Bull. Bibl. Storia Sc. Mat. e Fis.* **11** (1878), 783–789.

[15] É. Lucas, Sur les formules de Cauchy et de Lejeune–Dirichlet, *Ass. Française pour l'Avanc. des Sci., Comptes Rendus* **7** (1878), 164–173.

[16] D. A. Marcus, *Number Fields*, Second edition with a foreword by Barry Mazur, Springer, Cham, 2018.

[17] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Boston, Birkhäuser, 1985.

[18] A. Schinzel, On primitive factors of $a^n - b^n$, *Proc. Cambridge Philos. Soc.* **58** (1962), 555–562.

[19] A. Scholz, *Einführung in die Zahlentheorie*, Walter de Gruyter, Berlin-New York, 1973.

[20] P. Stevenhagen, On Aurifeuillian factorizations, *Indag. Math.* **49** (1987), 451–468.

[21] L. C. Washington, *Introduction to Cyclotomic Fields* (2nd ed.), Graduate Texts in Mathematics vol. 83, Springer-Verlag, New York, 1996.