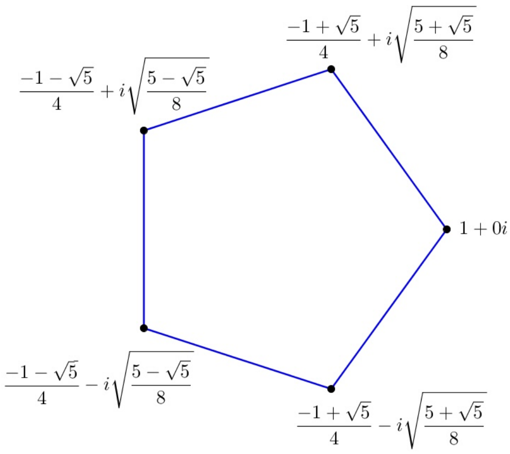



# Complex Roots of Unity

*A Bridge Across Four Olympiad Disciplines*

**Giuseppe Bassi**

ACADEMIC YEAR 2024/2025

*An Interdisciplinary Lecture for Mathematical Olympiads*

**Abstract**

These notes originate from two lectures I delivered at *Liceo Scientifico Niccolò Copernico* in Brescia on March 21st, 2024, and December 2nd, 2024, as part of an intensive training program aimed at preparing students for Mathematical Olympiads. The first lecture was an introductory lecture to complex numbers and its applications to polynomials, while the second aimed to present algebraic tools for solving problems in number theory and combinatorics. Extending this material, this work shows how *complex roots of unity* serve as an elegant bridge connecting the core areas of Olympiad mathematics: algebra, geometry, number theory, and combinatorics.

This material is designed for high school students with an intermediate to advanced Olympiad background. Accordingly, the approach discards university rigorousness and is more concrete, problem-oriented, and intuitive. Many exercises are drawn from Italian competitions, which can be found at [1] and [2].

Version 1.0 Date: 2025-04-13

# Contents

# 1 Complex Numbers

## 1.1 Introduction

The complex numbers extend the real numbers by incorporating the imaginary unit $i := \sqrt{-1}$, satisfying $i^2 = -1$. Thanks to this rule, any complex number can be manipulated by treating $i$ simply as a letter.

*Example* 1.1. Powers of $i$ are cyclic: $i^2 = -1$, $i^3 = i^2 \cdot i = -i$, $i^4 = i^2 \cdot i^2 = (-1)\cdot(-1) = 1$, and in general, for any integer $k$ and remainder $h$ with $0 \le h < 4$, $i^{4k+h} = (i^4)^k \cdot i^h = i^h$. More explicitly, we have

$$i^n = \begin{cases} i & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 2 \bmod 4, \\ -i & \text{if } n \equiv 3 \bmod 4, \\ 1 & \text{if } n \equiv 0 \bmod 4. \end{cases} \tag{1.1}$$

*Example* 1.2. Since the powers of $i$ reduce as shown, given a polynomial $P(x) \in \mathbb{R}[x]$ the evaluation $P(i)$ reduces to a form $a + bi$ with $a, b \in \mathbb{R}$. For example, if $P(x) = (x+2)(x^2+4x) - 4x + 1$, then

$$P(i) = (i+2)(i^2+4i) - 4i^2 + 1 = (i+2)((-1)+4i) - 4(-1) + 1 = (i+2)(4i-1) + 4 + 1 = -i - 6 + 8i + 5 = 7i - 1.$$

In fact, any expression involving $i$, even complicated ones such as $i^{\log i}$, can in principle be written in the form $a + bi$. For this reason, we define *complex numbers* as those numbers of the form

$$z = x + iy,$$

and denote the real and imaginary parts of $z$ by $x = \Re\mathrm{e}(z)$ and $y = \Im\mathrm{m}(z)$, respectively. The set of complex numbers is denoted by $\mathbb{C}$. For convenience, we define the *modulus* (also known as the norm, absolute value, or magnitude) of $z$ as

$$|z| = \sqrt{x^2 + y^2},$$

and the (complex) *conjugate* of $z$ as

$$\overline{z} = x - iy.$$

The following properties of the conjugate are particularly useful:

$$\boxed{\overline{z + w} = \overline{z} + \overline{w}}, \tag{1.2}$$

$$\boxed{\overline{z \cdot w} = \overline{z} \cdot \overline{w}} \implies \overline{z^n} = (\overline{z})^n \quad \forall n \in \mathbb{N}, \tag{1.3}$$

$$\boxed{\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}} \implies \overline{z^k} = (\overline{z})^k \quad \forall k \in \mathbb{Z}. \tag{1.4}$$

*Remark* 1.3. We have $z = \overline{z}$ if and only if $z$ is a real number; similarly, $z + \overline{z} = 0$ if and only if $z$ is a purely imaginary number (i.e., $z = bi$ for some $b \in \mathbb{R}$). Evidently, $\overline{(\overline{z})} = z$.

Sums, differences, and products in $\mathbb{C}$ are defined in the usual way. For divisions, one can proceed as follows:

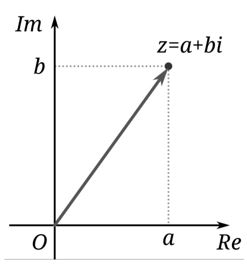
$$\frac{w}{z} = \frac{a+ib}{c+id} = \frac{a+ib}{c+id} \cdot \frac{c-id}{c-id} = \frac{(a+ib)(c-id)}{c^2+d^2} = w \cdot \frac{\overline{z}}{|z|^2}.$$

This method also yields two important relations:

$$\boxed{z\overline{z} = |z|^2} \quad \text{and} \quad \boxed{\frac{1}{z} = \frac{\overline{z}}{|z|^2}}. \tag{1.5}$$

## 1.2 The Complex Plane

Since we cannot represent all complex numbers on a single real line, we instead establish a bijective association between a complex number $z = x + iy$ and the point $(x, y)$ in a two-dimensional Cartesian plane. This plane is known as the *complex plane* (or the *Argand-Gauss plane*). Geometrically, every complex number can be viewed as a two-dimensional vector, and should be thought of as an arrow drawn from the origin to the point $(x, y)$. This arrow can be described either by its endpoint $(x, y)$ or in terms of its length and direction:



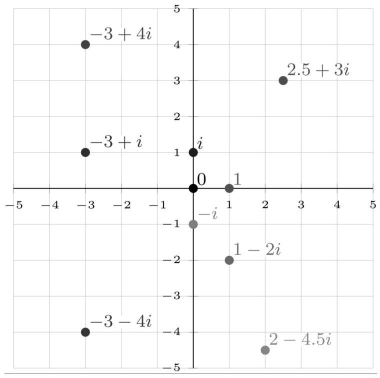



Figure 1: Various complex numbers depicted in the complex plane

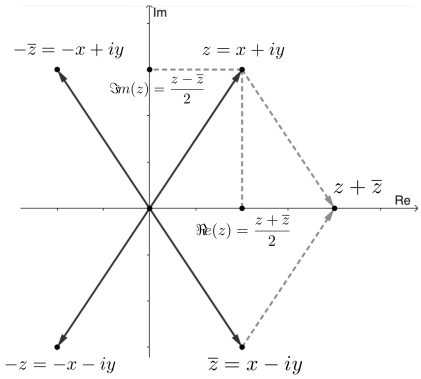



Figure 2: Addition, negation and conjugation graphically

- **Length:** By the Pythagorean theorem, the length of the arrow is $\sqrt{x^2+y^2} = |z|$, corresponding to the magnitude of $z$;
- **Direction:** The direction is conventionally given by the counterclockwise angle $\theta := \arctan\left(\frac{y}{x}\right)$ that the arrow forms with the positive real axis. This angle, called the *argument* of $z$ and denoted $\arg z$, is unique modulo 360°.

It is also straightforward to recover the Cartesian components from these two pieces of information. Specifically, if a complex number corresponds to an arrow of length $\rho$ and angle $\theta$, then its Cartesian coordinates are

$$\begin{cases} x = \rho\cos\theta, \\ y = \rho\sin\theta, \end{cases}$$

which implies that

$$z = \rho\cos\theta + i\,\rho\sin\theta.$$

We denote the complex number $\cos\theta + i\sin\theta$ by $e^{i\theta}$.[1] With this notation, every complex number can be expressed in the form

$$z = \rho e^{i\theta}, \quad \text{with } \rho = \sqrt{x^2+y^2} \quad \text{and} \quad \theta = \arctan\left(\frac{y}{x}\right).$$

In summary, a complex number can be represented equivalently in three forms:

$$\begin{aligned} \text{Cartesian form:} \quad & z = x+iy, \\ \text{Trigonometric form:} \quad & z = \rho\cos\theta + i\,\rho\sin\theta, \\ \text{Polar form:} \quad & z = \rho e^{i\theta} = \rho\exp(i\theta). \end{aligned}$$

Let us now focus on understanding how operations on complex numbers are interpreted graphically in the complex plane.

- **Modulus:** As expected, $|z|$ represents the distance between the point $z$ and the origin.
- **Addition:** Addition is performed component-wise, just as with vectors; no surprises occur here.
- **Negation:** Subtraction is defined as the addition of the opposite. The negative of $z$ is obtained by switching the signs of both coordinates, which graphically corresponds to a reflection through the origin.

[1]With the proper tools—such as the concept of holomorphic functions and Taylor expansions—it can be proven that $\cos\theta + i\sin\theta = e^{i\theta}$ is an identity between the trigonometric functions and the exponential function, rather than a notation. Specifically, one defines $\exp(z) : \mathbb{C} \to \mathbb{C}$ by $\exp(z) = e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$, and then shows that $\sin(z) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} z^{2n+1}$ and $\cos(z) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} z^{2n}$. Substituting $z = i\theta$ yields the claimed result. Notice that the most challenging part of the proof is to rigorously make sense of these infinite series of complex numbers. In fact, this identity is known as Euler's Formula because Euler was the first to identify the equivalence—even though he did not possess the rigorous mathematical tools later developed to fully justify his derivation.

