Complex Numbers as a Universal Tool in Olympiad Mathematics

Alexandru Bordei[†] and Marius Cerlat[†]

[†]"Orizont" Durlești Theoretical Lyceum

Abstract

This article explores the various applications of complex numbers across all mathematics olympiad domains, beginning with Geometry and then proceeding to Algebra, Combinatorics, and Number Theory. Complex numbers often provide elegant solutions to rather complicated mathematical setups, whether they were invoked in the statement or not. Through illustrative examples, we demonstrate how the complex plane offers both geometric intuition and algebraic efficiency. We aim to present a unified perspective on the role of complex numbers in olympiad mathematics, emphasizing connections among different mathematical domains.

Contents

0 Definitions

- Let $\mathbb{R}$ refer to the set of all real numbers.
- Let $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ refer to the set of all complex numbers.
- For any $z \in \mathbb{C}$, $z = a + ib$, where $a, b \in \mathbb{R}$ and i is the imaginary unit, such that $i^2 = -1$.
- The real part of $z = a + ib$ is $Re(z) = a$, and the imaginary part $Im(z) = b$.
- Addition of complex numbers: $z_1 + z_2 = (a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)$.
- Multiplication of complex numbers: $z_1 \cdot z_2 = (a_1 + ib_1)(a_2 + ib_2) = a_1a_2 - b_1b_2 + i(a_1b_2 + a_2b_1)$.
- The absolute value (module) of z is $|z| = \sqrt{a^2 + b^2}$, from the Pythagorean Theorem.
- If $z = a + ib$ then the conjugate of z: $\overline{z} = a - ib$. Property of the conjugate: $\overline{\Sigma\, z_i} = \Sigma\, \overline{z}_i$ and $\overline{\Pi\, z_i} = \Pi\, \overline{z}_i$. The proof is intuitive, because $\overline{z}$ is the mirror image of z over the real axis.
- $|z|^2 = z \cdot \overline{z} = (a + ib)(a - ib) = a^2 - (ib)^2 = a^2 + b^2$.
- $z = |z|e^{i\theta}$, where θ is the argument of z, i.e. the angle between OZ and the real axis.
- Euler's formula: $e^{i\theta} = \cos\theta + i\sin\theta$.

Furthermore, while solving problems, we will avoid using the $a + ib$ notation, and instead work only in terms of z, $\overline{z}$, and $|z|$, except for rarely invoking $\Re(z)$ or $\Im(z)$, the real and the imaginary parts, respectively, of z.

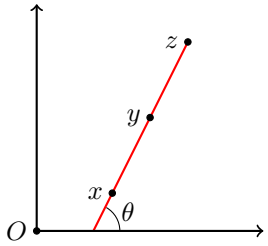
1 Complex Numbers in Geometry

Unless specified otherwise, lowercase letters (e.g., x, a) will refer to the complex numbers assigned to geometric points, i.e., the uppercase letters(X, A).

1.1 Basic Properties

Midpoint of two points: The midpoint of x and y is $\frac{x+y}{2}$, proven by invoking $a+bi$.
Collinearity Condition: Three points, x, y, and z, are collinear if and only if:

$$\frac{y-x}{z-x} \in \mathbb{R}$$

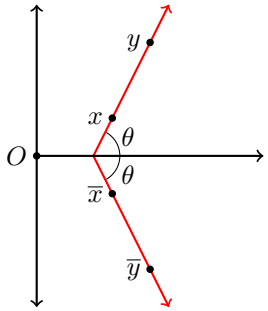


Two complex numbers have a real ratio if they are collinear with the origin ($\frac{x}{y} = \frac{|x|}{|y|} \cdot \frac{e^{i\theta_1}}{e^{i\theta_2}}$). The previous is explained by putting x as the origin. Then $y-x$ and $z-x$ are collinear with the origin if and only if their ratio is a real number.

We also know that $z \in \mathbb{R} \iff z = \overline{z}$ ($\Im(z) = 0$). This rewrites the collinearity condition as:

$$\frac{y-x}{\overline{y}-\overline{x}} = \frac{z-x}{\overline{z}-\overline{x}}$$

Complex slope of a line: The complex slope of a line is defined by $\frac{y-x}{\overline{y}-\overline{x}}$. This slope is equal to $e^{2i\theta}$, where θ is the angle between the real axis and the line.



It is derived from: $\frac{y-x}{\overline{y}-\overline{x}} = \frac{|y-x|e^{i\theta}}{|y-x|e^{i(-\theta)}} = e^{2i\theta}$, so it is actually equal to the square of the argument. The advantage of the complex slope is that we *avoid* taking moduli to find the argument when showing that two lines are parallel, or other angle conditions.

Having established the conditions for collinearity and parallelism (equality of the complex slopes), let us prove the following:

Perpendicularity of two lines: XY and ZT are perpendicular if and only if:

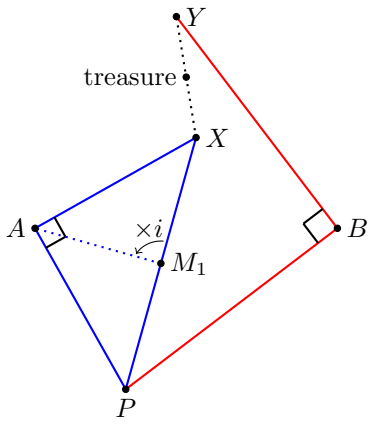
$$\frac{x-y}{\overline{x}-\overline{y}} = -\frac{z-t}{\overline{z}-\overline{t}}$$

We can rewrite this as $e^{2i\alpha} = -e^{2i\beta} \iff \cos 2\alpha + i\sin 2\alpha + \cos 2\beta + i\sin 2\beta = 0 \iff \cos 2\alpha = -\cos 2\beta$ and $\sin 2\alpha = -\sin 2\beta$. Clearly $2\alpha = 2\beta \pm \pi \iff \alpha = \beta \pm \pi/2$.

Addition and multiplication of complex slopes: Because of the form $e^{2i\theta}$ it is clear that for addition we multiply the expressions: $e^{2i\alpha} \cdot e^{2i\beta} = e^{2i(\alpha+\beta)}$, the complex slope of $k \cdot \theta$ is the complex slope of θ to the power of k. The angle between two lines is the ratio of the complex slopes, which we will refer to as **complex angle**, and the ratio must always be taken in the counterclockwise direction. That is because (multiplication by) i represents a **counterclockwise** $90°$ **rotation**. The following example problem puts this to use.

Example Problem 0.
A pirate found a treasure map on an island. The map says that on the island, there are 2 palm trees and one plank. It's said to go from the plank to the first palm tree, to rotate 90° to the right, walk the same distance again, and mark the first point. Then go from the plank to the second palm tree, rotate 90° to the left, walk the same distance again, and mark the second point. The treasure is buried at the midpoint of the two marked points. The pirate arrives, and the plank is missing. With the palm trees only, can he find the treasure?

Solution:



Let P represent the plank, and A and B represent the first and second palm trees, respectively. X and Y are the two marked points.
We notice that PAX is a right-angled isosceles triangle. Let M_1 be the midpoint of PX. Then we know geometrically that $AM_1 \perp PX$ and that $|AM_1| = \frac{|XP|}{2}$. Now let's express this in complex numbers. We have $m_1 = \frac{p+x}{2}$. But how do we get to a? We can avoid complex slopes and arguments

altogether, using that $a - m_1 = i \cdot (x - m_1) \iff a - m_1 = i\frac{x-p}{2}$. Thus $a = \frac{p+x}{2} + i\frac{x-p}{2}$. When doing the same for the triangle PYB, one can check that $b - m_2$ is obtained by rotating *clockwise*, so instead we multiply by $-i$. So $b = \frac{p+y}{2} - i\frac{y-p}{2}$. Now we calculate $\frac{x}{2} + \frac{y}{2}$:

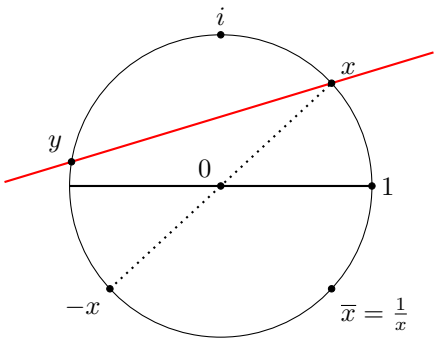
$$\frac{x}{2} = \frac{a + \frac{p}{2}(i-1)}{i+1} \qquad \frac{y}{2} = \frac{b - \frac{p}{2}(i+1)}{1-i}$$

$$\frac{x+y}{2} = \frac{a(1-i) - \frac{p}{2}(1-i)^2 + b(i+1) - \frac{p}{2}(i+1)^2}{(1+i)(1-i)} = \frac{a(1-i) + b(1+i)}{2}$$

So the endpoint *does not* depend on the position of the plank. The pirate can find the treasure starting from any point. Notice that the final equation ($\frac{a+b+i(b-a)}{2}$) is familiar, and we can, in fact, check with the diagram that the treasure also forms a right-angled isosceles triangle with A and B.

1.2 The Unit Circle

Complex numbers work best when the problem has a single circle that gets most of the attention. In this case, any geometry setup can be scaled so that this specific circle has its center in the origin and a radius of 1.



The benefit of this setup is that $\overline{x} = \frac{|x|^2}{x} = \frac{1}{x}$ for any x on the circle. This way, all the equations become more manageable.

Line on unit circle: Any Z on the line XY, where X and Y are points on the unit circle satisfies the equation:

$$\frac{z-x}{\overline{z}-\overline{x}} = \frac{x-y}{\overline{x}-\overline{y}} = \frac{x-y}{\frac{1}{x}-\frac{1}{y}} = -xy$$

$$z + xy\overline{z} = x + y$$

Equation of tangent: The equation for points Z on the tangent to the unit circle from X, $|x| = 1$:

$$z + x^2\overline{z} = 2x$$

One can do this by taking $\frac{z-x}{\overline{z}-\overline{x}} = -\frac{x-0}{\overline{x}-0} = -x^2$, but it's easier to remember this as a degenerate case of the previous equation, where both points are X.

Intersection of two tangents: The intersection Z of two tangents to the unit circle at points $|x| = |y| = 1$:

$$z = \frac{2xy}{x+y}$$

This is proven by directly invoking the previous formula.

Foot of altitude: The foot of Z on line XY, where X and Y are on the unit circle has the equation:

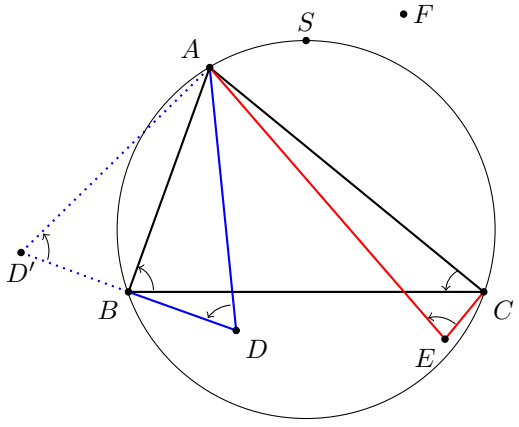
$$z' = \frac{1}{2}(x + y + z - xy\overline{z})$$

We prove this through the equation of the line: $z' + xy\overline{z'} = x + y$, and the perpendicularity equation: $z - z' = xy(\overline{z - z'})$. Subtracting these two, we arrive at our formula. Using this, find the reflection of Z over the line XY.

Example Problem 1. *CAPS 2025*
Let ABC be an acute triangle. Point D lies in the halfplane AB containing point C such that $DB \perp AB$ and $\angle ADB + 45^\circ + \frac{1}{2}\angle ACB$. Similarly, E lies in the halfplane AC containing point B such that $AC \perp EC$ and $\angle AEC = 45^\circ + \frac{1}{2}\angle ABC$. Let F be the reflection of A in the midpoint of the arc BC containing A. Prove that points A, D, E, F are concyclic.

Solution:

First, let's find the midpoint of arc BAC, let it be S. We know that $|s| = 1$ and that it lies on the perpendicular bisector of BC. Because this bisector passes through 0, its equation is: $\frac{x}{\overline{x}} = -\frac{b-c}{\frac{1}{b}-\frac{1}{c}} = bc$. So $s^2 = bc$. We will define x, y, z such that $a = x^2$, $b = y^2$, and $c = z^2$, and, simultaneously, the midpoint of the arc BC that *does not* contain A has equation $-yz$, the midpoint of the arc AC that does not contain B has equation $-xy$, and the midpoint of the arc AB that does contain C has equation $-xz$. The existence of (x, y, z) can be demonstrated but it is outside the scope of this handout. This is also mentioned in the next section. Then $s = yz$.



