Geometric Sums as Sums of Two Squares

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

Franz Lemmermeyer

Mörikeweg 1, 73489 Jagstzell, Germany

hb3@uni-heidelberg.de

key-words: cyclotomic polynomial, sum of two squares, minimal polynomial, Aurifeuillian factorization

2020 Mathematics Subject Classification: **11D04** 11D72 11D08

Abstract

For each positive odd integer n and for each prime p with $p \equiv 3 \pmod 4$, there are integers a and b such that $1+p^n+p^{2n}+p^{3n}+\ldots+p^{(p-1)n} = a^2+b^2$. Furthermore, for each positive even integer n and for each odd prime p, there are integers a and b such that $1-p^n+p^{2n}-\ldots+p^{(p-1)n} = a^2+b^2$. These results follow from representations of the cyclotomic polynomials Φ_{4p} as sum of two squares. Finally, we show that for primes p with $p \equiv 3 \pmod 4$, the minimal polynomial of $\sqrt{p}\cdot\sin(2\pi/p)$ over $\mathbb{Q}$ is of degree $(p-1)/2$.

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.

If n is even, then $1+7^n+\ldots+7^{6n} \equiv 3 \pmod 4$, and Problem (b) follows from the fact that no integer m such that $m \equiv 3 \pmod 4$ is the sum of two squares. Hence, Problem (a) cannot be generalised to arbitrary positive integers n. However, one can ask whether Problem (a) can be generalised 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. By some classical results (see, *e.g.*, [3]), 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. On the other hand, we shall see that for each positive odd integer n and for each prime p with $p \equiv 3 \pmod 4$, there are integers a and b such that $1 + p^n + p^{2n} + p^{3n} + \ldots + p^{(p-1)n} = a^2 + b^2$ (see Theorem 6). Similarly, for each positive even integer n and for each odd prime p, there are integers a and b such that $1 - p^n + p^{2n} - p^{3n} \pm \ldots + p^{(p-1)n} = a^2 + b^2$ (see Theorem 3). These results follow from representations of the cyclotomic polynomials Φ_{4p} as sum and difference of two squares (see Proposition 1).

As a side result we show that for each odd prime number p, the minimal polynomial of $\sqrt{p} \cdot \sin(2\pi/p)$ over $\mathbb{Q}$ has degree $(p-1)/2$ if $p \equiv 3 \pmod 4$ (see Theorem 8), and degree $p - 1$ if $p \equiv 1 \pmod 4$.

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

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

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

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

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 [19, 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 $p = 11$ and $p = 13$, respectively. Let $\bar{g}_p \in \mathbb{Z}/p\mathbb{Z}$ be a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$, *e.g.*, let $g_{11} = 6$ and $g_{13} = 2$. By the Chinese Remainder Theorem, there is a $\bar{h}_p \in \mathbb{Z}/4p\mathbb{Z}$, such that $h_p \equiv g_p \pmod p$ and $h_p \equiv 1 \pmod 4$, *e.g.*, $h_{11} = 17$ and $h_{13} = 41$. Then $\langle \bar{h}_p \rangle$ and $\langle \bar{2}\bar{p} + \bar{h}_p \rangle$ are two subgroups of index 2 in G; for example,

$$\begin{array}{rcl}
\langle \bar{1}\bar{7} \rangle & = & \big(\{1, 5, 9, 13, 17, 21, 25, 29, 37, 41 \pmod{44}\}, \cdot\big), \\
\langle \bar{2}\bar{2} + \bar{1}\bar{7} \rangle & = & \big(\{1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}\}, \cdot\big), \\
\langle \bar{4}\bar{1} \rangle & = & \big(\{1, 5, 9, 17, 21, 25, 29, 33, 37, 41, 45, 49 \pmod{52}\}, \cdot\big), \\
\langle \bar{2}\bar{6} + \bar{4}\bar{1} \rangle & = & \big(\{1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49 \pmod{52}\}, \cdot\big).
\end{array}$$