- **Conjugation:** The conjugate $\overline{z}$ of a complex number is obtained by reflecting $z$ across the real axis. This transformation has two useful properties with clear geometric interpretations:

$$\Re(z) = \frac{z+\overline{z}}{2} \quad \text{and} \quad \Im(z) = \frac{z-\overline{z}}{2i}. \tag{1.6}$$

Before proceeding to the discussion on multiplication, consider the following exercise, which illustrates the usefulness of conjugate numbers in mathematical olympiads.

**Exercise 1.4** (TdA Senior 2022)**.** *Given $z = 2+i$, let $a_n$ and $b_n$ be the integer numbers satisfying $z^n = a_n + b_n i$, for every $n \in \mathbb{N}$. Compute*

$$\sum_{n=0}^{\infty} \frac{a_n b_n}{7^n}.$$

**Solution.**
By combining identities (1.3) and (1.6) we deduce

$$a_n = \frac{z^n + \overline{z}^n}{2} \qquad \text{and} \qquad b_n = \frac{z^n - \overline{z}^n}{2i}.$$

Therefore, we can rewrite our sum as follows:

$$\sum_{n=0}^{\infty} \frac{a_n b_n}{7^n} = \sum_{n=0}^{\infty} \frac{(z^n + \overline{z}^n)(z^n - \overline{z}^n)}{4i \cdot 7^n} = \frac{1}{4i} \sum_{n=0}^{\infty} \frac{z^{2n} - \overline{z}^{2n}}{7^n}.$$

Since $z^2 = 3+4i$ and $\overline{z}^2 = 3-4i$, we can easily compute our sum as a sum of two geometric series:

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{a_n b_n}{7^n} &= \frac{1}{4i} \sum_{n=0}^{\infty} \frac{(3+4i)^n}{7^n} - \frac{(3-4i)^n}{7^n} = \frac{1}{4i} \cdot \left( \frac{1}{1-\frac{3+4i}{7}} - \frac{1}{1-\frac{3-4i}{7}} \right) \\ &= \frac{1}{4i} \cdot \left( \frac{7}{4-4i} - \frac{7}{4+4i} \right) = \frac{7}{4i} \cdot \left( \frac{8i}{32} \right) = \frac{14}{32} = \frac{7}{16}.\end{aligned}$$

□

## 1.3 Complex Multiplication

Up to now, working with complex numbers and vectors might seem completely equivalent. However, complex numbers introduce an additional operation absent in standard vector algebra: multiplication between complex numbers. In $\mathbb{R}^2$, the only natural multiplication between vectors is the inner product $v \cdot w$, which, however, yields a scalar. In contrast, multiplication of complex numbers behaves as a *spiral similarity*—that is, a combination of dilation and rotation. To see this, express a complex number in polar form as $z = re^{i\theta}$, where $r$ is the modulus and $\theta$ is the argument. The number $z$ can be interpreted as the result of applying two successive transformations to the unit number 1:

- Multiplication by the real number $r \geq 0$ dilates the unit vector by a factor of $r$, increasing its distance from the origin without changing its direction, as it happens with real numbers.
- We then multiply the vector $1 \cdot r$ by $e^{i\theta}$, obtaining $z$, as if we performed a rotation by a counterclockwise angle $\theta$.

Thus, multiplying two complex numbers $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$ corresponds to dilating $z_1$ by $r_2$ and rotating it by $\theta_2$.
This interpretation of *multiplying* the moduli and *adding* the angles is perfectly consistent with the properties of the exponential function:

$$z_1 z_2 = r_1 e^{i\theta_1} \cdot r_2 e^{i\theta_2} = r_1 r_2 e^{i(\theta_1+\theta_2)},$$

and is also easily verified in trigonometric form:

$$z_1 z_2 = r_1(\cos\theta_1 + i \sin\theta_1) r_2(\cos\theta_2 + i\sin\theta_2) = r_1 r_2 (\underbrace{[\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2]}_{\cos(\theta_1+\theta_2)} + i\underbrace{[\sin\theta_1\cos\theta_2 + \sin\theta_2\cos\theta_1]}_{\sin(\theta_1+\theta_2)}).$$

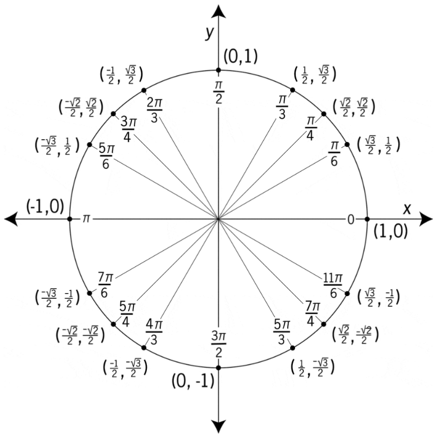


Figure 3: Sine and cosine of the most common angles, useful to compute the Cartesian form of a complex number starting from the polar or trigonometric one.

*Remark* 1.5. A nice consequence of this multiplicative rule is that it provides an intuitive "justification" for the sign rules we learned in middle school, that is, $(+) \cdot (+) = +$, $(-) \cdot (-) = +$, $(+) \cdot (-) = -$ and $(-) \cdot (+) = -$:

- Multiplying by a positive real number (which corresponds to an angle of $0°$) only affects the modulus, leaving the direction—and hence the sign—unchanged. Therefore, $(+) \cdot (+) = +$ and $(-) \cdot (+) = -$.
- Multiplying by a negative real number (corresponding to an angle of $180°$) rotates the vector by $180°$, thereby reversing its sign. This explains why $(+) \cdot (-) = -$ and $(-) \cdot (-) = +$.

Similarly, when computing $i^n$ (with $i = e^{i\pi/2}$), we are simply applying $n$ successive rotations of $90°$, which accounts for the cyclic behavior described in Equation (1.1).

---

*Example* 1.6. If we multiply a complex number $z$ with modulus 2 and angle $120°$ by a complex number $w$ with modulus 4 and angle $330°$, we expect to obtain a result with modulus $2 \cdot 4 = 8$ and angle $120° + 330° = 450°$, which is equivalent to $90°$, i.e., $8i$.
In polar form, this computation is straightforward:

$$z \cdot w = 2e^{\frac{2\pi i}{3}} \cdot 4e^{\frac{11\pi i}{6}} = 8e^{i\pi\left(\frac{2}{3}+\frac{11}{6}\right)} = 8e^{\frac{5i\pi}{2}} = 8i.$$

The same result can be obtained in Cartesian form. Referring to Figure 3, we deduce

$$z = 2\Big(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\Big) \quad \text{and} \quad w = 4\Big(\frac{\sqrt{3}}{2} - \frac{1}{2}i\Big).$$

Multiplying directly:

$$z \cdot w = 2\Big(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\Big) \cdot 4\Big(\frac{\sqrt{3}}{2} - \frac{1}{2}i\Big) = 2(-1 + \sqrt{3}i)(\sqrt{3} - i) = 8i.$$

# 2 Geometry: Complex Numbers and Spiral Similarities

In this section we will explore some basic geometric properties of complex numbers and present two challenging exercises solved using our new tools, that bridge the gap between algebra and geometry. For a complete illustration of this topic, refer to [3] and [4].

From a geometric perspective, complex numbers represent points on the plane subject to various transformations. For example, given points $a$, $b$, and $c$:

i) The point $m = \frac{1}{2}(a + b)$ is the midpoint of segment $AB$;

ii) The point $g = \frac{1}{3}(a + b + c)$ is the centroid $G$ of triangle $ABC$;

iii) Every point on the segment $AB$ can be written as $\lambda a + (1 - \lambda)b$ for some $\lambda \in [0, 1]$.

The most important transformation is the spiral similarity. Consider this simplified example:

*Example* 2.1. Let $a = 1 + i$ and $b = 3 - i$. How can we perform a $90°$ counterclockwise rotation of $AB$ about point $A$? This is equivalent to finding a point $B'$ such that the vector $\overrightarrow{AB'}$ is the vector $\overrightarrow{AB}$ rotated by $90°$. To achieve this, we first translate the entire diagram so that $A$ becomes the origin (by subtracting $a$), and then we impose

$$\overrightarrow{AB'} = i\,\overrightarrow{AB},$$

since a $90°$ rotation is equivalent to multiplication by $i$. Specifically,

$$b' - a = i(b - a) \implies b' = i(b - a) + a. \implies b' = i[3 - i - (1 + i)] + 1 + i = 3 + 3i.$$

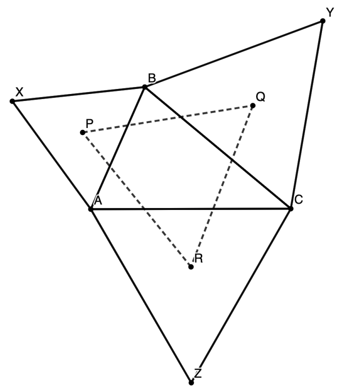
Of course, there's nothing special about a $90°$ rotation. For instance, a $60°$ rotation can be achieved by multiplying by $e^{\frac{i\pi}{3}} = \frac{\sqrt{3}}{2} + \frac{1}{2}i$. This property is particularly useful when proving that a certain quadrilateral is a rectangle or that a specific triangle is equilateral, as demonstrated by the following two exercises.