Let's write up the angle conditions in complex numbers. $DB \perp AB$ translates to $\frac{d-b}{\overline{d}-\overline{b}} = ab$. Now we have to interpret $\angle ADB + 45^\circ + \frac{1}{2}\angle ACB$ in terms of complex slopes. Note that there are two points for which this angle condition stands, separated by line AB, thus we have the halplane

condition. But this time, we do not need to worry about obtaining a quadratic equation, because the orientation of the angles takes care of the second point. Check the diagram to see that for the second point, D', $\angle BD'A$ has the complex angle the inverse of the complex angle of $\angle ADB$. So the "counterclockwise" condition of angles in complex numbers is of great help here. We rewrite the condition:

$$e^{2i\angle ADB} = e^{2i\cdot 45^\circ} \cdot e^{\frac{2i\angle ACB}{2}}$$

And $e^{2i\cdot 45^\circ} = e^{i\pi/2} = \cos\pi/2 + i\sin\pi/2 = i$. We need to express half of $\angle ACB$. We cannot do that from its complex angle, since the square root isn't a single-valued function in complex numbers. So we set P as the midpoint of the arc AB, not containing C, $p = -xy$, and express the complex angle of $\angle ACP = \frac{\angle ACB}{2}$. That is $\frac{-x^2\cdot z^2}{xy\cdot z^2} = -\frac{x}{y}$.

$$(\frac{d-a}{\overline{d}-\overline{a}}\cdot\frac{\overline{d}-\overline{b}}{d-b}) = i\cdot\left(-\frac{x}{y}\right)$$

$$\frac{d-x^2}{(xy)^2(\overline{d}-\overline{a})} = -i\frac{x}{y}$$

Inputting $\overline{d}$ from the perpendicularity condition:

$$\frac{d-x^2}{d+x^2-2y^2} = -i\frac{x}{y}$$

$$d = \frac{x(-ix^2+2iy^2+xy)}{y+ix}$$

Because e is defined like d on AC, one might be tempted to change $y \to z$ and find e by symmetry. But our diagram highlights that by just changing $y \to z$, we ignore that the orientation of $\angle AEC$ is now clockwise. It is an option to find e again from scratch, but we can still find it by symmetry if we redefine all default rotations to be clockwise by changing $i \to -i$. So:

$$e = \frac{x(ix^2-2iz^2+xz)}{z-ix}$$

Since $s = \frac{a+f}{2}$:

$$f = 2yz - x^2$$

Concyclicity condition: Let u, v, w and t be points in the complex plane. Then they are concylic if and only if:

$$\frac{u-v}{u-w}\cdot\frac{t-w}{t-v} \in \mathbb{R}$$

There are two angle conditions that yield concyclicity. If $\angle VUW$ and $\angle VTW$ are similarly oriented, then $\angle VUW = \angle VTW \iff U,T,W,V$-concyclic. If they are not similarly oriented, $\angle VUW + \angle VTW = 180^\circ \iff U,V,T,W-$concyclic. Both cases lead to the above equation.

Therefore, we need to prove that $\frac{(x^2-d)(f-e)}{(x^2-e)(f-d)} \in \mathbb{R}$. Inputting the values:

$$\frac{(x^2 - \frac{x(-ix^2+2iy^2+xy)}{y+ix})(2yz - x^2 - \frac{x(ix^2-2iz^2+xz)}{z-ix})}{(2yz - x^2 - \frac{x(-ix^2+2iy^2+xy)}{y+ix})(x^2 - \frac{x(ix^2-2iz^2+xz)}{z-ix})} \in \mathbb{R}$$

$$\frac{(2ix^3 - 2ixy^2)(2yz^2 - 2ixyz - 2x^2z + 2ixz^2)}{(2y^2z + 2ixyz - 2x^2y - 2ixy^2)(-2ix^3 + 2ixz^2)} \in \mathbb{R}$$

$$\frac{2ix(x^2 - y^2) \cdot z(2yz - 2ixy - 2x^2 + 2ixz)}{y(2yz - 2ixy - 2x^2 + 2ixz) \cdot 2ix(z^2 - x^2)} \in \mathbb{R}$$

$$\frac{z(x^2 - y^2)}{y(z^2 - x^2)} \in \mathbb{R}$$

Which is true since $|x| = |y| = |z| = 1$.

1.3 Applications of the Unit Circle

- The first one is quite straightforward: setting the **circumcenter** of the triangle ABC as the unit circle, $|a| = |b| = |c| = 1$. We further provide the formulas for the centers of the triangle:
  Centroid: It is intuitive: $g = \frac{a+b+c}{3}$. However, we can verify it. We know that $a, g, \frac{b+c}{2}$ are collinear for every permutation. So $a - g = \frac{2a-b-c}{3}$ and $a - \frac{b+c}{2} = \frac{2a-b-c}{2}$. Therefore, it's clear that they have the same complex slope.
  Orthocenter: We know that $AH \perp BC$, for every permutation. That means:

$$\frac{a-h}{\frac{1}{a} - \overline{h}} = bc \iff h - bc\overline{h} = a - \frac{bc}{a}$$

  We can check that the following expression fulfills every condition.

$$h = a + b + c$$

  The circumcenter is 0, of course, and we will return shortly about the incenter.

- The second option is to define the **incircle** as the unit circle. In this case we define D, E, F the contact points of the incircle with BC, AC and AB respectively.
  The vertices of the triangle: A is the intersection of tangents from E and F to the unit circle. We do have a formula for that, so we can find $a = \frac{2ef}{e+f}$, and the cyclic permutations: $b = \frac{2fd}{f+d}$, $c = \frac{2ed}{e+d}$.

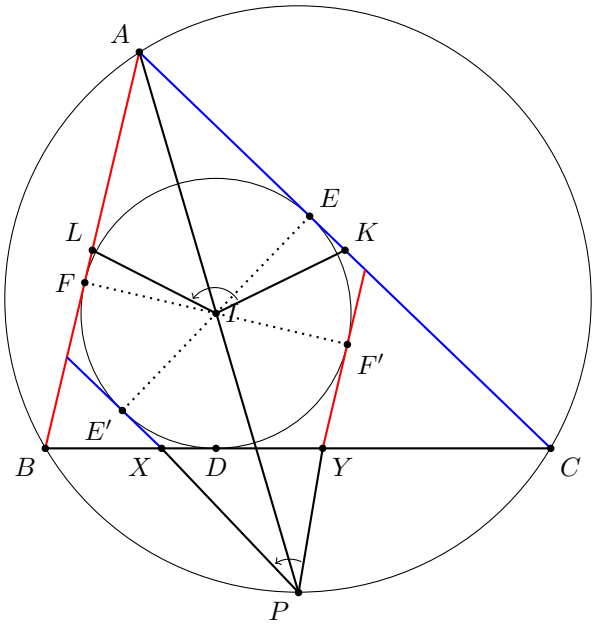
  We will use this setup only when the problem is primarily focused on the incircle, angle bisectors, etc. But we can still work around other centers (e.g., the circumcenter is $\frac{2def(d+e+f)}{(d+e)(e+f)(f+d)}$), though we will not bother to calculate them now. See Example Problem 2.

- What if you need to have the circumcenter as the unit circle, but also need the incenter? We have already seen this method in Example Problem 1. Let $a = x^2$, $b = y^2$ and $c = z^2$.
  Root choice: There *exists* a choice of x, y, z such that the midpoint of arc BC not containing A has equation $-yz$ and so on. Then the incenter is $-xy-xz-yz$ (the incenter of the triangle is the orthocenter of the arc midpoints). See Example Problem 3.

- There are also other non-traditional options such as setting the unit circle as the Nine Point Circle, or any other untraditional circle, if even set any at all.

Example Problem 2. *IMO 2024 P4*
Let ABC be a triangle with $AB < AC < BC$. Let the incenter and incircle of ABC be I and ω, respectively. Let X be the point on line BC different from C such that the line through X parallel to AC is tangent to ω. Similarly, let Y be the point on line BC different from B such that the line through Y parallel to AB is tangent to ω. Let AI intersect the circumcircle of triangle ABC at $P \neq A$. Let K and L be the midpoints of AC and AB.
Prove that $\angle KIL + \angle YPX = 180^\circ$

Solution:



Considering all the work around the incircle, we are motivated to set it as the unit circle, so let $|d| = |e| = |f| = 1$ be the tangency points of ω on BC, AC, and AB, respectively. We have already found the formulas for a, b, c.
We further notice that two tangents to a circle are parallel if and only if their points of tangency are diametrically opposed. This is clear since the tangent at e has the complex slope $-e^2$ and so does the tangent at $-e$ - i.e., the reflection over the center of the circle. So we conclude that x is

the intersection of the tangents from d and $-e$ to the incircle $\iff x = \frac{-2de}{d-e}$, and the same for y: $y = \frac{-2df}{d-f}$.
We know that the A-bisector intersects the circumcircle at the midpoint of arc BC, so P also lies on the perpendicular bisector of BC. Because $BC \perp ID$, the complex slope of BC is $-d^2$. So:

$$\frac{p - \frac{b+c}{2}}{\overline{p} - \overline{\frac{b+c}{2}}} = d^2$$

$$p - \frac{de}{d+e} - \frac{df}{d+f} = d^2\overline{p} - \frac{d^2}{d+e} - \frac{d^2}{d+f}$$

$$p - d^2\overline{p} = d(\frac{e-d}{d+e} + \frac{f-d}{d+f})$$

$$p - d^2\overline{p} = \frac{2d(ef-d^2)}{(d+e)(d+f)}$$

And from the first condition we get that $\frac{p}{\overline{p}} = \frac{a}{\overline{a}} = ef$. Then:

$$p\frac{(ef-d^2)}{ef} = \frac{2d(ef-d^2)}{(d+e)(d+f)} \iff p = \frac{2def}{(d+e)(d+f)}$$

The remaining points are the midpoints of the sides, which are easy to find. We obtain $k = \frac{ef}{e+f} + \frac{de}{d+e}$ and $l = \frac{ef}{e+f} + \frac{df}{d+f}$. We need to prove that $e^{2i\angle KIL} \cdot e^{2i\angle YPX} = e^{2i\pi} = 1$. So we need to show that the complex angle of $\angle KIL$ is the inverse of the complex angle $\angle YPX$. Let us calculate the first one.

$$\frac{k-0}{\overline{k}-0} \cdot \frac{\overline{l}-0}{l-0} = \frac{\frac{ef}{e+f} + \frac{de}{d+e}}{\frac{1}{e+f} + \frac{1}{d+e}} \cdot \frac{\frac{1}{e+f} + \frac{1}{d+f}}{\frac{ef}{e+f} + \frac{df}{d+f}} = \boxed{\frac{e(f(d+e)+d(e+f))(2f+d+e)}{f(2e+d+f)(e(d+f)+d(e+f))}}$$

We will leave this here, and look how the complex angle of $\angle YPX$ looks:

$$\frac{y-p}{\overline{y}-\overline{p}} = \frac{-\frac{2df}{d-f} - \frac{2def}{(d+e)(d+f)}}{-\frac{2}{f-d} - \frac{2d}{(d+e)(d+f)}} = \frac{df((d+e)(d+f)+e(d-f))}{(d+e)(d+f)+fd-d^2}$$

$$\frac{y-p}{\overline{y}-\overline{p}} = \frac{df(d^2+2ed+fd)}{2fd+ed+ef} = \frac{d^2f(2e+d+f)}{2fd+ed+ef}$$

We change e with f to find $\frac{x-p}{\overline{x}-\overline{p}}$:

$$\frac{x-p}{\overline{x}-\overline{p}} = \frac{d^2e(2f+d+e)}{2ed+fd+ef}$$

So:

$$\frac{y-p}{\overline{y}-\overline{p}} \cdot \frac{\overline{x}-\overline{p}}{x-p} = \boxed{\frac{f(2e+d+f)(2ed+fd+ef)}{e(2f+d+e)(2fd+ed+ef)}}$$

We can check that the two boxed expressions are indeed the inverse of each other. A remark for this problem: we actually proved that the sum of the angles is a multiple of π, as for any k, since

$e^{2ik\pi} = 1$. This always happens because complex angles are equivalent $\mod(\pi)$. In this case, we can prove that the sum of the angles is $< 2\pi$.

X and Y must be points inside the circumcircle and P is a point on it, so $\angle YPX < \pi$. We can also prove that $\angle KIL < \pi$ by showing that the incenter is constrained inside the midpoint triangle. We prove that I is on the same side of KL as BC(which are parallel) by showing that $r < \frac{AA'}{2}$, where r is the incenter radius and AA' is the A-altitude. $S = \frac{AB \cdot BC \sin B}{2}$ is the area of ABC.

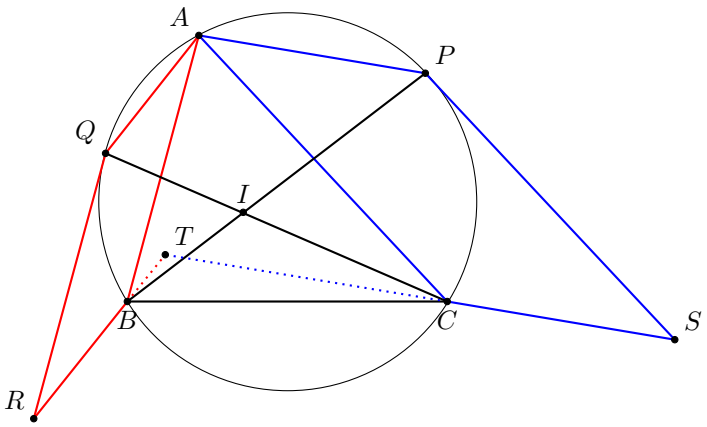
$$r = \frac{2 \cdot S}{AB + BC + AC} < \frac{AB \sin B}{2} \iff 4S < AB \sin B(AB + BC + AC)$$

$$2S < \frac{AB \cdot BC \sin B}{2} + \frac{AB \cdot (AB + AC) \sin B}{2}$$

Which is true from the inequality of the triangle: $AB + AC > BC$. So $\angle KIL + \angle YPX < 2\pi$.

Example Problem 3. *EGMO 2025 P4*
Let ABC be an acute triangle with incentre I and $AB \neq AC$. Let lines BI and CI intersect the circumcircle of ABC at $P \neq B$ and $Q \neq C$, respectively. Consider points R and S such that $AQRB$ and $ACSP$ are parallelograms (with $AQ \parallel RB, AB \parallel QR, AC \parallel SP$, and $AP \parallel CS$). Let T be the point of intersection of lines RB and SC. Prove that points R, S, T, and I are concyclic.