For the third subgroup of index 2 in G, let $\bar{k}_p \in \mathbb{Z}/4p\mathbb{Z}$ be such that $k_p \equiv g_p^2 \pmod p$ and $k_p \equiv 3 \pmod 4$, *e.g.*, $k_{11} = 3$ and $k_{13} = 43$. Then $\langle \bar{k}_p \rangle \cup \big(\bar{2}\bar{p} + \langle \bar{k}_p \rangle\big)$ is a subgroup of index 2 in G, where for $p \equiv 3 \pmod 4$, this subgroup is isomorphic to $\langle \bar{k}_p \rangle$; for example,

$$\begin{array}{rcl}
\langle \bar{3} \rangle & = & \big(\{1, 3, 5, 9, 15, 23, 25, 27, 31, 37 \pmod{44}\}, \cdot\big), \\
\langle \bar{4}\bar{3} \rangle \cup \big(\bar{2}\bar{6} + \langle \bar{4}\bar{3} \rangle\big) & = & \big(\{1, 3, 9, 17, 23, 25, 27, 29, 35, 43, 49, 51 \pmod{52}\}, \cdot\big).
\end{array}$$

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 subextension $\mathbb{Q}(\sqrt{-p}\,) = \mathbb{Q}(i\sqrt{p}\,)$ 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 $H_1 := \mathrm{Gal}\big(L/\mathbb{Q}(i)\big)$, $H_2 := \mathrm{Gal}\big(L/\mathbb{Q}(\sqrt{-p}\,)\big)$ and $H_3 := \mathrm{Gal}\big(L/\mathbb{Q}(\sqrt{p}\,)\big)$, we have

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

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

This is easy to see: Fix a primitive p-th root of unity ζ_p and set $\zeta_{4p} = i\zeta_p$. The Galois group G of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/4p\mathbb{Z})^\times \simeq (\mathbb{Z}/4Z)^\times(\mathbb{Z}/p\mathbb{Z})^\times$. For $(r, s) \in$

$(\mathbb{Z}/4Z)^\times(\mathbb{Z}/p\mathbb{Z})^\times$ define $\sigma_{(r,s)} \in G : i\zeta_p \mapsto i^r\zeta_p^s$. Clearly the elements $(1, s)$ fix $\mathbb{Q}(i)$, and these correspond to residue classes a mod $4p$ that satisfy $a \equiv 1$ mod 4, *i.e.*, $(\frac{-4}{a}) = +1$.

For example, let $p = 11$ and let $\zeta_{44} = i\zeta_{11}$ where $\zeta_{11} = e^{2\pi i/11}$. Then $i = \frac{\zeta_{44}+\zeta_{44}^{-1}}{\zeta_{11}-\zeta_{11}^{-1}}$, and since $\zeta_{11} = \zeta_{44}^{12}$, we have

$$i = \frac{\zeta_{44} + \zeta_{44}^{-1}}{\zeta_{44}^{12} - \zeta_{44}^{-12}}.$$

If we replace ζ_{44} by ζ_{44}^a for some $a \in H_1$, say $a = 5$, then we have

$$\frac{\zeta_{44}^5 + \zeta_{44}^{-5}}{\zeta_{44}^{12\cdot 5} - \zeta_{44}^{-12\cdot 5}} = \frac{\zeta_{44}^5 + \zeta_{44}^{-5}}{\zeta_{44}^{16} - \zeta_{44}^{-16}} = \frac{i\zeta_{11}^5 - i\zeta_{11}^{-5}}{\zeta_{11}^5 - \zeta_{11}^{-5}} = i,$$

which shows that $a = 5$ (which belongs to H_1) is an element of the fix-group of $\mathbb{Q}(i)$.

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 $L = \mathbb{Q}(\zeta_{4p})$ is $L^+ = \mathbb{Q}\left(i(\zeta_p - \zeta_p^{-1})\right)$. To see this, recall 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 below shows some of the intermediate fields of the field extension $L/\mathbb{Q}$.

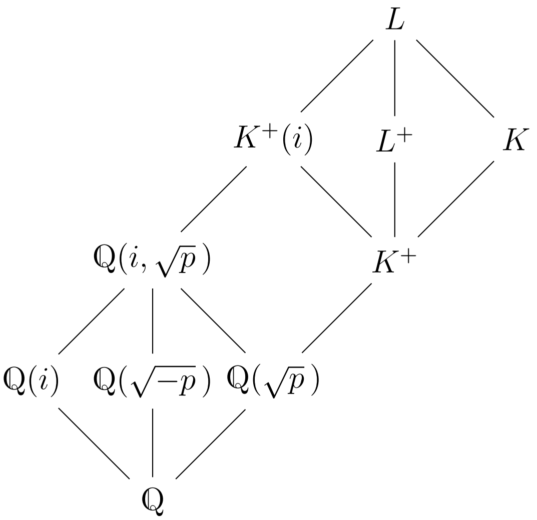

Figure 1: Subfield Diagram of $L = \mathbb{Q}(\zeta_{4p})$; here $K = \mathbb{Q}(\zeta_p)$, $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $L^+ = \mathbb{Q}\big(i(\zeta_p - \zeta_p^{-1})\big)$.