**Exercise 2.2** (Napoleon's Theorem)**.** *If we construct outward equilateral triangles on the sides of a triangle $ABC$, the lines connecting the centers of those equilateral triangles form an equilateral triangle.*[2]

**Solution.**

Refer to the figure on the right. Define $\zeta := e^{\frac{i\pi}{3}} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Given points $a$, $b$, and $c$, the vector $\overrightarrow{AX}$ is the vector $\overrightarrow{AB}$ rotated by $60°$ about $a$, and similarly for the points $y$ and $z$:

$$\begin{aligned} x - a &= \zeta(b - a), \\ y - b &= \zeta(c - b), \\ z - c &= \zeta(a - c). \end{aligned}$$




The centers $p$, $q$, and $r$ of triangles $ABX$, $BCY$, and $CAZ$ are then given by:

$$\begin{aligned} p &= \frac{a + b + x}{3} = \frac{a + b + \zeta(b - a) + a}{3}, \\ q &= \frac{b + c + y}{3} = \frac{b + c + \zeta(c - b) + b}{3}, \\ r &= \frac{c + a + z}{3} = \frac{c + a + \zeta(a - c) + c}{3}. \end{aligned}$$

To verify that $PQR$ is equilateral, we can show $PR = PQ$ and $\widehat{RPQ} = 60°$ by simply imposing that the vector $\overrightarrow{PQ}$ is the vector $\overrightarrow{PR}$ rotated by $60°$ about $P$:

$$\overrightarrow{PQ} \stackrel{?}{=} \zeta \cdot \overrightarrow{PR} \iff q - p \stackrel{?}{=} \zeta(r - p).$$

Now it's just a matter of computations:

$$\begin{aligned} 3(q - p - \zeta(r - p)) &= [\cancel{b} + c + \zeta(\cancel{c} - \cancel{b}) + b] - [a + \cancel{b} + \zeta(b - a) + a] - \zeta([\cancel{c} + \cancel{a} + \zeta(a - c) + c] - [\cancel{a} + \cancel{b} + \zeta(b - a) + a]) \\ &= [c + b - 2a] + \zeta[-b - c + 2a] + \zeta^2[c + b - 2a] = [c + b - 2a][1 - \zeta + \zeta^2] \\ &= [c + b - 2a][1 - (\frac{1}{2} + \frac{\sqrt{3}}{2}i) + (\frac{1}{2} + \frac{\sqrt{3}}{2}i)^2] \\ &= [c + b - 2a][1 - (\frac{1}{2} + \frac{\sqrt{3}}{2}i) + (-\frac{1}{2} + \frac{\sqrt{3}}{2}i)] = 0. \end{aligned}$$

□

We now turn to a more challenging problem, which appeared in the national finals of the Italian Team Math Olympiads in 2022 [1].

**Exercise 2.3** (GAS 2022)**.** *Let $ABC$ be a right triangle with legs of length 426 and $120\sqrt{3}$. Let $\omega_1$, $\omega_2$, and $\omega_3$ be circles of radius $d$ centered at $A$, $B$, and $C$ respectively, and let $A'$, $B'$, and $C'$ be points on $\omega_1$, $\omega_2$, and $\omega_3$ respectively. What is the minimum value of $d^2$ required so that the triangle $A'B'C'$ is equilateral?*

[2]It is believed that the intuition behind this result is attributable to Napoleon Bonaparte, even though he himself presented the theorem to Joseph-Louis Lagrange for a proof. The first publication mentioning this property dates back to 1825 [5].

**Solution.**
Consider the complex numbers:

$$a = 0, \quad b = 120\sqrt{3}, \quad c = 426i,$$

which represent the vertices of triangle $ABC$ on the Gauss plane.
Any point at a distance $r$ from a given point $p$ can be expressed as:

$$p + re^{i\theta}, \quad \theta \in [0, 2\pi).$$

Thus, we write the points $A'$, $B'$, and $C'$ as

$$\begin{cases} a' = a + de^{i\alpha} = de^{i\alpha}, \\ b' = b + de^{i\beta} = 120\sqrt{3} + de^{i\beta}, \\ c' = c + de^{i\gamma} = 426i + de^{i\gamma}. \end{cases}$$

In the language of complex numbers, asserting that $A'B'C'$ forms an equilateral triangle is equivalent to requiring that the vector $\overrightarrow{C'B'}$, when rotated by $60°$ (i.e. multiplied by $e^{i\theta}$ with $\theta = \pi/3$), coincides with the vector $\overrightarrow{C'A'}$. That is, we impose the condition:

$$b' - c' = (a' - c')e^{i\theta}.$$

Substituting the expressions for $a'$, $b'$, and $c'$ gives

$$d\big(e^{i\beta} - e^{i\gamma}\big) + 120\sqrt{3} - 426i = e^{i\theta}\Big(de^{i\alpha} - de^{i\gamma} - 426i\Big).$$

Rearranging leads to

$$d\Big(e^{i\beta} - e^{i\gamma} - e^{i(\theta+\alpha)} + e^{i(\theta+\gamma)}\Big) = 213i + 93\sqrt{3}.$$

By introducing the changes of variable

$$-e^{i(\theta+\alpha)} = e^{i\alpha'}, \quad \text{and} \quad -e^{i\gamma} + e^{i(\theta+\gamma)} = e^{i\gamma'},$$

with $\theta' = \frac{2\pi}{3}$ and hence $\gamma' = \gamma + \frac{2\pi}{3}$, the equation is recast as

$$d\Big(e^{i\beta} + e^{i\gamma'} + e^{i\alpha'}\Big) = 213i + 93\sqrt{3}.$$

Since the angles $\alpha'$, $\beta$, and $\gamma'$ are arbitrary in the interval $[0, 2\pi)$, minimizing $d^2$ requires maximizing

$$\Big|e^{i\beta} + e^{i\gamma'} + e^{i\alpha'}\Big|.$$

Geometrically, the sum represents the vector addition of three unit vectors. It is evident that the maximum is achieved when all three unit vectors are aligned, that is, when

$$\alpha' = \beta = \gamma'.$$

To verify this rigorously, one may apply the Cauchy-Schwarz inequality. Let $x$, $y$, and $z$ be three unit vectors; then we have:

$$\|x + y + z\|^2 = \|x\|^2 + \|y\|^2 + \|z\|^2 + 2\big(x \cdot y + y \cdot z + z \cdot x\big) \leq 1 + 1 + 1 + 2(1 + 1 + 1) = 9,$$

with equality if and only if $x$, $y$, and $z$ are collinear. Thus, the maximum norm is 3, and the minimum value of $d^2$ is determined by:

$$d^2 = \frac{213^2 + (93\sqrt{3})^2}{9} = 7924.$$

□

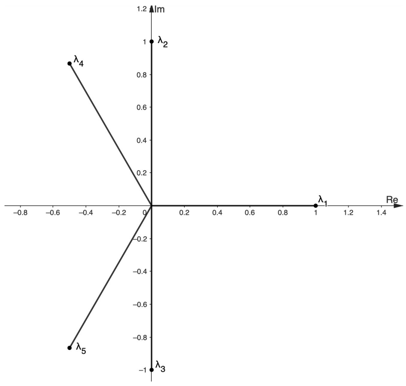



Figure 4: Roots of $P(x) = x^5 + x^3 - x^2 - 1$ plotted on the complex plane. Note that $P(x) = (x^2+1)(x^3-1) = (x-1)(x^2+1)(x^2+x+1)$. This factorization clarifies which root corresponds to which factor.

# 3 Algebra: Complex Roots of Polynomials

In this section we introduce roots of unity in the context of real-valued polynomials. This is the historical motivating scenario for the need of complex numbers, as we will now see.

## 3.1 The Fundamental Theorem of Algebra

Let us start with a motivating example.

*Example* 3.1. To decompose $P(x) = 4x^2 + 2x + 1$, we need to find the solutions $\alpha$ and $\beta$ of the equation $4x^2 + 2x + 1 = 0$, and then decompose $P(x)$ as $P(x) = 4(x-\alpha)(x-\beta)$. However, $\alpha$ and $\beta$ turn out to be complex, so the problem can only be solved in $\mathbb{C}$:

$$x_{1,2} = \frac{-2 \pm \sqrt{2^2 - 4 \cdot 1 \cdot 4}}{2 \cdot 4} = \frac{-2 \pm \sqrt{-12}}{8} = \frac{-2 \pm 2\sqrt{3}\sqrt{-1}}{8} = \frac{-1 \pm \sqrt{3}i}{4}.$$

The possibility to decompose a polynomial with real coefficients in $\mathbb{C}$ is a general fact, triumphantly known as the *Fundamental Theorem of Algebra* (FTA), proved by Gauss in 1799:

**Theorem 3.2** (FTA). *Every polynomial $P(x) \in \mathbb{R}[x]$ of degree $n \geq 1$ admits $n$ complex roots (counting multiplicity). That is, $P(x)$ can be decomposed as*

$$P(x) = \alpha(x-\lambda_1)(x-\lambda_2)\ldots(x-\lambda_n),$$

*where $\lambda_1, \ldots, \lambda_n$ are the $n$ complex roots (satisfying $P(\lambda_i) = 0$) and $\alpha$ is the leading coefficient of $P$.*

*Remark* 3.3. If $P(x) \in \mathbb{R}[x]$ and $P(\lambda) = 0$, then $P(\overline{\lambda}) = 0$. In other words, complex roots with nonzero imaginary part always occur in conjugate pairs. Consequently, the number of nonreal roots is even, and every polynomial of odd degree must have at least one real root. Moreover, every polynomial with real coefficients can be factored into polynomials of degree one with real roots and polynomials of degree two with nonreal roots $\lambda_i$ and $\overline{\lambda_i}$.

## 3.2 Some Exercises

In this section we solve a selection of exercises to illustrate various techniques with complex numbers.