Solution:



Let $a = x^2, b = y^2$ and $c = z^2$ with $|x| = |y| = |z| = 1$, such that the incenter, let it be v has equation $v = -(xy + yz + zx)$. Then $p = -xz$ and $q = -xy$. Now we need to be smart about the parallelogram condition. One property of a parallelogram is that its diagonals bisect each other, so $AQRB$ is a parallelogram if and only if $\frac{a+r}{2} = \frac{q+b}{2} \iff r = q + b - a \iff r = y^2 - x^2 - xy$. Similarly, $s = p + c - a \iff s = z^2 - x^2 - xz$. We are left with the algebra of finding t and checking the concyclicity condition. From T, B, R collinear:

$$\frac{y^2 - t}{\overline{y}^2 - \overline{t}} = \frac{y^2 - r}{\overline{y}^2 - \overline{r}} = \frac{x(x+y)}{\frac{x+y}{x^2 y}} = x^3 y$$

$$y^2 - t = \frac{x^3}{y} - x^3 y\bar{t} \iff t - x^3 y\bar{t} = y^2 - \frac{x^3}{y}$$

And for the same condition with T, C, S collinear, we will change $y \to z$:

$$t - x^3 z\bar{t} = z^2 - \frac{x^3}{z}$$

$$x^3\bar{t}(z-y) = y^2 - z^2 + \frac{x^3}{z} - \frac{x^3}{y}$$

$$\bar{t} = -\frac{y+z}{x^3} - \frac{1}{yz} = -\frac{yz(y+z)+x^3}{x^3 yz}$$

$$t = -\frac{x^3(y+z)+y^2z^2}{yz}$$

Finally, we need to show that r, s, t, v are concyclic. This rewrites as:

$$\frac{(r-t)(s-v)}{(s-t)(r-v)} \in \mathbb{R}$$

$$\frac{(y^2 - x^2 - xy + \frac{x^3}{yz}(y+z) + yz)(z^2 - x^2 - xz + xy + xz + yz)}{(z^2 - x^2 - xz + \frac{x^3}{yz}(y+z) + yz)(y^2 - x^2 - xy + xy + xz + yz)} \in \mathbb{R}$$

$$\frac{(y^2 - x^2 - xy + \frac{x^3}{yz}(y+z) + yz)(x+z)(-x+y+z)}{(z^2 - x^2 - xz + \frac{x^3}{yz}(y+z) + yz)(x+y)(-x+y+z)} \in \mathbb{R}$$

We can cancel out $y + z - x$ because $y + z - x = 0 \iff |y+z| = 1 \iff 2 + \frac{y}{z} + \frac{z}{y} = 1 \iff y^2 + z^2 + yz = 0 \iff a = x^2 = (y+z)^2 = yz$, meaning that $AB = AC$, which contradicts the condition. So our final expression is:

$$\frac{(y^3z - x^2yz - xy^2z + x^3(y+z) + y^2z^2)(x+z)}{(yz^3 - x^2yz - xyz^2 + x^3(y+z) + y^2z^2)(x+y)} \in \mathbb{R}$$

Since this expression doesn't reduce to anything simpler, to prove it is real we have to conjugate straight away:

$$\frac{(\frac{1}{y^3z} - \frac{1}{x^2yz} - \frac{1}{xy^2z} + \frac{(y+z)}{x^3yz} + \frac{1}{y^2z^2})\frac{(x+z)}{xz}}{(\frac{1}{yz^3} - \frac{1}{x^2yz} - \frac{1}{xyz^2} + \frac{(y+z)}{x^3yz} + \frac{1}{y^2z^2})\frac{(x+y)}{xy}} = \frac{(x^3z - xy^2z - x^2yz + y^2z(y+z) + x^3y)(x+z)}{(x^3y - xyz^2 - x^2yz + yz^2(y+z) + x^3z)(x+y)}$$

Which is equal to the initial expression, thus making it real.

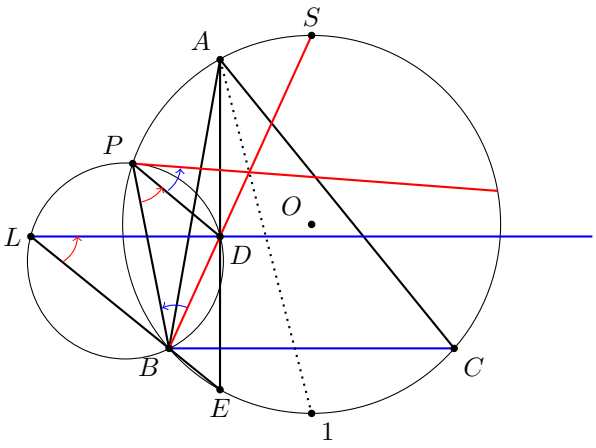
1.4 Rotations of the Complex Plane

Until now, problems have gone the usual way: choose the most important circle, scale, and move the diagram such that this circle is the unit circle in the complex plane. But can we make use of more aspects? What if we also rotate the diagram so that, let's say, the vertices of the triangle become a, b and 1 (don't!). This, in particular, is not at all helpful because the only thing it does is to get

rid of symmetry and homogeneity. But when we don't need these two, making such a movement can be a lot of help (not such a blunt choice as $c = 1$). For example, if your setup includes an extra randomly chosen point outside the unit circle, one can rotate the diagram until that point sits on the real axis, so it's a real number. This way, taking conjugates will be way easier. We have chosen 2 example problems to demonstrate this kind of use.

Example Problem 4. *IMO 2023 P2*
Let ABC be an acute-angled triangle with $AB < AC$. Let Ω be the circumcircle of ABC. Let S be the midpoint of the arc CB of Ω containing A. The perpendicular from A to BC meets BS at D and meets Ω again at $E \neq A$. The line through D parallel to BC meets line BE at L. Denote the circumcircle of triangle BDL by ω. Let ω meet Ω again at $P \neq B$. Prove that the line tangent to ω at P meets line BS on the internal angle bisector of $\angle BAC$.

Solution: It's clear that we need to set the circumcircle of ABC as the unit circle. But we also need the midpoint of the arc CB (containing A) and the angle bisector of $\angle BAC$ in the end, which is the line formed by point A and the other midpoint of the arc CB- not containing A.
But here we don't need to consider x, y, z as roots of the triangle vertices. Observe that the problem isn't symmetric in b, c, and we only need to work with the midpoints of the arc BC. So here we get the natural idea to set the midpoints of arc BC as 1 and -1. Now c will be the reflection of b over the real axis, so $c = \overline{b} = \frac{1}{b}$.



So let $|a| = |b| = 1$ and $a, b, \frac{1}{b}$ be the vertices of the triangle. We chose a such that $s = -1$. Now we find d, from $AD \perp BC$ and B, S, D collinear:

$$\frac{a-d}{\overline{a}-\overline{d}} = 1 \iff a - d = \frac{1}{a} - \overline{d}$$

$$d - b\overline{d} = b - 1$$

$$a - b\overline{d} = \frac{1}{a} - \overline{d} + b - 1 \iff \overline{d} = \frac{\frac{1}{a} - a + b - 1}{1 - b}$$

$$d = \frac{b(a^2-1) + a(1-b)}{a(b-1)}$$

And we can find e knowing that $|e| = 1$ and $AE \perp BC$:

$$ae = -1 \iff e = -\frac{1}{a}$$

Next, we will avoid calculating L by finding the tangent at P of circle ω through congruences of angles. From P, D, B, L-cyclic, we have $\angle BLD = \angle BPD$. We know that the complex slope of line LD, which is parallel to BC, is -1, and since E, B, L are collinear, the complex slope of LB is equal to $-be = \frac{b}{a}$. So now we can find p:

$$\frac{p-b}{\overline{p}-\overline{b}} \cdot \frac{\overline{p}-\overline{d}}{p-d} = \frac{-be}{-1} = -\frac{b}{a} \iff \frac{\overline{p}-\overline{d}}{p-d} = \frac{1}{ap}$$

$$a - ap\overline{d} = p - d$$

$$p = \frac{d+a}{1+a\overline{d}} = \frac{a^2b - b + a - ab + a^2b - a^2}{a(b-1)} \cdot \frac{b-1}{a^2 - 1 + a - ab + b - 1}$$

$$p = \frac{a^2b - b + a - ab + a^2b - a^2}{a(a^2 - 1 + a - ab + b - 1)} = \frac{b(a^2-1) + a - a^2 + ab(a-1)}{a(a^2 - 1 + a - 1 + b(1-a))}$$

$$p = \frac{2ab - a + b}{a(a - b + 2)}$$

Now, let's firstly define the second intersection of the tangent at P to ω with Ω as X. We know that $\angle DPX = \angle DBP$ so, in complex slopes:

$$\frac{d-p}{\overline{d}-\overline{p}} \cdot \frac{\overline{x}-\overline{p}}{x-p} = \frac{d-b}{\overline{d}-\overline{b}} \cdot \frac{\overline{p}-\overline{b}}{p-b}$$

Since B, D, S are collinear, $\frac{d-p}{\overline{d}-\overline{p}} = ap$ and the rest are chords of the unit circle:

$$\frac{ap}{-px} = \frac{b}{-pb} \iff x = ap$$

We need to prove that PX, BS, and the A-bisector concur in the same point. Because our expressions are quite large, usually the best approach is to show that the intersection between two lines is the same as the intersections of the other two. All these points are on the unit circle, so by the formula of the intersections of two chords, we need to show that:

$$\frac{p + x - b + 1}{px + b} = \frac{b - 1 - a - 1}{-b - a} = \overline{t}$$

Where t is the intersection point. Next, we will need to expand the equations.

$$(a+b)(p + ap - b + 1) = (ap^2 + b)(a - b + 2)$$

$$(a+b)\frac{(a+1)(2ab - a + b) + (1-b)a(a-b+2)}{a(a-b+2)} = (a-b+2)\frac{a(2ab-a+b)^2 + a^2b(a-b+2)^2}{a^2(a-b+2)^2}$$

$$a(a+b)\cdot((a+1)(2ab-a+b)+(1-b)a(a-b+2))=a\cdot((2ab-a+b)^2+ab(a-b+2)^2)$$

$$(a+b)(a+1)(2ab-a+b)+(a+b)(a-b+2)(1-b)a=(2ab-a+b)^2+ab(a-b+2)^2$$

$$(2ab-a+b)\cdot((a+b)(a+1)-2ab+a-b)=(a-b+2)\cdot(ab(a-b+2)-(a+b)(1-b)a)$$

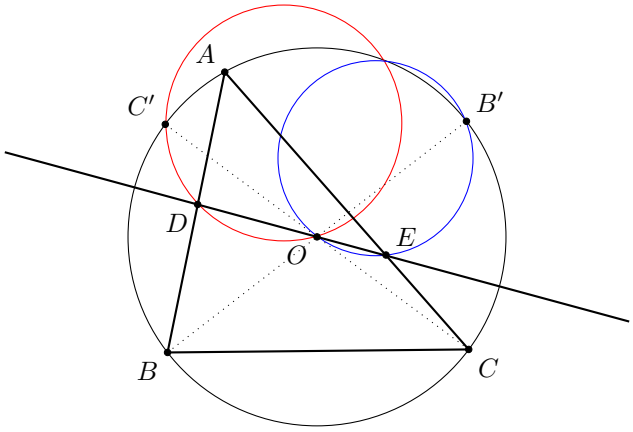
$$(2ab-a+b)(a^2-ab+2a)=(a-b+2)(2a^2b+ab-a^2)$$

$$(2ab-a+b)(a-b+2)=(a-b+2)(2ab-a+b)$$

Hence, we have proved that PX and BS meet on the A-bisector.

Example Problem 5. *Nordic 2022*
Let ABC be an acute-angled triangle with circumscribed circle k and centre of the circumscribed circle O. A line through O intersects the sides AB and AC at D and E.Denote by B' and C' the reflections of B and C over O, respectively. Prove that the circumscribed circles of ODC' and OEB' concur on k.

Solution:



We observe that we can avoid adding a variable, i.e., the intersection of the line with the unit circle, by rotating the complex plane such that the line is the real axis, which is possible since it passes through 0. Clearly, ABC must be the unit circle, so:
Let $|a|=|b|=|c|=1$ and the line that passes through O be the real axis. Since $d=\overline{d}$:

$$d+ab\cdot d=a+b\iff d=\frac{a+b}{ab+1}$$

We can find e by symmetry, but we don't need it. We can solve the problem by proving that x - the intersection of (ODC') and k is symmetric in b and c:

$$\frac{x-0}{x+c}\cdot\frac{d+c}{d-0}\in R$$

$$\frac{x}{x+c}\cdot\frac{\frac{a+b+c+abc}{ab+1}}{\frac{a+b}{ab+1}}\in R\iff\frac{x}{x+c}\cdot\frac{a+b+c+abc}{a+b}=\frac{\frac{1}{x}xc}{x+c}\cdot\frac{(ab+bc+ac+1)ab}{(a+b)abc}$$

$$x = \frac{ab + bc + ac + 1}{a + b + c + abc}$$

Which is indeed symmetric in b, c, hence (ODC') and (OEB') intersect on the same point on k.

1.5 Applications of Viète's relations

Sometimes, the conditions of the problem give complicated equations that are tedious to resolve straight away. In these cases, if a polynomial appears, we can work with Viète's relations. For example, if $X \neq B, C$ and both B, C satisfy the condition, the polynomial that describes x might have 3 solutions, X, B, C, hence x can be found just by looking at the x^0 term.
We have prepared the following problem, the last geometry in this article, to showcase a beautiful application of Viète's relations to avoid a long calculation.