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

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

where $X_1, Y_1,\ 2X_2, 2Y_2,\ 2X_3, 2Y_3 \in \mathbb{Z}[x]$*. Moreover, if* $p \equiv 1 \bmod 4$*, then* $X_2, Y_2 \in \mathbb{Z}[x]$*, and if* $p \equiv 3 \bmod 4$*, 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* $p \equiv 1 \pmod 4$ *the polynomial* 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.

Before we prove this proposition we consider the cases $p = 11$ and $p = 13$.

$p = 11$**:**

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

$p = 13$**:**

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

Proof of Proposition 1. Proposition 1 follows in part from the formulas of Gauss (see [6, §356–357], [5, 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], [12, p. 276], [13, p. 785], [2, 14, 17], and [16, 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.

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 $4p$. We define three polynomials of degree $p - 1$ and their conjugates by

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

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 K_j of $L = \mathbb{Q}(\zeta_{4p})$, namely

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

For example, $f_1(x) = X_1(x) + iY_1(x)$ and $g_1(x) = X_1(x) - iY_1(x)$, hence

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

Similarly, we have $f_2(x) = X_2(x) + \sqrt{-p}\, Y_2(x)$, $g_2(x) = X_2(x) - \sqrt{-p}\, Y_2(x)$, and $f_3(x) = X_3(x) + \sqrt{p}\, Y_3(x)$, $g_3(x) = X_3(x) - \sqrt{p}\, Y_3(x)$, and therefore we get $\Phi_{4p}(x) = X_2^2 + pY_2^2 = X_3^2 - pY_3^2$.

X_1 is even and Y_1 is odd: For this, we first show that $f_1 + g_1$ is even. Let

$$\Gamma_1 := \big\{ k:\ 1 \le k \le 4p-1,\ (-4/k) = +1,\ (k, 4p) = 1 \big\}.$$

Then $|\Gamma_1| = p - 1$ and

$$\begin{aligned} f_1(-x) &= \prod_{k \in \Gamma_1} (-x - \zeta^k) = (-1)^{p-1} \prod_{k \in \Gamma_1} (x + \zeta^k) = \prod_{k \in \Gamma_1} (x + \zeta^k) \\ &= \prod_{k \in \Gamma_1} (x - \zeta^{2p+k}) = g_1(x), \end{aligned}$$

where we have used the fact that p is odd and that $2p + k \equiv 3 \pmod 4$ when $k \equiv 1 \bmod 4$.

Thus $f_1(-x) = g_1(x)$, which implies that

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

is even as claimed. Furthermore,

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

and hence, Y_1 is odd, as claimed.

The parity of the polynomial X_2 and Y_2: In this case, we have to consider f_2. For

$$\Gamma_2 := \big\{ k:\ 1 \le k \le 4p-1,\ (-4p/k) = +1,\ (k, 4p) = 1 \big\}$$

we find again

$$f_2(-x) = \prod_{k \in \Gamma_2} (x - \zeta^{2p+k}).$$

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

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

Here, we have used that $2p+k \equiv 2+k \pmod 4$ and the 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 $p^* = p$. 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

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

Here, we have used again the quadratic reciprocity law $(\frac{m}{q}) = (\frac{q^*}{m})$, where in this case we have $p^* = -p$. Thus, f_2 and g_2 are even, which implies that X_2 and Y_2 are both even.

The parity of the polynomial X_3 and Y_3: In this case, we consider f_3. For

$$\Gamma_3 := \big\{k:\ 1 \le k \le 4p-1,\ (4p/k) = +1,\ (k,4p) = 1\big\}$$

we have again

$$f_3(-x) = \prod_{k\in\Gamma_3} (x - \zeta^{2p+k}).$$

If $p \equiv 1 \pmod 4$, then

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

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

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

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

Thus, we get again $f_2(-x) = g_3(x)$, which implies that X_3 is even and Y_3 is odd.