**Exercise 3.4.** *Simplify the following expressions:*

$$\frac{1-i}{3i-4} \qquad \sum_{n=1}^{2024} n i^n,$$

$$\frac{(1+i)^{2024}}{2^{2022}} \qquad (1+\sqrt{3}i)^{2024},$$

$$(1+i)^{2015} + (1-i)^{2015} \qquad \left(\frac{-1+\sqrt{3}i}{2}\right)^{-2}.$$

**Solution.**

$$\frac{1-i}{3i-4} = \frac{1-i}{3i-4} \cdot \frac{-3i-4}{-3i-4} = \frac{-3i-4-3+4i}{16+9} = \frac{i-7}{25}.$$

$$\frac{(1+i)^{2024}}{2^{2022}} = \left(\frac{1+i}{\sqrt{2}}\right)^{2024} \cdot \frac{1}{2^{1010}} = (e^{\frac{i\pi}{4}})^{2024} \cdot \frac{1}{2^{1010}} = \frac{(e^{2\pi i})^{253}}{2^{1010}} = \frac{1}{2^{1010}}$$

$$(1+i)^{2015} + (1-i)^{2015} = \left(\sqrt{2}e^{\frac{i\pi}{4}}\right)^{2015} + \left(\sqrt{2}e^{\frac{-i\pi}{4}}\right)^{2015} = 2^{2015/2}\left(e^{\cancelto{-1}{\frac{2015\pi i}{4}}} + e^{\cancelto{1}{\frac{-2015\pi i}{4}}}\right) =$$

$$= 2^{2015/2}\left(e^{\frac{-\pi i}{4}} + e^{\frac{\pi i}{4}}\right) = 2^{2015/2}\left(\frac{1-i}{\sqrt{2}} + \frac{1+i}{\sqrt{2}}\right) = 2^{1008}$$

$$\sum_{n=1}^{2024} ni^n = i + 2i^2 + 3i^3 + \cdots + 2024i^{2024} = i(1-3+5-\cdots-2023) + (-2+4-6+\cdots+2024) = 1012 - 1012i$$

$$(1+\sqrt{3}i)^{2024} = \left(2e^{\frac{i\pi}{3}}\right)^{2024} = 2^{2024}e^{\cancelto{2}{\frac{2024i\pi}{3}}} = 2^{2024}e^{\frac{2i\pi}{3}} = 2^{2024}\left(\frac{-1+\sqrt{3}i}{2}\right) = 2^{2023}(-1+\sqrt{3}i)$$

Note how raising a complex number to a power requires expressing it in polar form and reducing the angle modulo $360°$.
For the final expression, there are multiple possible approaches. Of course, one can simply perform all the computations by hand:

$$\left(\frac{-1+\sqrt{3}i}{2}\right)^{-2} = \left(\frac{2}{-1+\sqrt{3}i}\right)^{2} = \frac{4}{-2-2\sqrt{3}i} = -\frac{2}{1+\sqrt{3}i} \cdot \frac{1-\sqrt{3}i}{1-\sqrt{3}i} = \frac{-1+\sqrt{3}i}{2}$$

Even better, one can use polar form:

$$\left(\frac{-1+\sqrt{3}i}{2}\right)^{-2} = \left(e^{\frac{2i\pi}{3}}\right)^{-2} = e^{-\frac{4i\pi}{3}} = e^{\frac{2i\pi}{3}} = \frac{-1+\sqrt{3}i}{2}.$$

Finally, one can realize that the number $z = \frac{-1+\sqrt{3}i}{2}$ is such that $z^3 = 1$. Such number is known as *third root of unity*. As a consequence, $z^n = z^{n \bmod 3}$, and therefore $z^{-2} = z^1 = z$, since $-2 \equiv 1 \bmod 3$. □

**Exercise 3.5.** *Determine how many solutions of the equation*

$$z^{2024} = \sqrt{3} + i$$

*belong to the first quadrant.*

**Solution.**
By the Fundamental Theorem of Algebra, the equation has 2024 complex solutions. Since

$$|\sqrt{3}+i| = 2 \quad \text{and} \quad \arg(\sqrt{3}+i) = \frac{\pi}{6},$$

writing the solutions in polar form $re^{i\theta}$ we must have

$$r^{2024} = 2 \quad \Longrightarrow \quad r = 2^{1/2024},$$

and

$$2024\,\theta = \frac{\pi}{6} + 2k\pi, \quad k \in \mathbb{Z}.$$

Thus, the solutions that lie in the first quadrant are those for which

$$0 \le \frac{\pi/6 + 2k\pi}{2024} \le \frac{\pi}{2}.$$

This inequality simplifies to

$$0 \le 1 + 12k \le 6072,$$

implying $k = 0, 1, \ldots, 505$. Therefore, there are 506 solutions in the first quadrant. □

**Exercise 3.6.** *Let $\alpha$ and $\beta$ be the roots of the polynomial*

$$P(x) = x^2 - 2x + 2.$$

*Compute $\alpha^{2015} + \beta^{2015}$.*

**Solution.**
We start by noting that, for every $n \in \mathbb{N}$,

$$\begin{cases} \alpha^2 = 2\alpha - 2 \\ \beta^2 = 2\beta - 2 \end{cases} \implies \begin{cases} \alpha^{2+n} = 2\alpha^{1+n} - 2\alpha^n \\ \beta^{2+n} = 2\beta^{1+n} - 2\beta^n \end{cases}$$

By setting $S_n := \alpha^n + \beta^n$ the above yields the recurrence

$$S_{n+2} = 2S_{n+1} - 2S_n.$$

What we just did corresponds to the proof of the Newton-Girard formulas. Noting also that $S_0 = 2$ and $S_1 = 2$, we get a solvable linear recurrence relation. This recurrence, however, will have closed form $\alpha^n + \beta^n$, where $\alpha$ and $\beta$ are the complex roots of our polynomial! Therefore, this method is cyclic! One approach to solve this is to compute several initial terms of $S_n$:

| n | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | ... | 31 | $4k-1$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S_n$ | 2 | 2 | 0 | -4 | -8 | -8 | 0 | 16 | 32 | 32 | 0 | -64 | -128 | -128 | 0 | 256 | ... | $4^8$ | $(-4)^k$. |

From the pattern it can be deduced that $S_{4k-1} = (-4)^k$, which can be proved by induction on $k$.[a] Alternatively, one may compute the roots of $P(x)$ directly:

$$x^2 - 2x + 2 = 0 \implies x_{1,2} = 1 \pm i.$$

Writing these in polar form yields

$$(1+i)^{2015} + (1-i)^{2015} = 2^{2015/2}\left(e^{i\frac{2015\pi}{4}} + e^{-i\frac{2015\pi}{4}}\right) = 2^{2015/2}\left(e^{i\frac{\pi}{4}} + e^{-i\frac{\pi}{4}}\right) = 2^{2015/2}\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\right) = 2^{1008}.$$

□

[a] To do it, we need to prove, together with this, $S_{4k} = 2(-4)^k$. At this point we have

$S_{4k+4} = 2S_{4k+3} - 2S_{4k+2} = 2(2S_{4k+2} - 2S_{4k+1}) - 2(2S_{4k+1} - 2S_{4k}) = 4(2S_{4k+1} - 2S_{4k}) - 8S_{4k+1} + 4S_{4k} = -4S_{4k} = -8(-4)^k = 2(-4)^{k+1}$

and

$S_{4k+3} = 2S_{4k+2} - 2S_{4k+1} = 2(2S_{4k+1} - 2S_{4k}) - 2(2S_{4k} - 2S_{4k-1}) = 4(2S_{4k} - 2S_{4k-1}) - 8S_{4k} + 4S_{4k-1} = -4S_{4k-1} = -4(-4)^k = (-4)^{k+1}$.

## 3.3 Complex Roots of Unity

Our next step is to study roots of unity and their main properties.

**Definition 3.7.** Given $n \in \mathbb{N}$, we call the solutions $\omega_1, \ldots, \omega_n$ of the equation

$$z^n = 1 \tag{3.1}$$

the *n-th roots of unity.*

**Theorem 3.8.** *The n-th roots of unity form the vertices of a regular n-gon inscribed in the unit circle.*

**Proof.** Writing $z = re^{i\theta}$ and equating magnitude and argument on both sides of (3.1), we require

$$r^n = 1 \implies r = 1 \quad \text{and} \quad n\theta = 2k\pi, \quad k \in \mathbb{Z} \implies \theta = \frac{2k\pi}{n}$$

Therefore, we obtain the explicit formula:

$$\boxed{\omega_k = \exp\left(\frac{2\pi i k}{n}\right), \quad k = 1, \ldots, n.}$$

□

Roots of unity will be protagonists of the upcoming chapters. Arguably, the three main identities with roots of unity are the following:

$$\boxed{\omega_k^n = 1}, \quad \boxed{\omega_k = \omega_1^k}, \quad \boxed{\omega_1 + \omega_2 + \cdots + \omega_n = 0}.$$

The first identity is simply the definition. The second arises because expressing $\omega_k$ and $\omega_1$ in polar form shows that multiplying $\omega_1$ by itself $k$ times rotates the unit angle $\frac{2\pi}{n}$ $k$ times, reaching $\omega_k$. Finally, the third identity can be derived by writing

$$\omega_1 + \cdots + \omega_n = \omega_1 + \omega_1^2 + \cdots + \omega_1^{n-1} + \omega_1^n = 1 + \omega_1 + \omega_1^2 + \cdots + \omega_1^{n-1} = \frac{\omega_1^n - 1}{\omega_1 - 1} = 0.$$

*Remark* 3.9. The identity $\omega_1 + \omega_2 + \cdots + \omega_n = 0$ has a beautiful geometric derivation. The sum $\omega_1 + \cdots + \omega_n$ can be rephrased as the sum of $n$ equal forces acting in opposite directions as the vertices of a regular $n$-gon. Of course, by symmetry, these forces cancel out, yielding a net force of zero. But how to formally justify this argument? The trick is to assume by contradiction that the sum of the forces is nonzero. Then, it must point in some direction. If we rotate the system by $2\pi/n$ nothing changes to the initial configuration; however, the sum of the forces must have changed its direction. This is a clear contradiction. Algebraically, this rotation corresponds to multiply $S = 1 + \omega_1 + \cdots + \omega_1^{n-1}$ by $\omega_1$, obtaining

$$\omega_1 S = \omega_1 + \cdots + \omega_1^n + \omega_1^{n+1} = 1 + \omega_1 + \cdots + \omega_1^{n-1} = S.$$

From here, we deduce that $S = 0$.