Example Problem 6. *USA TSTST 2023 P6*
Let ABC be a scalene triangle and let P and Q be two distinct points in its interior. Suppose that the angle bisectors of $\angle PAQ$, $\angle PBQ$, and $\angle PCQ$ are the altitudes of triangle ABC. Prove that the midpoint of $\overline{PQ}$ lies on the Euler line of ABC.
(The Euler line is the line through the circumcenter and orthocenter of a triangle.)

Solution: We will work with ABC as the unit circle, so $|a| = |b| = |c| = 1$ and $h = a + b + c$. Let's transform the angle conditions through complex slopes, starting with the bisector of $\angle PAQ$:

$$\frac{a-h}{\overline{a}-\overline{h}} \cdot \frac{\overline{a}-\overline{p}}{a-p} = \frac{a-q}{\overline{a}-\overline{q}} \cdot \frac{\overline{a}-\overline{h}}{a-h}$$

And since $a - h = -(b + c)$, we simplify to:

$$b^2c^2(\overline{a}-\overline{p})(\overline{a}-\overline{q}) = (a-p)(a-q)$$

Considering $\overline{a} = \frac{1}{a}$, we obtain the following polynomial, from which we can find the other conditions by permutation, from symmetry:

$$a^4(a-p)(a-q) - a^2b^2c^2(\overline{p}a-1)(\overline{q}a-1) = 0$$

$$b^4(b-p)(b-q) - a^2b^2c^2(\overline{p}b-1)(\overline{p}b-1) = 0$$

$$c^4(c-p)(c-q) - a^2b^2c^2(\overline{p}c-1)(\overline{q}c-1) = 0$$

It is possible here to define $x = \frac{p+q}{2}$ and $r = p - x = q - x$ and solve the system, but we'll do something else, and we'll consider the polynomial:

$$P(x) = x^6 - (p+q)x^5 + pqx^4 - a^2b^2c^2\overline{pq}x^2 + a^2b^2c^2(\overline{p}+\overline{q})x - a^2b^2c^2$$

We know that a, b, c are 3 of the 6 roots of $P(x)$. Let the others be u, v, w. Now let's see what we can obtain from the Viète relations:

- From the x^0 term: $abcuvw = -a^2b^2c^2 \iff uvw = -abc$
- From the x term: $abcuvw(\Sigma\frac{1}{a}) = -a^2b^2c^2(\overline{p}+\overline{q}) \iff \Sigma\frac{1}{a} = \overline{p}+\overline{q}$
- From the x^3 term: $\Sigma abc = 0 \iff abc+uvw+(a+b+c)(uv+uw+vw)+(u+v+w)(ab+bc+ac) = 0$
- And from the x^5 term: $a+b+c+u+v+w = p+q$

By applying the x^0 condition twice to the equation from x^3, we obtain:

$$(a+b+c)(\frac{1}{u}+\frac{1}{v}+\frac{1}{w}) = (u+v+w)(\frac{1}{a}+\frac{1}{b}+\frac{1}{c})$$

The problem asks us to prove that the midpoint of PQ lies on the Euler line, i.e. $0, a+b+c, p+q$ are collinear. That means:

$$\frac{a+b+c}{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}} = \frac{p+q}{\overline{p}+\overline{q}}$$

Since we have expressed $p+q$ and $\overline{p}+\overline{q}$ from Viète, we need to prove:

$$\frac{a+b+c}{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}} = \frac{a+b+c+u+v+w}{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{u}+\frac{1}{v}+\frac{1}{w}}$$

Which is implied by the condition written beforehand, i.e.:

$$\frac{a+b+c}{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}} = \frac{u+v+w}{\frac{1}{u}+\frac{1}{v}+\frac{1}{w}}$$

So we've proven the statement.

1.6 Problems to Work on

- **Nordic 2025 P3** Let ABC be an acute triangle with orthocenter H and circumcenter O. Let E and F be points on the line segments AC and AB respectively such that $AEHF$ is a parallelogram. Prove that $|OE| = |OF|$.
- **IMO 2019 P6** Let I be the incentre of acute triangle ABC with $AB \neq AC$. The incircle ω of ABC is tangent to sides BC, CA, and AB at D, E, and F, respectively. The line through D perpendicular to EF meets ω at R. Line AR meets ω again at P. The circumcircles of triangle PCE and PBF meet again at Q.

  Prove that lines DI and PQ meet on the line through A perpendicular to AI.
- **IMO 2025 P2** Let Ω and Γ be circles with centres M and N, respectively, such that the radius of Ω is less than the radius of Γ. Suppose Ω and Γ intersect at two distinct points A and B. Line MN intersects Ω at C and Γ at D, so that C, M, N, D lie on MN in that order. Let P be the circumcentre of triangle ACD. Line AP meets Ω again at $E \neq A$ and meets Γ again at $F \neq A$. Let H be the orthocentre of triangle PMN.

  Prove that the line through H parallel to AP is tangent to the circumcircle of triangle BEF.

- **Balkan MO 2023 P2** In triangle ABC, the incircle touches sides BC, CA, AB at D, E, F respectively. Assume there exists a point X on the line EF such that

$$\angle XBC = \angle XCB = 45^\circ.$$

Let M be the midpoint of the arc BC on the circumcircle of ABC not containing A. Prove that the line MD passes through E or F

- **Balkan MO 2025 P2** In an acute-angled triangle ABC, H be the orthocenter of it and D be any point on the side BC. The points E, F are on the segments AB, AC, respectively, such that the points A, B, D, F and A, C, D, E are cyclic. The segments BF and CE intersect at P. L is a point on HA such that LC is tangent to the circumcircle of triangle PBC at C. BH and CP intersect at X. Prove that the points D, X, and L lie on the same line.

2 Complex Numbers in Algebra

2.1 Introductory Notions

We first introduce the tools used in this section. (Of course, we consider as known everything in the Definitions Section.

An important role in this section is that of the roots of unity. The n-th roots of unity are the n roots of the polynomial $x^n - 1$. We can show there are n such roots by listing them: $e^{\frac{2k\pi i}{n}} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$ are roots of the polynomial for any natural k. A primitive n-th root of unity is a root of $x^n - 1$, which is not a root of $x^m - 1$ for any natural $m < n$. For a primitive n-th root of unity ζ_n, any other root of unity can be written as ζ_n^k for some integer k. This is true since $\zeta_n^{k_1} = \zeta_n^{k_2}$ implies $\zeta_n^{k_1-k_2} = 1$, so $k_1 - k_2$ is divisible by n.

Another trick we use is that a number r is real if and only if $r = \overline{r}$. This is very useful for the simple reason that we can compute conjugates comfortably. As a result, the fact follows that whenever $P(r) = 0$ for a polynomial with real coefficients $P(\overline{r}) = \overline{P(r)} = 0$.

2.2 Functional Equations

In this section, we will discuss functional equations that have $\mathbb{C}$, the complex numbers, as a domain or codomain. Even if it would not seem plausible that problems explicitly asking to find all functions from $\mathbb{C}$ to $\mathbb{C}$, for example, appear at a contest, in the very recent period, multiple problems of this type appeared in shortlists and team selection tests of different countries.

Problem 1. *Romanian District Olympiad 2025 10.3*
Determine all functions $f : \mathbb{C} \to \mathbb{C}$ such that

$$|wf(z) + zf(w)| = 2|zw|$$

for all $w, z \in \mathbb{C}$.

Solution:

Denote the assertion in the problem by $P(w, z)$. Writing $P(a, b)$implies something, means that we plug in the equation a for x and b for y and draw conclusions. $P(1, 0) \Rightarrow f(0) = 0$. $P(x, x) \implies |f(x)| = |x|$ for any x. Dividing both sides of $P(z, 1)$ by $|z1|$, we get $|\frac{f(z)}{z} + f(1)| = 2$, however by triangle inequality:

$$2 = |\frac{f(z)}{z}| + |f(1)| \geq |\frac{f(z)}{z} + f(1)| = 2$$

with equality if and only if $\frac{f(z)}{z} = f(1)$, or in other words, $f(z) = zf(1)$ for any z. Thus, solutions of the given functional equation will be $f(x) = cx$ for any c with absolute value 1, which clearly fit.

Problem 2. *Iran 2024 3rd Round Test 1 P1*
Suppose that $T \in \mathbb{N}$ is given. Find all functions $f : \mathbb{Z} \to \mathbb{C}$ such that for all $m \in \mathbb{Z}$ we have $f(m+T) = f(m)$ and:

$$\forall\, a, b, c \in \mathbb{Z} : f(a)\overline{f(a+b)f(a+c)}f(a+b+c) = 1.$$

Where $\overline{a}$ is the complex conjugate of a. This was enough to deal with the condition, as we can clearly see that any k and ζ with absolute value 1 yield a valid solution. Now, to make the function satisfy $f(x+T) = f(x)$ ζ must satisfy $\zeta^T = 1$. So, solutions are all functions with $f(x) = k\zeta^x$ for k with absolute value 1 and any primitive $T-th$ root of unity ζ.

Solution:

First, plugging $b = c = 0$, we get $|f(a)| = 1$ for any a, thus substituting the conjugates we get $f(a)f(a+b+c) = f(a+b)f(a+c)$. Substituting 1 for b and c we get $f(x+2) = \frac{f(x+1)^2}{f(x)}$, which allows us to inductively determine $f(n)$. In particular, we see that letting $f(0) = k$ and $\frac{f(1)}{f(0)} = \zeta$, we can inductively show that $f(n) = k\zeta^n$ for any integer n.

Problem 3. *Iran 2024 3rd round Algebra Exam P2*
A surjective function $g : \mathbb{C} \to \mathbb{C}$ is given. Find all functions $f : \mathbb{C} \to \mathbb{C}$ such that for all $x, y \in \mathbb{C}$ we have

$$|f(x) + g(y)| = |f(y) + g(x)|.$$

Solution:

For any x define the function $g^{-1}(x)$ by assigning to that x an arbitrary but fixed value y with $f(y) = x$. Let $h(a) = f(g^{-1}(a))$. $P(x, g^{-1}(y)) \implies |h(x) + y| = |h(y) + x|$ for any x and y, which we will call $Q(x, y)$. $Q(a, -h(a)) \implies h(-h(a)) = -a$, and using this: $Q(x, -f(y) \Rightarrow |x - y| = |h(x) - h(y)|$. Let's call the last assertion $R(x, y)$. We will prove only using it that $f(x) = m + nx$ for any x or that $f(x) = m + n\overline{x}$ for any x, for some n with absolute value 1. Indeed, let $h_1(x) = h(x) - h(0)$, which satisfies $|h_1(x)| = |x|$ because of $R(x, 0)$. Let $h_2(x) = \frac{h_1(x)}{h_1(1)}$. $h_2(x)$ now satisfies $|h_2(x)| = |x|$ and $|h_2(x) - 1| = |x - 1|$, because of $R(x, 0)$ and $R(x, 1)$. From this place, there are two ways to get that $h_2(x)$ is either x or $\overline{x}$. The first one is geometrical. Labeling in the complex plane the point X with coordinate x and the point Y with coordinate $h_2(x)$. The first condition means that Y is on the circle with center 0 and radius $|x|$, and on the circle of center 1 and radius $|x - 1|$, and as the two circles can intersect at at most 2 points, there are at most 2 possible solutions for the equations, which clearly are x and $\overline{x}$. The second, algebraic, solution is to square both moduli. The first equation implies that $x \cdot \overline{x} = h_2(x) \cdot \overline{h_2(x)}$ and the second that $x \cdot \overline{x} - x - \overline{x} + 1 = h_2(x) \cdot \overline{h_2(x)} - h_2(x) - \overline{h_2(x)} + 1$, or by subtracting the second from the first we get: $x + \overline{x} = h_2(x) + \overline{h_2(x)}$, meaning that $2Re(x) = 2Re(h_2(x))$, which together with $|x| = |h_2(x)|$ is the required conclusion. Next, if for some non-real x, $h_2(x) = x$ and for some non-real y, $h_2(y) = \overline{y}$, substituting in the initial equation we get $|x - y| = |x - \overline{y}$, which is impossible as squaring the absolute values we get $(x + \overline{x})(y + \overline{y}) = 0$. The last step also has a geometric alternative. In the complex plane, the point with coordinate x is at the same distance from y as

from $\overline{y}$, meaning it is on the perpendicular bisector of the points with these coordinates, which is the real axis. Returning to the problem, $h(x)$ is either a linear function or of the form $m\overline{x}+n$. If $h(x)=mx+n$, $-x=h(-h(x))=-m^2x-mn+n$, implying that either $f(x)=x+c$ for any constant c, or $f(x)=-x$. If $h(x)=m\overline{x}+n$, $-x=h(-h(x))=-m\overline{m}-m\overline{n}+n$, meaning that either $h(x)=c\overline{x}$, for c with absolute value 1 or $h(x)=\frac{n}{\overline{n}}\overline{x}+n$. In this way, we obtained all the families of solutions for $h(x)$. Knowing that $f(g^{-1}(x))=h(x)$, is bijective, if $g(a)=g(b)=x_1$, performing the same operation once for $g^{-1}(x_1)=a$ and another time for $g^{-1}(x_1)=b$, we get a contradiction, so $g(x)$ is also injective, meaning that $g^{-1}(g(x))=x$, or that $f(x)=h(g(x)$. Next, we only have to substitute in the solutions we obtained for $h(x)$, $g(x)$. Finally, $f(x)$ is one of the functions below for any x:

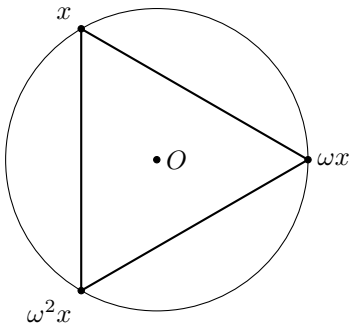
1. $f(x)=g(x)+a$, for any real number a.
2. $f(x)=-g(x)$.
3. $f(x)=cg(x)$, for some c with $|c|=1$.
4. $f(x)=\dfrac{d}{\overline{d}}\overline{x}+d$, for nonzero d.