Next we show that the polynomials f_j and g_j (for $1 \le j \le 3$) have integral coefficients, from which it follows that $X_1, Y_1 \in \mathbb{Z}[x]$, that $X_2, Y_2 \in \mathbb{Z}[x]$ for $p \equiv 1 \bmod 4$, and that$X_3, Y_3 \in \mathbb{Z}[x]$ for $p \equiv 3 \bmod 4$. To see this, notice that the coefficients of f_j and g_j are sums of products of roots of Φ_{4p}, and therefore, the coefficients are algebraic integers. Thus, it is enough to show that they are rational (see [15, Ch. 2]), which is clear since by definition $f_j, g_j \in \mathbb{Q}[x]$. *q.e.d.*

We now show that in the case when $p \equiv 3 \pmod 4$, the polynomials X_1 and Y_1 can be given explicitly.

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

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

where

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

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

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

hence,

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

since the second factor vanishes. *q.e.d.*

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

Theorem 3. *For each positive even integer n and for each odd prime p, 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 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

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

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

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

Hence,

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

as desired. *q.e.d.*

Example 1. For $p = 17$ and $n = 4$ we have

$$\begin{aligned} 1 - p^n + p^{2n} - \ldots + p^{(p-1)n} \;=\; & 5\,606\,938\,188\,524\,233\,972\,884\,833\,709\,876\,259\,715\,320 \\ & \qquad 120\,412\,834\,365\,746\,490\,518\,013\,679\,084\,903\,477\,761 \end{aligned}$$

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

$$\begin{aligned} a &= 2\,367\,883\,244\,007\,434\,985\,275\,084\,433\,544\,972\,212\,481, \\ b &= 8\,193\,367\,626\,323\,304\,447\,318\,631\,257\,941\,080\,320. \end{aligned}$$

Example 2. For $p = 19$ and $n = 4$ we have

$$\begin{aligned} 1 - p^n + p^{2n} - \ldots + p^{(p-1)n} \;=\; & 117\,559\,014\,338\,527\,165\,166\,244\,286\,348\,071 \\ & \qquad 379\,595\,604\,269\,270\,562\,262\,117\,202\,886 \\ & \qquad\qquad 547\,466\,177\,979\,905\,306\,611\,717\,019\,281 \end{aligned}$$

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

$$\begin{aligned} a &= 10\,842\,421\,882\,253\,262\,218\,528\,226\,247\,705\,356\,162\,489\,099\,600, \\ b &= -30\,034\,409\,646\,130\,920\,272\,931\,374\,647\,383\,258\,067\,836\,841. \end{aligned}$$

Theorem 4. *For each positive odd integer n and for each prime $p \equiv 1 \pmod 4$, 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 $p \equiv 1 \pmod 4$ 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 2. Since $Y_2(x)$ is odd, $Y_2(x) = x\tilde{Y}_2(x)$, for some even polynomial $\tilde{Y}_2(x)$. So, for all x we have

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

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

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

and since the polynomials X_2 and $\tilde{Y}_2$ are even, $a := X_2(\sqrt{p^{2k+1}})$ and $b := p^{k+1} \cdot \tilde{Y}_2(\sqrt{p^{2k+1}})$ are integers and

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

as desired. *q.e.d.*

Example 3. For $p = 17$ and $n = 5$ we have

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

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 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. On the other hand, since the construction of a and b in the proof yields the known Aurifeuillian factorization $(a-b)(a+b)$ of $\frac{p^p+1}{p+1}$ (see [4,17,18]), we will carry out the proof.

Proposition 5. *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, $Y_3(x) = x\tilde{Y}_3(x)$, for some even polynomial $\tilde{Y}_3(x)$. So, for all x we have

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

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

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

and since the polynomials X_3 and $\tilde{Y}_3$ are even, $a := X_3(\sqrt{p^{2k+1}})$ and $b := p^{k+1} \cdot \tilde{Y}_3(\sqrt{p^{2k+1}})$ are integers and

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

as desired. *q.e.d.*

Example 4. For $p = 19$ and $n = 5$ we have

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

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

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

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

Theorem 6. *For each positive odd integer n and for each prime p with $p \equiv 3 \pmod 4$, 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 $p \equiv 3 \pmod 4$ 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 $\tilde{b}$ with

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

This implies

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

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

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

as desired. *q.e.d.*

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

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

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

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

The next 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, even though this result is trivial, since our construction of a and b yields an Aurifeuillian factorization of $\frac{p^p-1}{p-1}$, we will carry out the proof.