### 3.3.1 Third Roots of Unity

Third roots of unity are

$$\omega_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \qquad \omega_2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i \quad \text{and} \quad \omega_3 = \omega_0 = 1.$$

$\omega := \omega_1$ and $\omega_2 = \omega^2$ naturally arise as the roots of $x^2 + x + 1$, a terribly common polynomial in mathematical olympiads. As a remarkable property,

$$\boxed{\omega^2 = \overline{\omega} = \omega^{-1} = \frac{1}{\omega}} \implies \omega + \overline{\omega} = \omega + \frac{1}{\omega} = -1.$$

**Exercise 3.10.** *Let $x_1, x_2, x_3$ be the roots of $x^3 - 1$. Prove that, for every $n \in \mathbb{N}$,*

$$x_1^n + x_2^n + x_3^n = x_1^n x_2^n + x_2^n x_3^n + x_3^n x_1^n.$$

**Solution.**
Write $x_1 = \omega$, $x_2 = \omega^2$, and $x_3 = \omega^3 = 1$. Then,

$$\omega^n + \omega^{2n} + 1 \stackrel{?}{=} \omega^n \omega^{2n} + \omega^{2n}\omega^{3n} + \omega^{3n}\omega^n = \omega^{3n} + \omega^{2n} + \omega^n = 1 + \omega^{2n} + \omega^n.$$

□

**Exercise 3.11.** *Prove that $x^2 + x + 1 | x^7 + x^2 + 1$.*

**Solution.**
It suffices to show that both $\omega$ and $\omega^2$ (the roots of $x^2 + x + 1$) are roots of $x^7 + x^2 + 1$. Observe that

$$\omega^7 + \omega^2 + 1 = (\omega^3)^2 \cdot \omega + \omega^2 + 1 = 1 + \omega + \omega^2 = 0,$$

and similarly,

$$(\omega^2)^7 + (\omega^2)^2 + 1 = \omega^{14} + \omega^4 + 1 = (\omega^3)^4 \cdot \omega^2 + \omega^3 \cdot \omega + 1 = 1 + \omega + \omega^2 = 0.$$

Alternatively, we anticipate polynomial congruences which will be a crucial topic of the next chapter. We need to compute $x^7 + x^2 + 1 \bmod (x^2 + x + 1)$. Since $x^3 - 1 = (x-1)(x^2 + x + 1)$, we have $x^3 \equiv 1$ modulo $(x^2 + x + 1)$, which implies $x^7 + x^2 + 1 \equiv x + x^2 + 1 \equiv 0 \bmod (x^2 + x + 1)$. □

**Exercise 3.12.** *If $x + \frac{1}{x} = -1$, compute*

$$\sum_{n=1}^{1010} x^{2n} + x^n + 1.$$

**Solution.**
Multiplying the equation by $x$, we deduce that $x$ satisfies $x^2 + x + 1 = 0$, or, equivalently, $x^3 = 1$. Therefore, $x = \omega$. In particular, if $3 \nmid n$, then

$$x^{2n} + x^n + 1 = \frac{x^{3n} - 1}{x^n - 1} = 0,$$

while if $3 \mid n$, then $x^{2n} + x^n + 1 = 1 + 1 + 1 = 3$. Therefore,

$$\sum_{n=1}^{1010} \left(x^{2n} + x^n + 1\right) = \sum_{k=1}^{\lfloor 1010/3 \rfloor} 3 = 336 \cdot 3 = 1008.$$

□

**Exercise 3.13.** *Find a formula to solve cubic equations $ax^3 + bx^2 + cx + d = 0$.*

**Solution.**
This derivation is taken from [6]. Start with the classic decomposition

$$x^3 + a^3 + b^3 - 3abx = (x + a + b)(x^2 + a^2 + b^2 - ax - bx - ab).$$

Let us find the roots of the quadratic term:

$$x_i = \frac{1}{2}\left(a + b \pm \sqrt{(a+b)^2 - 4a^2 - 4b^2 + 4ab}\right) = \frac{1}{2}\left(a + b \pm \sqrt{-3}\sqrt{a^2 + b^2 - 2ab}\right) = -(a\omega^i + b\omega^{2i}).$$

Hence, the cubic equation $x^3 - 3abx + a^3 + b^3 = 0$ has the solutions

$$x_1 = -a - b, \quad x_2 = -a\omega - b\omega^2, \quad x_3 = -a\omega^2 - b\omega.$$

Therefore, to solve $x^3 + px + q = 0$, we require $p = -3ab$ and $q = a^3 + b^3$, or

$$a^3 b^3 = -p^3/27 \quad \text{and} \quad a^3 + b^3 = q.$$

Then $a^3$ and $b^3$ are the roots of the quadratic

$$z^2 - qz - p^3/27 = 0,$$

implying

$$a^3, b^3 = \frac{1}{2}\left(q \pm \sqrt{q^2 + \frac{4p^3}{27}}\right) \implies a, b = \sqrt[3]{\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Finally, the solutions to $x^3 + px + q = 0$ are

$$x_1 = -\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

$$x_2 = -\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\left(\frac{-1 + \sqrt{3}i}{2}\right) - \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\left(\frac{-1 - \sqrt{3}i}{2}\right)$$

$$x_3 = -\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\left(\frac{-1 - \sqrt{3}i}{2}\right) - \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\left(\frac{-1 + \sqrt{3}i}{2}\right)$$

Any cubic can be transformed into this form by dividing by $a$ and setting $x = t - \frac{b}{3a}$.[a] □

[a] This formula was originally developed by Scipione Del Ferro and later independently discovered by Niccolò Tartaglia, who kept it secret to gain an advantage in mathematical challenges (known as *disfide matematiche*). Eventually, Gerolamo Cardano obtained Tartaglia's method and published it in his seminal work *Ars Magna*, which is why the formula is now known as Cardano's Formula [7].

### 3.3.2 Higher Order Roots of Unity

Fourth roots of unity are simply $\pm 1$ and $\pm i$. Similarly, the sixth roots of unity are $\pm 1$, $\pm\omega$ and $\pm\omega^2$, where $\omega$ is the canonical third root of unity (i.e. $e^{2\pi i/3}$). In general, if $d$ is an odd integer, then the $2d$-th roots of unity consist of the combined solutions of $z^d = 1$ and $z^d = -1$, given by their opposites.

**Exercise 3.14.** *Compute* $\cos(72°)$ *and* $\sin(72°)$.

**Solution.**
Since $72° = \frac{2\pi}{5}$, we simply need to compute $\omega = \omega_1$, where $\omega_1$ denotes the canonical fifth root of unity. We have

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0 \iff \omega^2 + \frac{1}{\omega^2} + \omega + \frac{1}{\omega} + 1 = 0 \iff \left(\omega + \frac{1}{\omega}\right)^2 + \omega + \frac{1}{\omega} - 1 = 0.$$

From here, we can find $\omega + \frac{1}{\omega} = \frac{\sqrt{5}-1}{2}$. There's no need of solving the equation directly: it suffices to note that $1/\omega = \omega^{-1} = \overline{\omega}$, meaning that $\omega + \overline{\omega} = \frac{\sqrt{5}-1}{2}$, or

$$\Re\mathfrak{e}(\omega) = \frac{\sqrt{5}-1}{4} \implies \Im\mathfrak{m}(\omega) = \sqrt{1 - \Re\mathfrak{e}^2(\omega)} = \sqrt{\frac{5+\sqrt{5}}{8}} \implies \omega = \underbrace{\frac{\sqrt{5}-1}{4}}_{\cos(72°)} + i \underbrace{\sqrt{\frac{5+\sqrt{5}}{8}}}_{\sin(72°)}.$$

□

**Exercise 3.15** (USAMO 1996)**.** *Compute*

$$\frac{1}{45}\sum_{n=1}^{90} n \sin\left(\frac{n\pi}{90}\right)$$

**Solution.**
We begin with a gaussian pairing[a] to simplify the computation:

$$\sum_{n=1}^{90} n \sin\left(\frac{n\pi}{90}\right) = 90\sin(\pi) + 45\sin\left(\frac{\pi}{2}\right) + \sum_{n=1}^{44} n \sin\left(\frac{n\pi}{90}\right) + (90-n)\sin\left(\frac{(90-n)\pi}{90}\right) = 45 + \sum_{n=1}^{44} 90 \sin\left(\frac{(90-n)\pi}{90}\right).$$

Therefore, our goal reduces to computing

$$S = 1 + 2\sum_{n=1}^{44} \sin\left(\frac{n\pi}{90}\right).$$

To handle the sum of sines, it is often useful to recall (1.6), and so write

$$\sin\left(\frac{n\pi}{90}\right) = \frac{\exp\left(\frac{n\pi i}{90}\right) - \exp\left(-\frac{n\pi i}{90}\right)}{2i} = \frac{\omega^n - \omega^{-n}}{2i},$$

where $\omega := \omega_1$ is the canonical 180-th root of unity. Therefore

$$\begin{aligned}
1 + 2\sum_{n=1}^{44} \sin\left(\frac{n\pi}{90}\right) &= 1 + \frac{1}{i}\sum_{n=1}^{44} \omega^n - \omega^{-n} = 1 + \frac{1}{i}\left[\frac{\omega^{45} - \omega}{\omega - 1} - \frac{\omega^{-45} - \omega^{-1}}{\omega^{-1} - 1}\right] = 1 + \frac{1}{i}\left[\frac{i - \omega}{\omega - 1} - \frac{-i - \omega^{-1}}{\omega^{-1} - 1}\right] \\
&= 1 + \frac{1}{i}\left[\frac{i - \omega}{\omega - 1} + \frac{i\omega + 1}{1 - \omega}\right] = 1 + \frac{1}{i}\left[\frac{i - \omega}{\omega - 1} + i\frac{i - \omega}{\omega - 1}\right] = 1 + \frac{1+i}{i}\cdot\frac{i - \omega}{\omega - 1} \\
&= \frac{\omega - 1 + (-i+1)(i - \omega)}{\omega - 1} = i\frac{\omega + 1}{\omega - 1} = i\frac{\cos\theta + i\sin\theta + 1}{\cos\theta - 1 + i\sin\theta},
\end{aligned}$$

with $\theta = \pi/90$. Further simplifications yield

$$\begin{aligned}
i\frac{\cos\theta + i\sin\theta + 1}{\cos\theta - 1 + i\sin\theta}\cdot\frac{\cos\theta - 1 - i\sin\theta}{\cos\theta - 1 - i\sin\theta} &= i\frac{\cos^2\theta + \sin^2\theta - 1 - 2i\sin\theta}{\cos^2\theta + 1 - 2\cos\theta + \sin^2\theta} = \frac{2\sin\theta}{2 - 2\cos\theta} = \frac{\sin\theta}{1 - \cos\theta} \\
&= \frac{2\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right)}{2\sin^2\left(\frac{\theta}{2}\right)} = \frac{1}{\tan\left(\frac{\pi}{180}\right)} = \cot\left(\frac{\pi}{180}\right).
\end{aligned}$$

□

[a]Gaussian pairing refers to the brilliant trick that the young Gauss used to quickly find the sum of the first 100 positive integers. He paired numbers $n$ and $101-n$ together before summing: $\sum_{n=1}^{100} n = \sum_{n=1}^{50} n + (101-n) = 5050$.