All of these functions can be directly verified to work.

Problem 4. *BMO 2024 Shortlist G7*
Let $f:\pi\to\mathbb{R}$ be a function from the Euclidean plane to the real numbers such that $f(A)+f(B)+f(C)=f(O)+f(G)+f(H)$ for any acute triangle ΔABC with circumcenter O, centroid G and orthocenter H. Prove that f is constant.

Introduce the complex plane and assign to each point its complex coordinate. Let f now be a function from the set of complex numbers to the set of real numbers, and assume without loss of generality by shifting the function by a constant that $f(0)=0$ Substituting points a, b and c with equal absolute value we get:

$$f(a)+f(b)+f(c)=f(0)+f(g)+f(h)=0+f(\frac{a+b+c}{3})+f(a+b+c)$$



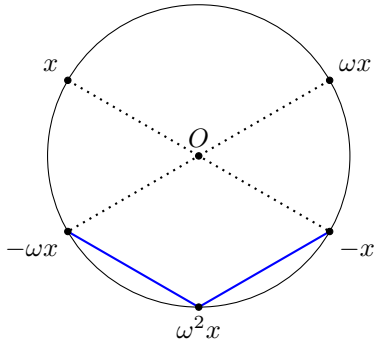
The facts that g and h have coordinates $\frac{a+b+c}{3}$ and $a+b+c$, respectively, are explained in the geometry section. Now, substituting $(a,b,c) = (x, wx, w^2x)$ where w is a primitive third root of unity (a root of $w^3 = 1$ which is not 1), we know that multiplying by a complex number with absolute value 1 means just rotating with the argument of the number, so the triangle with vertices (x, wx, w^2x) is, in fact, equilateral so it is clearly acute.

Also $w^3 = 1$ implies that $(w-1)(w^2+w+1) = 1$ so $w^2+w+1 = 0$, thus:

$$f(x) + f(wx) + f(w^2x) = f(x(1+w+w^2)) + f(\frac{x(1+w+w^2)}{3}) = 0$$

Similarly, substituting x, wx and y, we get:

$$f(y) - f(w^2x) = f(x) + f(wx) + f(y) = f(x+wx+y) + f(\frac{x+wx+y}{3}) = f(y-w^2x) + f(\frac{y-w^2x}{3})$$



Let's focus on the acute angle condition. As we see from the drawing, it is equivalent to $|w^2x - y| < |x|$, or by taking $y = b$ and $w^2x = a$, we get $f(a) - f(b) = f(\frac{a-b}{3})$ whenever $|a-b| < |b| = |a|$. We see that the right side of the equation only depends on $a-b$, so let $f(t) + f(\frac{t}{3}) = g(t)$ for a function g. It is not intuitive to prove that for x and y with the same absolute value, $f(x) - f(y)$ only depends on $x-y$. For two numbers x and y, let $\zeta^6 = \frac{y}{x}$. Next, for any x and y with the same absolute value, divide the circle arc connecting them into 6 equal sides. Next, clearly each of the sides has length at most $|x|$, meaning that

$$f(y) - f(x) =$$

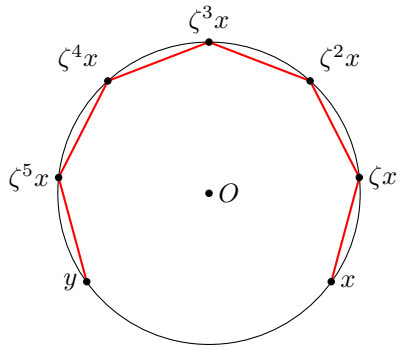
$$= (f(y)-f(r^5x))+(f(r^5x)-f(r^4x))+(f(r^4x)-f(r^3x))+(f(r^3x)-f(r^2x))+(f(r^2x)-f(rx))+(f(rx)-f(x))$$

Which, together with the fact that $g(x)$ is additive, means that the sum only depends on $x-y$, signifying that $f(x) - f(y)$ only depends on $x-y$ for x and y with the same absolute value. This means that $f(x) - f(y) = f(-y) - f(-x)$, or equivalently that $f(x) + f(-x)$ only depends in $|x|$, but as $0 = f(x) + f(x) + f(w^2x) + f(-x) + f(-wx) + f(-w^2x)$, we get that $f(x) + f(-x) = 0$.

Finally:

$$f(-a) = -f(a) = f(wa) + f(w^2a) = f(wa) - f(-w^2a) = g((w+w^2)a) = g(-a)$$

This means that $f(x) = g(x)$ for every x, but in the beginning we had $g(x) = f(x) + f(\frac{x}{3})$, which means that $f(x) = 0$ for every $x \in \mathbb{C}$.



2.3 Application of Geometry

Since we use complex numbers to solve geometry problems, it would only be fair if we solved complex number problems through geometry from time to time. This procedure is quite straightforward: we assign the complex numbers to geometrical points in the plane and solve synthetically.
The next example uses a technique more advanced than the problem, but it is a worthwhile application.

Linearity of the Power of a Point:

The Power of a Point, $\mathbb{P}(x, y)$, where (x, y) are the cartesian coordinates of the point, is the output of: $\mathbb{P}(x, y) = (x-a)^2 + (y-b)^2 - R^2$, where (a, b) are the coordinates of the center of the circle, and R is the radius of the circle. This is a quadratic in (x, y).
Let's define the function $F(x, y) = \mathbb{P}_1(x, y) - \mathbb{P}_2(x, y)$, where $\mathbb{P}_1$ and $\mathbb{P}_2$ are the powers of point functions of two separate circles. Then, the quadratic terms vanish, and we are left with a linear equation: $F(x, y) = 2(a_2 - a_1)x + 2(b_2 - b_1)y + C$. The only important thing here is that, considering $\Sigma\alpha_i = 1$, we have:

$$X = \Sigma\alpha_i P_i \iff F(X) = \Sigma\alpha_i F(P_i)$$

Example Problem 5. *Mathematical Magazine 2003*
Demonstrate that for any $z_1, z_2, z_3 \in \mathbb{C}$ with $|z_1| = |z_2| = |z_3| = R$ and $z = \frac{z_1+z_2+z_3}{3}$:

$$\min(|z-z_1| \cdot |z-z_2|, |z-z_2| \cdot |z-z_3|, |z-z_3| \cdot |z-z_1|) \leq R^2 - |z|^2$$

Solution: Let z_1, z_2, z_3 correspond to A, B, C. Since they are equal in module, the origin of the complex plane corresponds to the center of the circumscribed circle, which has radius R. z corresponds

to the centroid, G, of ABC. So we have to prove:

$$\min(AG \cdot BG, BG \cdot CG, CG \cdot AG) \leq R^2 - OG^2$$

We notice that $R^2 - OG^2$ is the module of the power of G with respect to (ABC). Let's define the function $F(X) = \mathbb{P}_1(X) - \mathbb{P}_2(X)$, where $\mathbb{P}_1$ is the power of X with respect to (ABC), and $\mathbb{P}_2$ is the power with respect to the circle with the center in G and radius 0. Knowing that $G = \frac{A+B+C}{3}$, we have:

$$F(A) = 0 - AG^2; \quad F(B) = 0 - BG^2; \quad F(C) = 0 - CG^2$$

$$F(G) = \mathbb{P}_1(G) - 0 = OG^2 - R^2 = \frac{F(A) + F(B) + F(C)}{3} = -\frac{AG^2 + BG^2 + CG^2}{3}$$

So we are left with proving:

$$\min(AG \cdot BG, BG \cdot CG, CG \cdot AG) \leq \frac{AG^2 + BG^2 + CG^2}{3}$$

Which is true, since taking the arithmetic mean of the three values gives a classic inequality.

Example Problem 6. *Romanian Math Tournament 1996*
Let z_1, z_2, z_3 be complex numbers such that $|z_1| = |z_2| = |z_3| = 1$, and $z_1 + z_3 + z_3 = 1$ Demonstrate that for any $n \in N$:

$$z_1^{3^n} + z_2^{3^n} + z_3^{3^n} = 1$$

Solution:
Let z_1, z_2, z_3 correspond to A, B, C, so 0 corresponds to the center of (ABC). We know from the geometry section that the orthocenter is equal to $h = z_1 + z_2 + z_3 \iff h = 1 \iff H$ is on the circumcircle of ABC. By Hamilton, we know that the reflection of H over AB, BC and AC must also be on the circumcircle. Let's first analyze, without loss of generality, the line BC. The reflection of H over BC is $H' \in (ABC) \iff AC$ is the perpendicular bisector of the chord $HH' \iff AC$ passes through the center of the circle. But only one of the sides of the triangle can pass through 0, so for the other two, H must coincide with its reflection $\iff H \in AB, H \in AC \iff H \equiv A \iff h = z_1 = 1 \iff z_2 = -z_3$. Therefore, since $3^n \equiv 1 \mod 2$:

$$z_1^{3^n} + z_2^{3^n} + z_3^{3^n} = z_1^{3^n} = 1$$

2.4 Miscellaneous Problems

In this section, we will exhibit solutions of problems asking us something about complex numbers. Most of the problems are in some way different from the others; however, a vast majority will succumb to basic algebra identities and concepts, or at most knowing how a conjugate works.

Problem 7. *2025 ELMO Shortlist A2*
Over all complex-coefficient polynomials $P(x)$ of degree n, what is the maximum number of complex numbers x with magnitude 1 such that $P(x)$ is real?

Solution: The answer is $2n$ for $n \geq 1$. A construction which shows we can have $2n$ such numbers is $P(x) = x^n$. Clearly, any root of $x^{2n} - 1 = 0$ satisfies $(x^n)^2 = 1$, so x^n is either 1 or -1. As there are $2n$ such roots, the answer is at least $2n$. To show that we can't do better, assume $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. $P(x) \in \mathbb{R}$ is equivalent to

$$P(x) = \overline{P(x)} = \overline{a_n}\overline{x^n} + \overline{a_{n-1}}\overline{x^{n-1}} + \cdots + \overline{a_0} = \frac{\overline{a_n}}{x^n} + \frac{\overline{a_{n-1}}}{x^{n-1}} + \cdots + \overline{a_0}$$

It is clear that after multiplying both sides by x^n, we have a polynomial in x which has at most $2n$ roots.

Problem 8. *2023 USA TSTST Problem 5*
Suppose a, b, and c are three complex numbers with product 1. Assume that none of a, b, and c are real or have absolute value 1. Define $p = (a+b+c) + \left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right)$ and $q = \frac{a}{b} + \frac{b}{c} + \frac{c}{a}$. Given that both p and q are real numbers, find all possible values of the ordered pair (p, q).

Solution: Let $a = \frac{x}{y}$, $b = \frac{y}{z}$ and $c = \frac{z}{x}$.

$$p = \sum \frac{x}{y} + \sum \frac{y}{x} = \sum \frac{x}{y} + \frac{y}{x} = \sum \frac{x^2z + y^2z}{xyz} = \frac{(x+y+z)(xy+yz+zx)}{xyz} - 3$$

Similarly:

$$q = \sum \frac{x^2}{yz} = \frac{\sum x^3}{xyz} = 3 + \frac{\sum x^3 - 3xyz}{xyz} = \frac{(x+y+z)(x^2+y^2+z^2-xy-yz-zx)}{xyz}$$

We can now focus on the two expressions which we know are real:

$$\frac{(x+y+z)(x^2+y^2+z^2-xy-yz-zx)}{xyz} \text{ and } \frac{(x+y+z)(xy+yz+zx)}{xyz}$$

Adding three times the second to the first, we obtain that $\frac{(x+y+z)^3}{xyz}$ is real. We can scale x, y and z by setting for example $x_1 = x\frac{|x+y+z|}{x+y+z}$, and so on for y_1 and z_1 so their sum is now real. So we can assume $x+y+z$ is real. If $x+y+z$ is not 0, because $\frac{(x+y+z)^3}{xyz}$ is real, xyz also is. Similarly, because $\frac{(x+y+z)(xy+yz+zx)}{xyz}$ is real, $xy+yz+zx$ also is real. Now, we know that by Viète's formulas, x, y, and z are all roots of a cubic equation with real coefficients. If all three of them are real, then a, b, and c are also real. And if $P(x) = 0$, for some non-real x, $P(\overline{x})$ is als 0, meaning one of a, b and c has the form $\frac{x}{\overline{x}}$ or $\frac{\overline{x}}{x}$, which clearly has absolute value 1. Now, if $x+y+z = 0$, we must have $p = -3$ and $q = 3$. An example numbers for which $p = -3$ and $q = 3$ are $x = 10+5i$, $y = 2-3i$ and $z = -12-2i$.

Problem 9. *USA TSTST 2020 Problem 7*
Find all non-constant polynomials $P(z)$ with complex coefficients for which all complex roots of the polynomials $P(z)$ and $P(z) - 1$ have absolute value 1.