Proposition 7. *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 $\tilde{b}$ with

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

This implies

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

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

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

as desired. *q.e.d.*

Example 6. For $p = 17$ and $n = 5$ we have

$$\begin{aligned} 1 + p^n + p^{2n} + \ldots + p^{(p-1)n} \;=\; & 272\,843\,753\,916\,493\,453\,326\,592\,154\,471\,252\,228 \\ & 008\,693\,153\,768\,573\,519\,357\,641\,119\,380\,280 \\ & 571\,696\,470\,094\,485\,235\,540\,600\,070\,801 \end{aligned}$$

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

$$\begin{aligned} a &= 16\,518\,081\,628\,817\,619\,620\,544\,774\,714\,274\,402\,979\,427\,456\,957\,265, \\ b &= 57\,155\,750\,267\,950\,500\,435\,205\,735\,853\,405\,846\,342\,799\,896\,868. \end{aligned}$$

3 On the minimal polynomial of $\sqrt{p} \cdot \sin(2\pi/p)$

Below we show that for primes $p \equiv 3 \pmod 4$, the degree of the minimal polynomial of $\sqrt{p} \cdot \sin(2\pi/p)$ over $\mathbb{Q}$ is always $(p-1)/2$. Notice that since the minimal polynomial of $\sqrt{5} \cdot \sin(2\pi/5)$ over $\mathbb{Q}$ is $125 - 100x^2 + 16x^4$, the result does not hold in general for primes $p \equiv 1 \pmod 4$.

Theorem 8. *For each prime $p \equiv 3 \pmod 4$, the minimal polynomial of $\sqrt{p} \cdot \sin(2\pi/p)$ over $\mathbb{Q}$ is of degree $(p-1)/2$.*

Proof. Let $p \equiv 3 \bmod 4$ be a prime number and let $\zeta_p = \cos(\frac{2\pi}{p}) + i\sin(\frac{2\pi}{p})$. Then

$$s_p := \sqrt{p} \cdot \sin(\tfrac{2\pi}{p}) = \sqrt{p} \cdot \frac{\zeta_p - \zeta_p^{-1}}{2i} = \frac{p}{2} \cdot \frac{\zeta_p - \zeta_p^{-1}}{\sqrt{-p}}.$$

Since for $p \equiv 3 \pmod 4$ we have

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \cdot \zeta_p^k = \sqrt{-p}$$

the real number s_p is an element of $\mathbb{Q}(\zeta_p)$ fixed by complex conjugation. Hence, it is an element of the maximal real subfield of $\mathbb{Q}(\zeta_p)$, and since $|\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = p-1$ (recall that $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong C_{p-1}$), the degree of s_p is a proper divisor of $p-1$ and therefore the degree of s_p is at most $\frac{p-1}{2}$.

On the other hand, $\sin(\frac{2\pi}{p})$ has degree $p-1$ (see below) and $\sqrt{p}$ has degree 2, so their product must have degree at least $\frac{p-1}{2}$. Thus, s_p has degree $\frac{p-1}{2}$. *q.e.d.*

In order to compute for primes $p \equiv 3 \pmod 4$ the minimal polynomial of $\sqrt{p} \cdot \sin(2\pi/p)$ over $\mathbb{Q}$, we proceed as follows. Let p be a prime with $p \equiv 3 \pmod 4$, let $q := (p-1)/2$, and let $\varphi_p := 2\pi/p$. In [1] one finds that the minimal polynomial of $\sin(\varphi_p)$ over $\mathbb{Q}$ is

$$f_p(x) = \sum_{k=0}^{q} (-1)^{q-k} \binom{p}{2k+1} (1-x^2)^{q-k} x^{2k},$$

which we can also express as

$$f_p(x) = \sum_{k=0}^{q} c_{2k}\, x^{2k}$$

where for $k \in \{0, \ldots, q\}$,

$$c_{2k} := (-1)^{k+1}\, p^{(p+1)/2}\, \frac{\prod_{j=0}^{k-1} \left(p^2 - (2j+1)^2\right)}{p^k (2k+1)!}.$$