# 4 Number Theory: Primitive Roots of Unity and Congruences

As anticipated in Exercises 3.11 and 3.12, algebraic computations with roots of unity can often be reinterpreted as modular arithmetic on their exponents. In this section, we delve deeper into the underlying structure of these numbers. To begin, let us consider an exercise that explicitly demonstrates this shift in perspective from algebra to number theory:

**Exercise 4.1** (Mathesis Vicentina 2022). *Let $\omega_1, \omega_2, \ldots, \omega_{100}$ be the 100 distinct complex roots of $x^{101}-1$ different from 1. Define*

$$I = \Big\{ n \in \mathbb{N} : n = \operatorname{card}\{\omega_{\sigma(1)}, \omega_{\sigma(2)}^2, \ldots, \omega_{\sigma(100)}^{100}\},\ \sigma \in S_{100} \Big\},$$

*i.e. $I$ is the set of all possible cardinalities of*

$$\{\omega_{\sigma(1)}, \omega_{\sigma(2)}^2, \ldots, \omega_{\sigma(100)}^{100}\}$$

*as $\sigma$ ranges over the possible permutations of $\{1,\ldots,100\}$. Calculate $\max I - \min I$.*

**Solution.**
It's clear that

$$\{\omega_{\sigma(1)}, \omega_{\sigma(2)}^2, \ldots, \omega_{\sigma(100)}^{100}\} = \{\omega^{1\sigma(1)}, \omega^{2\sigma(2)}, \ldots, \omega^{100\sigma(100)}\}.$$

We can directly focus on the exponents, and the problem becomes equivalent to asking "*What is the minimum and maximum number of distinct residues modulo 101 that the set*

$$I = \{i \cdot \sigma(i) \bmod 101 : i = 1, \ldots, 100\}$$

*can have as $\sigma$ varies over all permutations of $\{1,\ldots,100\}$?*". For the minimum, choose the permutation $\sigma$ defined by

$$\sigma(i) = i^{-1} \mod 101,$$

(which is a permutations, thanks to the existence and uniqueness of multiplicative inverse modulo 101), so that

$$i\,\sigma(i) \equiv 1 \pmod{101} \quad \text{for all } i.$$

Then the resulting set has only one element, and thus $\min I = 1$.
For the maximum, one can show that the set cannot have 100 distinct elements. In fact, if it did, then

$$\prod_{i=1}^{100} \big(i\,\sigma(i)\big) \equiv \prod_{i=1}^{100} i \pmod{101}.$$

This would imply

$$(100!)^2 \equiv 100! \pmod{101},$$

so that $100! \equiv 1 \pmod{101}$; however, by Wilson's Theorem (since 101 is prime) we have $100! \equiv -1 \pmod{101}$, a contradiction. It turns out that one can choose a permutation for which the set has 99 distinct elements; for instance, define

$$\sigma(i) = 1 + i^{-1} \pmod{101} \quad \text{for } i = 1, \ldots, 99,$$

and set $\sigma(100) = 1$. We then obtain $I = \{2, 3, \ldots, 100, 100\}$, which has cardinality 99. Then $\max I = 99$ and the difference is

$$\max I - \min I = 99 - 1 = 98.$$

□

The following theorem—and its generalization to composite numbers—is arguably one of the most important results of this section:

**Theorem 4.2.** *Let $p$ be a prime number and let $\omega_1, \omega_2, \ldots, \omega_p$ denote the $p$-th roots of unity. Then, for every integer $m$ with $p \nmid m$,*

$$\{\omega_1, \omega_2, \ldots, \omega_p\} = \{\omega_1, \omega_1^2, \ldots, \omega_1^p\} = \{\omega_m, \omega_m^2, \ldots, \omega_m^p\}.$$

**Proof.** Let $\omega := \omega_1$. We must show that

$$\{\omega^m, \omega^{2m}, \ldots, \omega^{pm}\} = \{\omega, \omega^2, \ldots, \omega^p\}.$$

Since $\omega^p = 1$, the exponents are taken modulo $p$. Therefore, passing to the exponents, it suffices to prove that

$$\{1, 2, \ldots, p\} = \{m, 2m, \ldots, pm\} \pmod p.$$

This is a standard fact in number theory when $m$ is coprime to $p$. □

*Remark* 4.3. The reasoning above, which translates problems about $n$-th roots of unity into problems about their exponents modulo $n$, is the bridge between number theory and algebra.

**Corollary 4.4.** *If $p$ is a prime number, $\omega := \omega_1$, and $\omega_i$ denote the $p$-th roots of unity, then for every $n \in \mathbb{Z}$,*

$$\sum_{i=1}^{p} \omega^{ni} = \begin{cases} 0, & \text{if } p \nmid n, \\ p, & \text{if } p \mid n. \end{cases}$$

To understand what happens when $p$ is not prime, let us first define what it means for a root of unity to be *primitive*, in analogy with the concept of a generator in modular arithmetic.

**Definition 4.5** (Primitive Roots of Unity)**.** Let $n$ be a positive integer. A primitive $n$-th root of unity $\omega$ is an $n$-th root of unity satisfying

$$\omega^n = 1 \quad \text{and} \quad \omega^k \neq 1 \quad \text{for any positive integer } k < n.$$

When $n$ is composite, some roots of unity other than 1 may fail to be primitive. For instance, $-1$ is a fourth root of unity, but it is not primitive since $(-1)^2 = 1$. Primitive roots of unity act like generators in modular arithmetic: they "travel through" all the distinct roots before returning to 1. In this way, they generate the full set of $n$-th roots over their cycle.

**Theorem 4.6.** *The primitive $n$-th roots of unity are given by $\omega_k = \exp\left(\frac{2\pi i k}{n}\right)$ for all $k$ with $\gcd(k, n) = 1$. Consequently, there are $\phi(n)$ primitive $n$-th roots of unity, where $\phi(n)$ denotes Euler's totient function.*

**Proof.** First, note that $\omega_1 = \exp\left(\frac{2\pi i}{n}\right)$ is a primitive $n$-th root of unity since its powers $\omega_1^k$ for $k = 1, \ldots, n$ are all distinct and $\omega_1^n = 1$. If $\gcd(k, n) = d > 1$, then $(\omega_k)^{n/d} = \omega_1^{nk/d} = (\omega_1^n)^{k/d} = 1$, so $\omega_k$ is not primitive. Conversely, if $\gcd(k, n) = 1$ and $\omega_k^r = 1$, then $\omega_1^{kr} = 1$. Since $\omega_1$ is a primitive root of unity, then $n | kr$. Since $n$ and $k$ are coprime, it follows that $n \mid r$, hence $\omega_k$ is indeed a primitive $n$-th root of unity. □

The equivalent number-theoretic formulation of this fact is as follows: if $\gcd(k, n) = 1$, then

$$\{1, 2, \ldots, n\} \equiv \{k, 2k, \ldots, kn\} \pmod n.$$

**Exercise 4.7.** *Let $f_n(x) = x^{4n} + x^{3n} + x^{2n} + x^n + 1$. Find the remainders when $f_2(x)$ and $f_5(x)$ are divided by $f_1(x)$.*

**Solution.**
Since

$$f_1(x)(x-1) = x^5 - 1,$$

we can factorize

$$f_1(x) = (x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4),$$

where $\omega$ is a primitive 5th root of unity. For any $i = 1, \ldots, 4$ and any exponent $n$, evaluate

$$f_n(\omega^i) = \omega^{4in} + \omega^{3in} + \omega^{2in} + \omega^{in} + 1.$$

We can easily conclude thanks to corollary 4.4. To better understand what's going on, let us explicitly show all the computations. For $n = 5$ we have $\omega^{5ki} = 1$ for any integer $k$; hence, for every $i$,

$$f_5(\omega^i) = 1 + 1 + 1 + 1 + 1 = 5.$$

Thus,
$$f_5(x) \equiv 5 \pmod{(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4)},$$
i.e. $f_5(x) \equiv 5 \pmod{f_1(x)}$.
For $n = 2$ we compute
$$f_2(\omega^i) = \omega^{8i} + \omega^{6i} + \omega^{4i} + \omega^{2i} + 1.$$

- Se $i = 1$ we obtain $f_2(\omega) = \omega^8 + \omega^6 + \omega^4 + \omega^2 + 1 = \omega^3 + \omega + \omega^4 + \omega^2 + 1 = 0$.
- Se $i = 2$ we obtain $f_2(\omega^2) = \omega^{16} + \omega^{12} + \omega^8 + \omega^4 + 1 = \omega + \omega^2 + \omega^3 + \omega^4 + 1 = 0$.
- Se $i = 3$ we obtain $f_2(\omega^3) = \omega^{24} + \omega^{18} + \omega^{12} + \omega^6 + 1 = \omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$.
- Se $i = 4$ we obtain $f_2(\omega^4) = \omega^{32} + \omega^{24} + \omega^{16} + \omega^8 + 1 = \omega^2 + \omega^4 + \omega + \omega^3 + 1 = 0$.