Solution: Scale the polynomial such that it is monic, and the constant terms only differ. Consider two polynomials $P(x)$ divided by their leading coefficient, and call them $Q_1(x)$.

$$Q_1(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + u \text{ and } Q_2(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + v$$

Let $Q_1(x)$ have roots $x_1, x_2 \dots x_n$ and $Q_2(x)$ have roots $y_1, y_2, \dots y_n$. We now show that $x_i^n + u = 0 = y_i^n + v$. We show this for x_i, and the proof is analogous for y_i. Indeed,

$$Q_2(x_i) = (x_i - y_1)(x_i - y_2)\cdots(x_i - y_n) = v - u$$

. We will also use that $|u| = |v| = 1$, by Viète's formulas. For x and y with absolute value 1, $\frac{x-y}{\overline{x-y}} = \frac{x-y}{\frac{1}{x}-\frac{1}{y}} = -xy$. By applying this to the relation we get

$$\prod_{j=1}^{n}(x_i - y_j) = v - u \implies \frac{\prod_{j=1}^{n}(x_i - y_j)}{\overline{\prod_{j=1}^{n}(x_i - y_j)}} = \frac{v-u}{\overline{v-u}} \Rightarrow (-1)^n x_i^n \prod_{j=1}^{n} y_j = -uv$$

However, by Viète's formulas $(-1)^n \prod y_i = v$, so we get $x_i^n = -u$. This means that all the roots of $x^n + u = 0$ are also roots of $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + u$, so these are also roots of $a_{n-1}x^{n-1} + \cdots + a_1x = 0$. which can only be true if all the a_i's are 0 as $x^n = -u$ has n distinct roots. Finally, we get that all the coefficients of $P(x)$ except for the first and the last are 0, so solutions are polynomials of the form $P(x) = \frac{x^n+u}{u+v}$ for u and v with absolute value 1.

2.5 Problems to Work on

3 Complex Numbers in Combinatorics

3.1 Roots of Unity Filter

The following identity is used to compute the sum of coefficients of a polynomial: If $P(x) = \sum_{i=0}^{d} a_i x^i$, than the sum of the coefficients of all powers divisible by some $n \in \mathbb{N}$ can be computed as:

$$a_0 + a_n + a_{2n} + \dots a_{n\lfloor \frac{d}{n} \rfloor} = \frac{P(\zeta_1) + P(\zeta_2) + \dots + P(\zeta_n)}{n}$$

where ζ_i are all n-th roots of unity. If you are unfamiliar with the term roots of unity, we suggest checking the Introductory Notions in the Algebra Section or the Roots of Unity and Cyclotomic Polynomials Subsection.

The proof of this is natural. Consider a primitive root of unity of order n, ζ. Clearly all the roots are $\zeta, \zeta^2, \zeta^3 \dots \zeta^n$. Then:

$$P(\zeta_1)+P(\zeta_2)+\dots+P(\zeta_n) = na_0+a_1(\zeta_1+\zeta_2+\dots+\zeta_n)+a_2(\zeta_1^2+\zeta_2^2+\dots+\zeta_n^2)+\dots+a_d(\zeta_1^d+\zeta_2^d+\dots+\zeta_n^d)$$

Which, using our ζ notation equals:

$$na_0 + a_1(\zeta + \zeta^2 + \dots + \zeta^n) + a_2(\zeta^2 + \zeta^4 + \dots + \zeta^{2n}) + \dots + a_d(\zeta^d + \zeta^{2d} + \dots + \zeta^{nd})$$

So we must, in fact, show that

$$\zeta^x + \zeta^{2x} + \dots + \zeta^{nx} = \begin{cases} n, & \text{if } n \mid x, \\ 0, & \text{otherwise.} \end{cases}$$

If $n \mid x$, it is clear. Else,

$$\zeta^x + \zeta^{2x} + \dots + \zeta^{nx} = \zeta^x \frac{\zeta^{nx} - 1}{\zeta^x - 1} = 0$$

as a sum of a geometric progression. The strategy to use when solving problems with this technique is to create a polynomial, which multiplied by some other polynomial or raised to some power, reinterprets the problem condition.

Problem 0. *Authors' Problem*
In a class, there are 36 students who must go on an excursion. The tickets to the excursion can only be bought for 4 people, so the group of people must have a size divisible by 4. How many different possibilities are there to pick such a group of students?

Solution:
We see that we can pick a group of $4k$ students in $\binom{36}{4k}$ ways so we must compute:

$$\binom{36}{0} + \binom{36}{4} + \binom{36}{8} + \binom{36}{12} + \binom{36}{16} + \binom{36}{20} + \binom{36}{24} + \binom{36}{28} + \binom{36}{32} + \binom{36}{36}$$

Sadly, numbers like $\binom{36}{16}$ are too big to be computed by hand, here our new method comes handy.

We remember that all of these are coefficients in the polynomial $P(x) = (x+1)^{36}$, so we must count the sum of the coefficients of this polynomial which stand next to exponents divisible by 4. Using the Roots of Unity Filter formula, the sum we need is:

$$\frac{P(1) + P(i) + P(-1) + P(-i)}{4} = \frac{(1+1)^{36} + (1+i)^{36} + (1-1)^{36} + (1-i)^{36}}{4}$$

This is clearly an answer, but we still need to make it real. For this, we must remember $(1+i)^4 = (1-i)^4 = -4$, so $(1+i)^{36} = (1-i)^{36} = (-4)^9 = -2^{18}$, meaning:

$$\frac{(1+1)^{36} + (1+i)^{36} + (1-1)^{36} + (1-i)^{36}}{4} = \frac{2^{36} - 2 \cdot 2^{18}}{4} = 2^{34} - 2^{17}$$

Problem 1. *IMC 1999 P8*
A dice with 6 faces is rolled n times. What is the probability that the sum of all the results is divisible by 5?

Solution:

Consider $P(x) = (x + x^2 + x^3 + x^4 + x^5 + x^6)^n$. It is clear that if there if there are a_k ways to obtain the sum k by throwing the dice, then a_k is the coefficient next to x^k in the polynomial. Thus, we must compute the sum of all the coefficients of the polynomial which are divisible by 5, which is in fact:

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

where ζ is a fifth root of unity which is not 1. In fact, because $\zeta^5 = 1$, but $\zeta \neq 1$, $\zeta^4+\zeta^3+\zeta^2+\zeta+1 = 0$, so $\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta = \zeta^6 = \zeta$, so the expression we must compute is in fact:

$$\frac{6^n + \zeta^n + \zeta^{2n} + \zeta^{3n} + \zeta^{4n}}{5} = \begin{cases} \dfrac{6^n + 4}{5}, & \text{if } 5 \mid n, \\ \dfrac{6^n - 1}{5}, & \text{otherwise.} \end{cases}$$

But as we were asked for the probability, not the number of ways this can happen (and we have 6^n different dice throws), the answer to the problem is:

$$\begin{cases} \dfrac{6^n + 4}{5 \cdot 6^n}, & \text{if } 5 \mid n, \\ \dfrac{6^n - 1}{5 \cdot 6^n}, & \text{otherwise.} \end{cases}$$

In the same way we computed the sum of the coefficients which are divisible by some n of a polynomial, we can, in fact, compute the sum of the coefficients which give an exact residue when divided by n. It is just enough to observe that the sum of the coefficients which give residue r upon division by n equals the sum of the coefficients which are divisible by n in the polynomial $x^{n-r}P(x)$, so:

$$\sum_{i\equiv r \mod n} a_i = \frac{\zeta_1^{n-r}P(\zeta_1)+\zeta_2^{n-r}P(\zeta_2)+\cdots+\zeta_n^{n-r}P(\zeta_n)}{n} = \frac{\sum_{i=1}^{n}\zeta^{i(n-r)}P(\zeta^i)}{n}$$

Where ζ is a primitive n-th root of unity.

Problem 2. *Leningrad 1991*
A finite sequence $a_1, a_2, ..., a_n$ is called p-balanced if any sum of the form $a_k + a_{k+p} + a_{k+2p} + \cdots$ is the same for any $k = 1, 2, ..., p$. Prove that if a sequence with 50 members is p-balanced for each of $p = 3, 5, 7, 11, 13, 17$, then all its members are equal to zero.

Solution:

Consider the polynomial $P(x) = a_1x + a_2x^2 + \cdots + a_{50}x^{50}$ and a root of unity of order p, ζ_p where p is one of $3, 5 \ldots 17$. Counting the sum of the coefficients next to powers which give residue r upon division by n by the formula above, we have:

$$P(1) + P(\zeta_p) + \cdots + P(\zeta_p^{p-1}) =$$

$$= P(1) + \zeta_p P(\zeta_p) + \cdots + \zeta_p^{p-1}P(\zeta_p^{p-1}) =$$

$$\cdots$$

$$= P(1) + \zeta_p^{p-1}P(\zeta_p) + \cdots + \zeta_p^{(p-1)^2}P(\zeta_p^{p-1})$$

Let the common value of the above expressions be c. Considering $Q(x) = x^{p-1}P(\zeta_p^{p-1}) + x^{p-2}P(\zeta_p^{p-2}) + \cdots + P(1) - c$, $Q(x)$ has degree $p-1$ but has at least p roots, which are the p-th roots of unity, so it is the zero polynomial, meaning that $P(\zeta_p) = \cdots = P(\zeta_p^{p-1}) = 0$. Thus, $P(x)$ has as roots all primitive p-th roots of unity for p being a prime from $3, 5, 7, 11, 13, 17$. They are clearly all distinct. Thus, $P(x)$ has degree 50 and $(3-1)+(5-1)+(7-1)+(11-1)+(13-1)+(17-1) = 50$ roots, which are roots of unity, and also has 0 as a root. Thus, $P(x)$ has at least 51 roots but has degree 50, so it must be the zero polynomial.

Problem 3. *IMO 1995 P6*
Let p be an odd prime number. How many p-element subsets A of $\{1, 2, \ldots, 2p\}$ are there, the sum of whose elements is divisible by p?

Solution:

Let ζ be a p-th root of unity which is not 1 and consider:

$$P(x) = \prod_{i=1}^{p}(x-\zeta^i) = \prod_{i=1}^{p}(x-\zeta^i)^2 = (x^p-1)^2 = x^{2p} - 2x^p + 1$$

The term next to x^p contains is added an $-\zeta^r$ each time we pick a subset of $\{1, 2, \ldots, 2p\}$ with sum congruent to r mod p. So if we denote by a_k the number of subsets of $\{1, 2, \ldots, 2p\}$ with sum congruent to k mod p, than $2 = a_0 + \zeta a_1 + \zeta^2 a_2 + \ldots \zeta^{p-1}a_{p-1}$. Thus, letting $Q(x) = a_0 - 2 + xa_1 + x^2a_2 + \cdots + x^{p-1}a_{p-1}$, then all primitive p-th roots of unity are roots of this polynomial, and as

there are $p-1$ such roots, the polynomial $1+x+x^2+\dots x^{p-1}$ divides $Q(x)$. Clearly, this implies $a_0-2=a_1=\cdots=a_{p-1}$. And as $a_0+a_1+\cdots+a_{p-1}=\binom{2p}{p}$, we obtain $a_0=\frac{\binom{2p}{p}-2}{p}+2$ which is the answer of the problem.

Problem 4. *Thailand 2025 TST 3 P5*
Let $p\geq 3$ be a prime number and r be a positive integer. Prove that for any positive integer n with $n>r(p-1)$, the expression

$$\binom{n}{0}-\binom{n}{p}+\binom{n}{2p}-\binom{n}{3p}+\dots$$

is divisible by p^r.

(Note that $\binom{n}{k}=0$ whenever $k>n$.)

Solution:

Let $P(x)=(1-x)^n$, the given sum equals $\frac{\sum_{i=1}^{p}P(\zeta_i)}{p}$, where ζ_i are the p-th roots of unity. Next, by the well known identity $\binom{p-1}{k}\equiv(-1)^k \mod p$:

$$(1-x)^{p-1}=\sum_{k=0}^{p-1}\binom{p-1}{k}(-1)^k x^k=(1+x+x^2+\cdots+x^{p-1})+p\cdot Q(x)$$

Where $Q(x)$ is a polynomial with integer coefficients. Let $n=(p-1)r+m$. The sum rewrites as:

$$\frac{\sum_{i=1}^{p}(1-\zeta_i)^n}{p}=\frac{\sum_{i=1}^{p}p^r\cdot Q(\zeta_i)(1-\zeta_i)^m}{p}=p^r\frac{\sum_{i=1}^{p}Q(\zeta_i)(1-\zeta_i)^m}{p}$$

We used that $1+x+\dots x^{p-1}$ is 0 if x is a root of unity which is not 1 and $(1x)^m$ is 0 if $x=1$. The last sum equals the sum of the coefficients of the powers divisible by p of $Q(x)(1-x)^m$, so it is an integer.

Problem 5. *China 2010 Quiz 2 P2*
Let $M=\{1,2,\cdots,n\}$, each element of M is colored in either red, blue, or yellow. Set $A=\{(x,y,z)\in M\times M\times M | x+y+z\equiv 0 \mod n,\ x,y,z \text{ are of same color}\}$, $B=\{(x,y,z)\in M\times M\times M | x+y+z\equiv 0 \mod n,\ x,y,z \text{ are of pairwise distinct color}\}$. Prove that $2|A|\geq|B|$.