This is a polynomial of degree $p-1$ with zeroes $\sin(k\,\varphi_p)$ for $k \in \{1, \ldots, p-1\}$. If we replace in $f_p(x)$ the indeterminate x by $x/\sqrt{p}$ and multiply by p^q, we get a polynomial $g_p(x)$ of the same degree with integral coefficients with zeroes $\sqrt{p} \cdot \sin(k\,\varphi_p)$ (for $k \in \{1, \ldots, p-1\}$). Therefore, the minimal polynomial of $\sqrt{p} \cdot \sin(\varphi_p)$ over $\mathbb{Q}$ must divide $g_p(x)$. In particular, the polynomial $g_p(x)$ can always be factorised into two polynomials of the same degree as follows:

$$g_p(x) = (a_0 + a_1 x + a_2 x^2 + \ldots + a_{q-1} x^{q-1} + a_q x^q) \cdot \\ (-a_0 + a_1 x - a_2 x^2 \pm \ldots - a_{q-1} x^{q-1} + a_q x^q)$$

where $a_0 = p^{(p+1)/4}$ and $a_q = 2^q$ (the latter follows from the fact that $a_q^2 = c_{2q} = 2^{p-1}$). The structure of the two factors comes from the fact that the polynomial $f_p(x)$ is even. It turns out that the zeroes of one of the factors are $\sqrt{p}\left(\frac{\ell}{p}\right)\sin(\ell\,\varphi_p)$ (for $\ell \in \{1, \ldots, q\}$), and that the zeroes of the other factor are $-\sqrt{p}\left(\frac{\ell}{p}\right)\sin(\ell\,\varphi_p)$ (for $\ell \in \{1, \ldots, q\}$). Since the degree of the minimal polynomial of $\sqrt{p} \cdot \sin(\varphi_p)$ over $\mathbb{Q}$ is at least q, and since $\sqrt{p} \cdot \sin(\varphi_p)$ is a zero of one of the factors, we find that one of factors must be the minimal polynomial of $\sqrt{p} \cdot \sin(\varphi_p)$ over $\mathbb{Q}$.

Example 7. For $p = 11$, the minimal polynomial of $\sin(\varphi_p)$ over $\mathbb{Q}$ is

$$-11 + 220x^2 - 1232x^4 + 2816x^6 - 2816x^8 + 1024x^{10}.$$

Replacing x by $x/\sqrt{11}$ and multiplying by 11^5 gives us

$$-1771561 + 3221020x^2 - 1639792x^4 + 340736x^6 - 30976x^8 + 1024x^{10},$$

which factorises as

$$(1331 - 2662x + 1452x^2 - 176x^4 + 32x^5) \cdot (-1331 - 2662x - 1452x^2 + 176x^4 + 32x^5)$$

and the minimal polynomial of $\sqrt{11} \cdot \sin(2\pi/11)$ over $\mathbb{Q}$ is

$$1331 - 2662x + 1452x^2 - 176x^4 + 32x^5.$$

References

[1] Scott Beslin and Valerio De Angelis. The minimal polynomials of $\sin\left(\frac{2\pi}{p}\right)$ and $\cos\left(\frac{2\pi}{p}\right)$. ***Mathematics Magazine***, 77(2):146–149, 2004.

[2] Richard P. Brent. On computing factors of cyclotomic polynomials. ***Mathematics of Computation***, 61(203):131–149, 1993.

[3] Chris Busenhart, Lorenz Halbeisen, Norbert Hungerbühler, and Oliver Riesen. On primitive solutions of the diophantine equation $x^2 + y^2 = M$. ***Open Mathematics***, 19(1):863–868, 2021.

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

[5] Peter Gustav Lejeune Dirichlet. ***Vorlesungen über Zahlentheorie.*** Friedr. Vieweg & Sohn, Braunschweig, 1894.

[6] Carl Friedrich Gauss. ***Disquisitiones Arithmeticae.*** G. Fleischer, Leipzig, 1801.

[7] Andrew Granville, Peter Pleasants. Aurifeuillian factorization. ***Math. Comp.*** 75 (2006) 497–508

[8] Koopa Tak Lun Koo. Problem 12295. ***American Mathematical Monthly*** *(Problems and Solutions)*, 129(1):86–95, 2022.

[9] Maurice Kraitchik. ***Recherches sur Ia Théorie des Nombres***. Gauthiers-Villars, Paris, 1924.

[10] Maurice Kraitchik. ***Recherches sur Ia Théorie des Nombres, Tome II, Factorization***. Gauthiers-Villars, Paris, 1929.

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

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

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

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

[15] Daniel A. Marcus. ***Number fields***. [Second edition with a foreword by Barry Mazur] Springer, Cham, 2018.

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

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

[18] Peter Stevenhagen. On Aurifeuillian factorizations. ***Indag. Math. 49, 451-468 (1987)***.

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