Therefore, $\omega^i$ is a root of $f_2(x)$ for every $i = 1, \dots, 4$, which implies that $f_1(x) \mid f_n(x)$. More generally, one can observe that
$$\{0,\ in,\ 2in,\ 3in,\ 4in\} \equiv \{0, 1, 2, 3, 4\} \pmod 5$$
for every $i = 1, 2, 3, 4$ provided that $5 \nmid n$, whereas $\{0,\ in,\ 2in,\ 3in,\ 4in\} \equiv \{0\} \pmod 5$ if $5 \mid n$.

□

**Exercise 4.8.** *Let $P(x)$ be a monic quartic polynomial. It is given that $P(x)$ leaves a remainder of $3-3x$ upon division by $x^2+x+1$, and a remainder of $-5x-43$ upon division by $x^2-x+1$. Calculate the sum of all possible values of $P(5)$.*

**Solution.**
Proceed as you would when working with congruences over the integers, namely by substitution. Write
$$P(x) = Q(x)(x^2+x+1) + (3-3x),$$
where $Q(x)$ is a monic quadratic polynomial, say $Q(x) = x^2 + ax + b$. Next, impose the congruence condition modulo $x^2 - x + 1$:
$$\begin{aligned}
P(x) &= (x^2+ax+b)(x^2-x+1) + 3 - 3x \\
&= \big[(x^2-x+1) + (a+1)x + (b-1)\big]\big[(x^2-x+1) + 2x\big] + 3 - 3x \\
&\equiv \big[(a+1)x + (b-1)\big] \cdot 2x + 3 - 3x \\
&= (2a+2)x^2 + (2b-2-3)x + 3 \\
&\equiv (2a+2)(x^2-x+1) + (2b-5+2a+2)x + (3-2a-2) \\
&\equiv (2b+2a-3)x + (1-2a) \equiv -5x - 43 \pmod{x^2-x+1}.
\end{aligned}$$
From this congruence we deduce that the unique solution is $a = 22$ and $b = -23$. Therefore,
$$P(x) = (x^2+22x-23)(x^2+x+1) + 3 - 3x.$$
Hence, $P(5) = 3460$ is the unique possible value.[a] □

[a] Note that if one substitutes $x = 5$ from the outset, one obtains
$$P(5) \equiv -12 \equiv 19 \pmod{31} \quad \text{and} \quad P(5) \equiv -68 \equiv 16 \pmod{21}.$$
Solving this system yields $P(5) = 205 + 651k$, with $k$ an integer. However, it is not immediately obvious how to conclude that the only value of $k$ satisfying the conditions is $k = 5$. Therefore, polynomial congruences seem to be the only applicable road.

**Exercise 4.9.** *Find the remainder when $x^{1959} - 1$ is divided by $(x^2+1)(x^2+x+1)$.*

**Solution.**
First, consider dividing $x^{1959} - 1$ by $x^2 + 1$. Since $x^2 \equiv -1 \pmod{x^2+1}$, it follows that
$$x^{1959} - 1 \equiv -x - 1 \pmod{x^2+1}.$$

Next, observing that $x^3 - 1 = (x-1)(x^2+x+1)$, then $x^3 \equiv 1 \pmod{x^2+x+1}$ and

$$x^{1959} - 1 \equiv x^{(1959 \bmod 3)} - 1 \equiv 1 - 1 \equiv 0 \pmod{x^2+x+1}.$$

The problem then reduces to finding a linear polynomial $Q(x) = ax + b$ such that

$$Q(x)(x^2+x+1) \equiv -x-1 \pmod{x^2+1}.$$

Since $x^2 + 1 \equiv 0 \bmod (x^2+1)$, then clearly

$$Q(x)(x^2+x+1) \equiv xQ(x) \equiv x(ax+b) \equiv ax^2 + bx \equiv -a + bx \pmod{x^2+1} \implies a = 1, b = -1.$$

Thus, thanks to the Chinese remainder theorem, $x^{1959} - 1 \equiv x^3 - 1 \pmod{(x^2+1)(x^2+x+1)}$. □

## 5 Combinatorics: Counting with Roots of Unity

In this section, we explore how complex numbers can be used to solve counting problems. The key idea is to encode the combinatorial structure into a generating polynomial whose coefficients represent the quantities to be counted. Then, by evaluating the polynomial at appropriate roots of unity, we can "filter out" unwanted terms and isolate those of interest—a process known as the *roots of unity filter*. We will illustrate its power through a series of concrete examples.

**Exercise 5.1.** *Compute*

$$\sum_{k=0}^{33} \binom{33}{k} \quad \text{and} \quad \sum_{k=0}^{11} \binom{33}{3k}.$$

**Solution.**
The first sum is simply the sum of the coefficients of the polynomial $P(x) = (1+x)^{33}$. To find it, we simply evaluate $P$ at $x = 1$, obtaining $P(1) = (1+1)^{33} = 2^{33}$.
The second sum is the sum of the coefficients corresponding to exponents divisible by 3 in the same polynomial. To compute it, we use the *roots of unity filter*. This corresponds to the *arithmetic mean* of values of $P$ evaluated in the $n$-th roots of unity, with a certain $n$. Since we wish to select terms where the exponent is divisible by 3, it suffices to consider the 3rd roots of unity, computing

$$\sum_{k=0}^{11} \binom{33}{3k} = \frac{P(1)+P(\omega)+P(\omega^2)}{3} = \frac{(1+1)^{33}+(1+\omega)^{33}+(1+\omega^2)^{33}}{3} = \frac{2^{33}+(-\omega^2)^{33}+(-\omega)^{33}}{3} = \frac{2^{33}-2}{3}.$$

To understand why this works, we recall that

$$\omega^{2n} + \omega^n + 1^n = \begin{cases} 1+1+1 & \text{se } 3|n \\ 1+\omega+\omega^2 = 0 & \text{se } 3 \not| n \end{cases}$$

Therefore, when summing $P(1) + P(\omega) + P(\omega^2)$, for every term $a_n x^n$, we will obtain

$$a_n = \frac{a_n \cdot 1^n + a_n\omega^n + a_n\omega^{2n}}{3}$$

if and only if $3|n$. For this reason, the $n$-th roots of unity are *filters*, which filter only terms corresponding to exponents divisible by $n$, and making zero all the others. □

**Exercise 5.2** (High-School Mathematics, 1994/1, Qihong Xie)**.** *[8] Compute the number of subsets of* $\{1, 2, \ldots, 2000\}$*, the sum of whose elements is divisible by* 5.

**Solution.**
Consider the generating function

$$P(x) = (1+x)(1+x^2)(1+x^3)\cdot \ldots \cdot (1+x^{2000}).$$

There is a clear bijection between the subsets of $\{1, 2, \dots, 2000\}$ and the terms in the expansion of $P(x)$ of the form

$$x^{a_1+a_2+\cdots+a_m}.$$

Hence, the problem reduces to finding the sum of the coefficients corresponding to exponents divisible by 5 in $P$. Using the roots of unity filter, we evaluate

$$\frac{P(1)+P(\omega)+P(\omega^2)+P(\omega^3)+P(\omega^4)}{5},$$

where $\omega$ is a primitive 5th root of unity. Noting that

$$\begin{aligned}(1+\omega)(1+\omega^2)(1+\omega^3)(1+\omega^4)(1+\omega^5) &= 2(1+\omega)(1+\omega^2)(1+\frac{1}{\omega^2})(1+\frac{1}{\omega}) = 2(2+\omega+\frac{1}{\omega})(2+\omega^2+\frac{1}{\omega^2}) \\ &= 2(4+\omega^3+\frac{1}{\omega^3}+\omega+\frac{1}{\omega}+2(\omega+\omega^2+\frac{1}{\omega}+\frac{1}{\omega^2})) \\ &= 2(4+\underbrace{\omega^3+\omega^2+\omega+\omega^4}_{-1}+2(\underbrace{\omega+\omega^2+\omega^4+\omega^3}_{-1}) \\ &= 2(4-1-2) = 2.\end{aligned}$$

Thanks to this observation we conclude that

$$P(\omega) = P(\omega^2) = P(\omega^3) = P(\omega^4) = 2^{400},$$

and $P(\omega^5) = P(1) = 2^{2000}$. We finally conclude that

$$\frac{P(1)+P(\omega)+P(\omega^2)+P(\omega^3)+P(\omega^4)}{5} = \frac{2^{2000}+2^{400}+2^{400}+2^{400}+2^{400}}{5} = \frac{2^{2000}+2^{402}}{5}.$$

□

**Exercise 5.3** (OliMaTo 2023)**.** *[2] There are* 2023 *pens numbered from* 1 *to* 2023*. Dragons are to be placed in some of these pens so that the sum of the numbers of the occupied pens leaves a remainder of* 2023 *when divided by* 2048*. How many ways are there to choose which pens to occupy?*

**Solution.**
*First solution:* We consider the generating function

$$P(x) = (1+x)(1+x^2)\cdots(1+x^{2023}).$$

Similarly to the previous problem, the coefficients of this polynomial represent the subsets of $\{1, 2, \dots, 2023\}$. The problem asks for the sum of the coefficients of the monomials with exponents congruent to 2023 modulo 2048. To do it, we introduce a shifted polynomial $Q(x) = x^{25}P(x)$ and use the roots of unity filter with the 2048th roots of unity:

$$\frac{1}{2048}\sum_{i=1}^{2048} Q(\omega^i) = \frac{1}{2048}\sum_{i=1}^{2048} \omega^{25i}(1+\omega^i)(1+\omega^{2i})\cdot\ldots\cdot(1+\omega^{2023i}).$$