Solution:

Consider the polynomial $R(x)$ where $R(x)=x^{r_1}+x^{r_2}+...+x^{r_k}$, and r_i are the elements of M that are coloured red. Define in the same way $Y(x)$ and $B(x)$. Let ζ be a primitive n^{th} root of unity. For any m such that $n\nmid m$ the following holds true:

$$R(\zeta^k)+B(\zeta^k)+Y(\zeta^k)=\zeta^k+\zeta^{2k}+...+\zeta^{nk}=0$$

Next, the coefficient next to x^a in $R(x)^3$ equals the number of ways to get a subset with sum a of 3 red elements. Thus, the number of ways to get a monochromatic triple x,y,z with sum divisible by

n equals the sum of the coefficients of powers divisible by n if $R(x)^3 + Y(x)^3 + B(x)^3$. Which is

$$\frac{\sum_{i=1}^{n} R(\zeta^i)^3 + Y(\zeta^i)^3 + B(\zeta^i)^3}{n}$$

Now, the crucial identity is: $r^3 + y^3 + b^3 = (r + y + b)(\frac{(r-y)^2+(y-b)^2+(r-b)^2}{2})$. Using this identity:

$R(\zeta^i)^3+Y(\zeta^i)^3+B(\zeta^i)^3 = 3R(\zeta^i)Y(\zeta^i)B(\zeta^i)$ if i is not divisible by n and $R(1)^3+Y(1)^3+B(1)^3 \geq 3R(1)Y(1)B(1)$

Finally:

$$\frac{\sum_{i=1}^{n} R(\zeta^i)^3 + Y(\zeta^i)^3 + B(\zeta^i)^3}{n} \geq \frac{\sum_{i=1}^{n} 3R(\zeta^i)Y(\zeta^i)B(\zeta^i)}{n}$$

Where the last sum stands for the sum of the coefficients of powers divisible by n in the product of the polynomials, which counts the number of triples with sum divisible by n of different colours without overlaps (meaning that only one of $(x, y, z), (y, z, x)$ and all other permutations of a triple is counted). Thus, as each triple can be permuted in 6 ways, we obtained $|A| \geq \frac{3|B|}{6}$, which is the needed result.

Problem 6. *USA TST 2024 P3*
Let $n > k \geq 1$ be integers and let p be a prime dividing $\binom{n}{k}$. Prove that the k-element subsets of $\{1, \ldots, n\}$ can be split into p classes of equal size, such that any two subsets with the same sum of elements belong to the same class.

Solution: By Lucas' theorem the condition that p divides $\binom{n}{k}$ means that there is a natural r such that the residue obtained when n is divided by p^r is bigger than the residue when k is divided by p^r.Let $\sigma(S)$ denote the sum of the elements in S and define:

$$P(x) = \sum_{\substack{S \subseteq \{1,\ldots,n\} \\ |S|=k}} x^{\sigma(S)}$$

We will show that $P(x)$ is divisible by

$$\Phi_{p^r}(x) = \Phi_p(x^{p^{r-1}}) = x^{(p-1)p^{r-1}} + \cdots + x^{p^{r-1}} + 1.$$

Note that $P(x)$ is the coefficient of y^k in the polynomial

$$Q(x, y) = (1 + xy)(1 + x^2y) \ldots (1 + x^ny).$$

Let $n = p^ru + a$ and $m = p^rv + b$ with $a < b$. Let ζ be a primitive p^r-th root of unity. Then

$$Q(\zeta, y) = \left[(1 + \zeta y)(1 + \zeta^2 y) \cdots (1 + \zeta^{p^r} y)\right]^u (1 + \zeta y)(1 + \zeta^2 y) \ldots (1 + \zeta^a y).$$

Clearly, $\zeta, \zeta^2, \ldots, \zeta^{p^r}$ are all the p^r-th roots of unity. Thus:

$$\begin{aligned}&(1+\zeta y)(1+\zeta^2 y)\cdots(1+\zeta^{p^r} y)\\&=(1-\zeta(-y))(1-\zeta^2(-y))\cdots(1-\zeta^{p^r}(-y))\\&=1-(-y)^{p^r},\end{aligned}$$

so

$$Q(x,y)=(1-(-y)^{p^r})^u(1+\zeta y)(1+\zeta^2 y)\ldots(1+\zeta^a y).$$

So, if we had some term with y^k in $Q(\zeta, x)$, it would have some terms with exponent p^r from the first bracket, and some (at most a) from the other brackets. However, we have already established that $a < b$meaning that $P(x) = 0$ whenever x is a primitive p^r-th root of unity, which means that $\Phi_{p^r}(x)$ divides $P(x)$.
Back to the problem, let $a_0, a_1, \ldots$ denote the coefficients of P, and define

$$s_i = \sum_{j \equiv i \pmod{p^r}} a_j.$$

The divisibility proved above implies

$$\begin{aligned}s_0 = s_{p^{r-1}} = \cdots = s_{(p-1)p^{r-1}},\\s_1 = s_{p^{r-1}+1} = \cdots = s_{(p-1)p^{r-1}+1},\\\vdots\\s_{p^{r-1}-1} = s_{2p^{r-1}-1} = \cdots = s_{p^r-1}.\end{aligned}$$

This means we can construct the p classes by placing a set with sum $\sigma(S)$ in the class number

$$\left\lfloor \frac{(\sigma(S) \bmod p^r)}{p^{r-1}} \right\rfloor.$$

3.2 Board Problems

Sometimes, the problem asks to tile some board, and it can be solved by assigning each coordinate some power of a primitive root of unity, and observing how the problem property transforms.

Problem 1.
Can a 2021×2021 square with the central square removed be tiled with rectangles 4×1 and 1×4?

Solution:

Assume such a tiling is possible and assign to each square with coordinates (x, y) the number i^{x+2y}. Clearly, the sum of the numbers on each tiled rectangle is zero; thus, the sum of all the labels

equals the label of the central square which is i^{3033}, thus:

$$i^{3033} = (i + i^2 + \cdots + i^{2021})((-1) + 1 + \cdots + (-1) + 1 - 1) = i^3$$

which is not true.

Problem 2. *BMC 2000*
Consider a rectangle that can be tiled by a finite combination of $1 \times m$ and $n \times 1$ rectangles, where m, n are positive integers. Prove that it is possible to tile this rectangle using only $1 \times n$ rectangles or only $m \times 1$ rectangles.

Solution:

Assign to each square with coordinate (x, y) inside the rectangle the number $\zeta_m^x \zeta_n^y$. Clearly, the sum of the labels of the squares covered by a $1 \times m$ or $n \times 1$ tile is zero, and as all the rectangle is tiled, the sum of all the labels is zero. Let the rectangle be have $a \times b$ squares. By summing:

$$0 = \sum_{1 \le x \le a; 1 \le y \le b} \zeta_m^x \zeta_n^y = (\sum_{i=1}^{a} \zeta_m^i)(\sum_{j=1}^{b} \zeta_n^j)$$

So either a is divisible by m or b is divisible by n, which solves the problem.

3.3 Problems to Work on

- **Indonesia TST 2021 P8** Let p be an odd prime. Determine the number of nonempty subsets from $\{1, 2, \ldots, p-1\}$ for which the sum of its elements is divisible by p.
- **Moldova 2016 TST P6** Let $n \in \mathbb{Z}_{>0}$. The set S contains all positive integers written in decimal form that simultaneously satisfy the following conditions: each element of S has exactly n digits; each element of S is divisible by 3; each element of S has all its digits from the set $\{3, 5, 7, 9\}$ Find $\mid S \mid$.
- **IMO 2008 P5** Let n and k be positive integers with $k \ge n$ and $k - n$ an even number. Let $2n$ lamps labelled 1, 2, ..., $2n$ be given, each of which can be either on or off. Initially, all the lamps are off. We consider sequences of steps: at each step, one of the lamps is switched (from on to off or from off to on).

  Let N be the number of such sequences consisting of k steps and resulting in the state where lamps 1 through n are all on, and lamps $n+1$ through $2n$ are all off.

  Let M be the number of such sequences consisting of k steps, resulting in the state where lamps 1 through n are all on, and lamps $n+1$ through $2n$ are all off, but where none of the lamps $n+1$ through $2n$ is ever switched on.

  Determine $\frac{N}{M}$.
- **USA TSTST 2018 P6** Let $S = \{1, \ldots, 100\}$, and for every positive integer n define

$$T_n = \{(a_1, \ldots, a_n) \in S^n \mid a_1 + \cdots + a_n \equiv 0 \pmod{100}\}.$$

Determine which n have the following property: if we color any 75 elements of S red, then at least half of the n-tuples in T_n have an even number of coordinates with red elements.

- **RMM 2021 P3** A number of 17 workers stand in a row. Every contiguous group of at least 2 workers is a *brigade*. The chief wants to assign each brigade a leader (who is a member of the brigade) so that each worker's number of assignments is divisible by 4. Prove that the number of such ways to assign the leaders is divisible by 17.

- **Taiwan TST 2019 P6** Given a prime $p = 8k + 1$ for some integer k. Let r be the remainder when $\binom{4k}{k}$ is divided by p. Prove that $\sqrt{r}$ is not an integer.

4 Complex Numbers in Number Theory

4.1 Gaussian Integers in Number Theory

For this part, we will work with the ring of Gaussian integers.

Definition: The ring of Gaussian Integers, denoted by $\mathbb{Z}[i]$ is the set of complex numbers of the form $a + bi$ where both a and b are integers.

For example $1 + i$ and $2 - 3i$ are Gaussian integers, but $\frac{1}{2}$; $\sqrt{2} + 3i$ and $3 + \frac{i}{2}$ are not.

It turns out $\mathbb{Z}[i]$ carries out most of $\mathbb{Z}$'s concepts and properties.

- **Units:** The numbers $i, i^2 = -1, i^3 = -i$ and $i^4 = 1$, or alternatively the Gaussian integers with norm 1, are called units.
- **Divisibility:** We say $a|b$ for Gaussian a and b if $\frac{b}{a} \in \mathbb{Z}[i]$. Also, $a|b$ implies $|a|^2$ divides $|b|^2$, but not the other way.
- **gcd:** We denote the greatest common divisor of a and b as a Gaussian integer g that divides both a and b, such that any other common divisor of a and b also divides g. g is unique up to multiplication by units, so a gcd can be both $1 + i$ and $1 - i$. This is a small abuse of notation, but it is harmless when solving problems.
- **Euclidean Algorithm:** The Euclidean Algorithm still works for $\mathbb{Z}[i]$.
- **Primes and Factorization:** There also exist primes in $\mathbb{Z}[i]$ (in fact, all irreducible elements are primes), and any number can be uniquely factored as a product of primes to some exponents, and the factorization uniquely determines a number up to multiplication by units.

This being the set of basic definitions and properties, everything should look familiar. In fact, they all reduce to the Gaussian integers being a Unique Factorization Domain or an Euclidean Domain. Rigorously proving the above is outside the scope of the article.

The first natural question to ask is what happens to the primes. The answer is also natural, if $p \equiv 3 \mod 4$ is a prime, it stays a prime in the Gaussian integers, else it splits into two primes which are conjugates of each other.

To see why, assume for the sake of contradiction that $p \equiv 3 \mod 4$ and it can be written as $p = xy$ for some Gaussian x and y. The absolute values of x and y squared both divide the absolute value of p squared, which is p^2, and as none of them is 1, both of them are p, which fails writing $x = a + bi$ and checking that $a^2 + b^2 = p$ fails by $\mod 4$.

For primes 1 mod 4, if you are familiar to Fermat's Christmas Theorem (hyperlink), we can take $a^2 + b^2 = p$ and thus $(a + bi)(a - bi) = p$, and it is clear that both $a + bi$ and $a - bi$ are primes as if they could be factored, the moduli of the factors would multiply to p.

If $p = 2$, $2 = (1+i)(1-i)$. In fact, you might remember from above that $1+i$ and $1-i$ are more closely linked than just conjugates. This is a useful thing to notice, as it leads to $(1 + i)^4 = (1 - i)^4 = -4$. You might want to keep this in mind, as these are the only Gaussian integers that are not purely real or purely complex, but become real raised to a power.

After reading the property above, it should already be clear that the one and only use of Gaussian integers is: $\boxed{a^2 + b^2 = (a + bi)(a - bi)}$. This identity might not seem so useful, but it is, in fact, extremely powerful.

Problem 0. *Folklore*
Find all pairs of integers x and y such that $x^3 = y^2 + 1$.

Solution:

Rewrite the relation as $x^3 = (y + i)(y - i)$. We will show that the brackets from the right side are coprime. Indeed, let $d = \gcd(y + i; y - i)$. Clearly, $d|(y + i) - (y - i)$, so d is a divisor of 2. Thus, $|d|^2$ divides 4, but $|d|^2$ also divides $|y + i|^2 = y^2 + 1$. Clearly, if y is odd, the right side of the equation can't be divisible by 4, but is divisible by 2, so it can't be a perfect cube. So $|d| = 1$, meaning d is a unit.

So, both $y + i$ and $y - i$ are perfect cubes multiplied by units, and as each unit is also a perfect cube, we can conclude they are both perfect cubes of some Gaussian Integers. Let $y+i = (a+bi)^3 = a^3 - 3ab^2 + (3a^2b - b^3)i$, so $3a^2b - b^3 = 1$. This means b divides 1 (as an integer), so b is 1 or -1. If $b = 1$, the equation rewrites as $3a^2 = 2$, impossible. If $b = -1$, $a = 0$ so $y + i = (-i)^3 = i$, meaning $y = 0$. So $(x, y) = (1, 0)$ is the only solution.

The next example is a general problem and is useful to remember as a result.

Problem 1. *Gauss*
For a positive integer n, how many ordered pairs of integer solutions does the equation $n = a^2 + b^2$ have ?

Solution:

If n has a prime factor of the form $4k + 3$ at an odd power, the answer is 0. If not, the answer is

$$4 \prod_{\substack{p \equiv 1 \mod 4 \\ p|n}} (v_p(n) + 1)$$

If the question is asked for nonnegative integers, the answer is:

$$\left\lceil \frac{\prod\limits_{\substack{p \equiv 1 \mod 4 \\ p \mid n}} (v_p(n)+1)}{2} \right\rceil$$

The scary number inside the product is the number of divisors of n if we delete all powers of 2 and primes which are 3 mod 4 from its factorization.