To simplify this expression, we first observe that $\omega^{2012} = -1$. Therefore, for any index $i$ for which there exists some $n$ with

$$ni \equiv 2012 \pmod{2048},$$

we have $(1+\omega^{ni}) = 1-1 = 0$, so that the entire product $Q(\omega^i) = 0$.
In particular, if $i$ is odd, one can simply take $n = 2012$. If $i$ is even, one may choose $n = \frac{2012}{2^x}$, where $x$ is the 2-adic valuation of $i$. The only case where $Q$ does not vanish is when $i \equiv 0 \pmod{2048}$, i.e. when $i = 2048$; in this case, $\omega^{2048} = 1$ and hence $Q(1) = 2^{2023}$.
Thus, we obtain

$$\frac{1}{2048}\sum_{i=1}^{2048} Q(\omega^i) = \frac{2^{2023}}{2048} = 2^{2012}.$$

*Alternate solution:* The official solution is less technical and more elegant. Denote by $s(A)$ the sum of the elements of a set $A$. Notice that for every integer $0 \le k \le 2047$ there exists exactly one subset $X_k$

of
$$X = \{2^0, 2^1, \ldots, 2^{10}\}$$
such that $s(X_k) = k$ (with the convention $s(\emptyset) = 0$). Consequently, for any subset $Y$ of $\{1, 2, \ldots, 2023\} \setminus X$, there is a unique subset of $X$ such that the combined sum $s(Y) + s(X_k)$ is congruent to 2023 modulo 2048. Therefore, the answer is simply the number of subsets of $\{1, 2, \ldots, 2023\} \setminus X$, which is $2^{2012}$. □

**Exercise 5.4.** *A fair six-sided die is rolled* 10 *times. Calculate the probability of obtaining a total sum between* 57 *and* 59 *(inclusive).*

**Solution.**
Consider the generating function
$$P(x) = (x + x^2 + x^3 + x^4 + x^5 + x^6)^{10}.$$
The problem reduces to computing the coefficients of $x^{57}$, $x^{58}$, and $x^{59}$ in $P(x)$, and then dividing their sum by the total number $6^{10}$ of outcomes.

- The coefficient of $x^{59}$ can be obtained only by choosing $x^6$ in 9 of the factors and $x^5$ in the remaining one, yielding 10 ways.
- The coefficient of $x^{58}$ can be obtained either by selecting $x^5$ in two factors or by choosing $x^4$ in one factor (with $x^6$ in the others). This gives $10 + \binom{10}{2} = 55$ ways.
- The coefficient of $x^{57}$ can be interpreted as choosing $x^6$ in all factors to get $x^{60}$ and then "distributing 3 unit subtractions" among the 10 factors. By the stars and bars argument, the number of ways is
$$\binom{10+3-1}{10-1} = 220.$$

Thus, the total number of favorable outcomes is $10 + 55 + 220 = 285$, and the probability is
$$\frac{285}{6^{10}}.$$
□

**Exercise 5.5.** *Determine the probability that after $n$ rolls of a fair six-sided die, the total sum of the outcomes is divisible by* 5.

**Solution.**
Again, consider the generating function
$$P(x) = (x + x^2 + x^3 + x^4 + x^5 + x^6)^n,$$
where the coefficient of $x^k$ represents the number of ways to obtain a total sum of $k$. To count the outcomes where the sum is a multiple of 5, we apply the roots of unity filter with the 5th roots of unity. Notice that for each $i \in \{1, 2, 3, 4\}$ we have:
$$\omega^i + \omega^{2i} + \omega^{3i} + \omega^{4i} + \omega^{5i} + \omega^{6i} = (1 + \omega^i + \omega^{2i} + \omega^{3i} + \omega^{4i}) + \omega^i = \omega^i,$$
where $\omega$ is a primitive 5th root of unity. Therefore, we obtain
$$P(\omega^i) = \omega^{ni}, \quad \text{and} \quad P(1) = 6^n.$$
Then the filtered sum, divided by $6^n$, is
$$\frac{1}{5 \cdot 6^n} \sum_{i=1}^{5} P(\omega^i) = \frac{1}{5 \cdot 6^n} \Big( 6^n + \omega^n + \omega^{2n} + \omega^{3n} + \omega^{4n} \Big).$$
Hence, thanks to corollary 4.4, the probability is given by
$$\begin{cases} \frac{6^n - 1}{5 \cdot 6^n} & \text{if } 5 \nmid n, \\ \frac{6^n + 4}{5 \cdot 6^n} & \text{if } 5 \mid n. \end{cases}$$

□

The next exercise appeared in the national semifinals of the Italian Team Math Olympiads in 2017 [1].

**Exercise 5.6** (GAS 2017)**.** *During the siege of Jerusalem, the Arabs attempted a sortie each day through one of the four city gates (located at the four cardinal directions). On the first day they used the North gate, and from the second day onward they adopted an ingenious strategy: at dawn they flipped a coin, and if it landed heads they would exit through the gate of the previous day, otherwise through the next gate in anticlockwise order (with the sequence being North, West, South, East). What is the probability that on the* 52*nd day the Arabs will choose the North gate?*

**Solution.**

The total number of outcomes is $2^{52}$. The favorable cases occur when the number of heads is a multiple of 4 (i.e. $52, 48, 44, \dots, 0$). Thus, the desired probability is

$$\frac{1}{2^{52}} \sum_{k=0}^{13} \binom{52}{4k}.$$

This sum is equivalent to the sum of the coefficients corresponding to monomials with exponents that are multiples of 4 in the expansion of

$$P(x) = (1+x)^{52}.$$

Using the roots of unity filter with the fourth roots of unity (namely, $\pm 1$ and $\pm i$), we obtain

$$\begin{aligned}\frac{1}{2^{52}} \sum_{k=0}^{13} \binom{52}{4k} &= \frac{1}{2^{52}} \frac{P(1)+P(-1)+P(i)+P(-i)}{4} = \frac{(1+1)^{52}+(1-1)^{52}+(1+i)^{52}+(1-i)^{52}}{2^{54}} \\ &= \frac{2^{52}+0+\sqrt{2}^{52}(e^{i\pi/4}+e^{-i\pi/4})}{2^{54}} = \frac{2^{52}-2^{27}}{2^{54}} = \frac{2^{25}-1}{2^{27}}.\end{aligned}$$

□

**Exercise 5.7** (Bay area Math Circle 1999)**.** *[8] Let $m$ and $n$ be positive integers. Suppose that a given rectangle can be tiled by a combination of horizontal $1 \times m$ strips and vertical $n \times 1$ strips. Prove that it can be tiled using only one of the two types.*

**Solution.**

It's clear that the rectangle has integer dimensions $a$ and $b$. The proof involves a clever double-counting argument by assigning a complex number to each unit square and summing these over the entire rectangle. Specifically, let $\omega = \exp\left(\frac{2\pi i}{m}\right)$ and $\zeta = \exp\left(\frac{2\pi i}{n}\right)$ be the $m$-th and $n$-th (primitive) roots of unity, respectively. To the square with coordinates $(x, y)$, assign the number $\omega^x \zeta^y$.
Consider a vertical strip of $n \times 1$. If the bottom square in this strip has coordinates $(x, y)$, then the sum of the numbers in that strip is:

$$\omega^x \zeta^y (1 + \zeta + \zeta^2 + \dots + \zeta^{n-1}) = \omega^x \zeta^y \frac{\zeta^n - 1}{\zeta - 1} = 0.$$

Similarly, for a horizontal $1 \times m$ strip with the leftmost square at $(x, y)$, the sum is:

$$\omega^x \zeta^y \left(1 + \omega + \omega^2 + \dots + \omega^{m-1}\right) = \omega^x \zeta^y \frac{\omega^m - 1}{\omega - 1} = 0.$$

Since the entire rectangle is tiled by such strips, the sum of all numbers over the rectangle must be 0. On the other hand, if we sum the numbers over the entire rectangle by rows and columns, we obtain:

$$\left(\omega + \omega^2 + \dots + \omega^a\right)\left(\zeta + \zeta^2 + \dots + \zeta^b\right) = \omega \frac{\omega^a - 1}{\omega - 1} \cdot \zeta \frac{\zeta^b - 1}{\zeta - 1}.$$

This implies either $\omega^a = 1$ or $\zeta^b = 1$, which in turn imply $m | a$ or $n | b$, since $\omega$ and $\zeta$ are primitive roots of unity. □

## References

[1] Olimpiadi della Matematica. *Gara a Squadre*. URL: https://olimpiadi.dm.unibo.it/le-gare/gara-a-squadre/.

[2] Sandro Campigotto. *Progetto PhiQuadro*. URL: https://www.phiquadro.it/.

[3] Evan Chen. *Euclidean Geometry in Mathematical Olympiads (EGMO)*. 2016. URL: https://olympiads.org/egmo.

[4] Olimpiadi della Matematica. *Il Senior in Pillole*. URL: https://olimpiadi.dm.unibo.it/il-senior-in-pillole/.

[5] Wikipedia contributors. *Napoleon's Theorem*. 2025. URL: https://en.wikipedia.org/wiki/Napoleon%27s_theorem.

[6] Arthur Engel. *Problem-Solving Strategies*. 1997. URL: https://mathematicalolympiads.wordpress.com/wp-content/uploads/2012/08/75427434-problem-books-in-mathematics-problem-solving-strategies.pdf.

[7] Wikipedia contributors. *Cardano's Formula*. 2025. URL: https://en.wikipedia.org/wiki/Cubic_equation%5C#Cardano's_formula.

[8] Titu Andreescu and Zuming Feng. *102 Combinatorial Problems: From the Training of the USA IMO Team*. 2003. URL: https://rainymathboy.wordpress.com/wp-content/uploads/2011/01/102-combinatorial-problems.pdf.