First, it is well known that if $p \mid a^2 + b^2$ and $p \equiv 3 \mod 4$, $p \mid a$ and $p \mid b$, so we can assume n is not divisible by any primes congruent to 3 mod 4. Next, we show that the number of ways to write $2n$ as a sum of squares equals the number of ways to write n as a sum of squares by constructing a bijection between the sets of solutions. Indeed, if $n = a^2 + b^2$, $2n = (a+b)^2 + (a-b)^2$, or equivalently if $2n = a^2 + b^2$, $n = (\frac{a+b}{2})^2 + (\frac{a-b}{2})^2$. So indeed, if (a, b) satisfies $a^2 + b^2 = n$ we obtain the pair of solutions $(\frac{a+b}{2}, \frac{a-b}{2})$, the sum of squares of which is n, and the other way with $(a+b; a-b)$, meaning we can also assume n is odd.

Now, for any prime divisor p of n (which only has divisors of the form $4k+1$), let $p = z_p\overline{z_p}$ where z_p and $\overline{z_p}$ are Gaussian primes. Using the factoring trick we obtain:

$$\prod_{\substack{p \equiv 1 \mod 4 \\ p \mid n}} (z_p\overline{z_p})^{v_p(n)} = (a+bi)(a-bi)$$

Now, we focus on the $a+bi$ factor. For any prime divisor z_p denote $v_{z_p}(a+bi)$ to be the largest exponent at which z_p divides $a+bi$. Then, clearly $v_{\overline{z_p}}(a-bi) = v_{z_p}(a+bi)$. Thus, if $v_{z_p}(a+bi) = x$, $v_{\overline{z_p}}(a+bi) = v_p(n) - x$. So our freedom of choice is not that big. We can pick the exponent of z_p (in $v_p(n)+1$ ways) for each prime, and the exponent of $\overline{z_p}$ is automatically picked, and then we can multiply the result by a unit (i. e. by i, -1, $-i$ or 1) so we get the answer to be 4 times the exponent of each prime plus one.

4.2 Useful Facts about Gaussian Integers

The following are general properties of the Gaussian integers. Proving these, even tho is not hard, is outside the scope of this article.

- **Bezout's Theorem:** For any Gaussian integers a and b there exist Gaussian x and y such that $ax + by = \gcd(a, b)$
- **Remainders:** For any Gaussian a and b there exists a remainder r and a quotient q such that $a = bq + r$ and the absolute value of q is at most half the absolute value of b.
- **Modular inverses:** divisibility $b \mid ax - 1$ has a solution if and only if a and b are coprime.

4.3 Other Extensions of $\mathbb{Z}$

In the same way we defined $\mathbb{Z}[i]$, we can define $\mathbb{Z}[\sqrt{-d}]$ for any natural d to be the set of numbers of the form $a + b\sqrt{-d}$ for integer a and b. (In fact, we can also work with $\mathbb{Z}[\sqrt{d}]$ for positive d, but it has infinitely many units and a few other problems). It is known that $\mathbb{Z}[\sqrt{-d}]$ is a Unique Factorization Domain (meaning that it carries out the same properties of $\mathbb{Z}$ as $\mathbb{Z}[i]$) only for

$$d \in \{1,\ 2,\ 3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163\}$$

So we can nicely factor expressions of the form $a^2 + db^2$ for any d from the list above. In fact, in olympiad problems, except $\mathbb{Z}[i]$, the only ones which naturally appear are $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{-3}]$, so it is not necessary to remember all the numbers. Let's now see an example problem.

Problem 2. *Brazil Olympic Revenge 2023 P2*
Find all triples (*a*,*b*,*n*) of positive integers such that $a^3 = b^2 + 2^n$

Solution: First, we solve the case when b is odd in two parts:

a) b **is odd and** n **is even**
$a^3 = b^2 + 2^n$ factors out as $a^3 = (b + 2^{\frac{n}{2}}i)(b - 2^{\frac{n}{2}}i)$. This is very similar to Problem 0, and indeed, we can show both brackets are coprime. If g is the greatest common divisor of the brackets, then the absolute value of g squared divides the absolute value of each bracket squared, which is $b^2 + 2^n$, which is odd. Also, g divides the difference of the two terms which is $(b+2^{\frac{n}{2}}i) - (b-2^{\frac{n}{2}}i) = 2^{\frac{n}{2}+1}i$. Thus, $|g|^2$ divides $|2^{\frac{n}{2}+1}i|^2$, so $|g|^2$ is a power of 2, but as $|g|^2$ is odd it is in fact 1, so g is a unit.
Now, as in Problem 0, let $b+2^{\frac{n}{2}}i = (u+vi)^3 = u^3 - 3uv^2 + (3u^2v - v^3)i$. $u^3 - 3uv^3 = b$ means that u is odd and v is even. $v(3u^2 - v^2) = 2^{\frac{n}{2}}$ means that v is of the form 2^m of -2^m for some natural m.
If $v = 2^m$, we get that $3u^2 - 4^m$ is a power of 2 also, but as it is odd, $3u^2 - 4^m = 1$, which fails by mod 3.
If $v = -2^m$, $3u^2 = 4^m - 1$, meaning that $m = 1$ by mod 8. So $b + 2^{\frac{n}{2}}i = (u + vi)^3 = (1 - 2i)^3$ or $(-1 - 2i)^3$, giving the only solution $(a, b, n) = (5, 11, 2)$.

b) b **is odd and** n **is odd**
We can't factor the equation in $\mathbb{Z}[i]$, but instead we can try our new tool. Rewrite the equation as $a^3 = (b + 2^{\frac{n-1}{2}}\sqrt{-2})(b - 2^{\frac{n-1}{2}}\sqrt{-2})$. Let g be the greatest common divisor of the brackets in $\mathbb{Z}[\sqrt{-2}]$. In the same way as in the first case, the absolute value of g squared divides $b^2 + 2^n$, which is again odd, and in the same way it divides the absolute value of

$$(b + 2^{\frac{n-1}{2}}\sqrt{-2}) - (b - 2^{\frac{n-1}{2}}\sqrt{-2})$$

, which is a power of 2, so g is a unit (note that as i and $-i$ are not in $\mathbb{Z}[\sqrt{-2}]$ the only units are 1

and -1). Denote $\frac{n-1}{2}$ by k. Let

$$b + 2^k\sqrt{-2} = (x + y\sqrt{-2})^3 = x^3 - 6xy^2 + (3x^2y - 2y^3)\sqrt{-2}$$

. Since b is odd, it follows that x must also be odd. Therefore, the expression $3x^2 - 2y^3$ is odd as well. In particular, this implies $k = 0$, and we are left with the equation $3x^2y - 2y^3 = 1$, the only integer solutions of which are $y = 1$ and $x = \pm 1$.

Because $b > 0$, we must take $x = -1$, which leads to $b = 5$. Substituting back, we get $a = 3$, and obtain the solution $(a, b, n) = (3, 5, 1)$.

Now we are left to deal with b being even. We aim to show that b is divisible by 8, which would allow us to jump to a smaller solution of the equation. We again have 3 cases:

c) $v_2(b) = 1$

Clearly, a is even. Let $x = \frac{a}{2}$, $y = \frac{b}{2}$. The equation becomes $2x^3 = y^2 + 2^{n-2}$, immediately implying that $n = 2$, so $2x^3 = y^2 + 1$. We work in $\mathbb{Z}[i]$ again. $2x^3 = (y + i)(y - i)$. This time, however, the brackets are not compulsory coprime. Again, take g to be their greatest common divisor. The absolute value of g squared also divides a power of 2, but also divides $y^2 + 1$, which is 2 mod 4. So the absolute value of g squared is either 1 or 2, so it is either a unit, or $(1 + i)$ multiplied by a unit. If the numbers are coprime, as in integers, one of them must be a perfect cube so we either have $y + i = (u + vi)^3$ or $i - y = (m + ni)^3$. The first case was already solved in Problem 0, and the second one is the exact same, just that y is negative. Just for completeness we solve

$$i - y = (m + ni)^3 = m^3 - 3mn^2 + (3m^2n - n^3)i$$

Clearly, as n divides 1 it is either 1 or -1. $n = 1$ would imply $3m^2 = 2$ and $n = -1$ gives $y = 0$ which does not fit.

More interesting is the case when $g = 1 + i$. Then we get that:

$$y + i = (u + vi)^3(1 + i) = \left(u^3 - 3u^2v - 3uv^2 + v^3\right) + i\left(u^3 + 3u^2v - 3uv^2 - v^3\right)$$

Here, we observe that: $u^3 + 3u^2v - 3uv^2 - v^3 = (u - v)(u^2 + 4uv + v^2)$, so we are again only left with two cases:

$$u - v = u^2 + 4uv + v^2 = 1 \text{ or } u - v = u^2 + 4uv + v^2 = -1$$

Both of them are quadratic equations, solving which only yields the solution $(x, y) = (1, 1)$ or $(a, b, n) = (2, 2, 2)$.

d) $v_2(b) = 2$

If $n = 3$ this gives $a^3 = 1 + 2(\frac{b}{4})^2$, to solve which we again need to work in $\mathbb{Z}[\sqrt{-2}]$. Again, let $c = \frac{b}{4}$, so $a^3 = (1 + c\sqrt{-2})(1 - c\sqrt{-2})$. As above, the absolute value of the greatest common divisor

of the two brackets squared divides a power of 2 and an odd number, so the brackets are coprime. For the final time in this problem, let

$$(1 + c\sqrt{-2}) = (m + n\sqrt{-2})^3 = (m^3 - 6mn^2) + \sqrt{-2}(3m^2n - 2n^3)$$

. Again, m is 1 or -1 and we get no solutions.

If $n \geq 4$ we get that a is divisible by 4, and a contradiction mod 4.

e) $v_2(b) \geq 3$

Clearly by mod 4, $n \geq 5$ so wo conclude that $v_2(a) \geq 2$ so $n \geq 6$. Thus, we can jump from the solution (a, b, n) to $(\frac{a}{4}; \frac{b}{8}, n - 6)$. So each of the solutions is either one of the three triples, or obtained from them by the operation above.

Finally, (a, b, n) is one of $(2^{2x+1}, 2^{3x+1}, 6x + 2)$; $(3 \cdot 2^{2x}, 5 \cdot 2^{3x}, 6x + 1)$; $(5 \cdot 2^{2x}, 11 \cdot 2^{3x}, 6x + 2)$, where x is an arbitrary nonnegative integer.

4.4 Roots of Unity and Cyclotomic Polynomials

The n-th roots of unity are the n complex roots of $x^n = 1$, and the primitive roots are the roots to $x^n = 1$ which do not satisfy $x^m = 1$ for any m less than n. They have the form $e^{\frac{2k\pi i}{n}} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$, for k being coprime to n. We now introduce the cyclotomic polynomials:
Let $\Phi_n(x) = \prod(x - \zeta_i)$, where ζ_i are the n-th primitive roots of unity. It can be rewritten as $\Phi_n(x) = \prod(x - e^{2\pi i \frac{k}{n}})$, where the product runs through all $k \leq n$ such that k and n are coprime.
It turns out these polynomials have a lot of good properties, which we will not proof here, as it would take too long.

- **Integer coefficients:** Monic polynomials have only integer coefficients, which read the same from left to right and from right to left unless it is the first polynomial.
- **Irreducibility:** Any cyclotomic polynomials are irreducible.
- **Product:** $\prod_{d|n} \Phi_d(x) = x^n - 1$
- **Degree:** $\deg \Phi_n(x) = \varphi(n)$, which is the number of numbers less than or equal to n which are coprime to n.
- **Powers:** If a, n are positive integers and $\gcd(a, n) = 1$, we have $\Phi_n(x^a) = \prod_{d|a} \Phi_{nd}(x)$.
- **Relation with divisors:** Let n be a positive integer and p a prime number. Then, if $p \mid n$ we have $\Phi_{np}(x) = \Phi_n(x^p)$. If $p \nmid n$ we have $\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$, and as a corrolary if n is an odd integer, we have $\Phi_{2n}(x) = \Phi_n(-x)$.

- **Mobius Inversion:** The cyclotomic polynomial can be expressed as: $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$, where the exponent is the Mobius Function.
- **Bound:** Using the Mobius Inversion Formula for the polynomial, for $n \in \mathbb{Z}_{>1}$, $S \cdot n^{\varphi(r)} \leq \Phi_r(n) \leq \frac{1}{S} \cdot n^{\varphi(r)}$, where $S = \prod_{m=1}^{\infty}(1 - n^{-m})$.
- **gcd:** The greatest common divisor of $\Phi_n(x)$ and $\Phi_m(x)$ for $n < m$ can be a power of a prime number p^x if $\frac{m}{n} = p^\alpha$ for some natural α, and is 1 otherwise.
- **Key Property:** If a prime p satisfies $p|\Phi_n(x)$ for some integer x, than $p \mid n$ or $p \equiv 1 \mod n$.

This is the list of the first 12 cyclotomic polynomials:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1 \\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1 \\
\Phi_{11}(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_{12}(x) &= x^4 - x^2 + 1
\end{aligned}$$

Let's now solve the first example problem:

Problem 1. *IMSC 2025 Number Theory MOCK P3*
Find all positive integers n such that:

$$1 + 2 + \cdots + 2^n \mid (1 + 2)(1 + 2^2) \ldots (1 + 2^n) - 1$$

Solution: The answer is all n such that $n + 1$ is an odd prime. First, we show that all such n satisfy, by proving the following key claim.

Claim: $\Phi_n(x)$ divides $(1 + x)(1 + x^2) \ldots (1 + x^{n-1}) - 1$, as polynomials.

It is clear that the divisibility is $\mathbb{R}[x]$ would imply divisibility in $\mathbb{Z}[x]$, as the cyclotomic polynomial is monic and the other one has integer coefficients. Thus, it is enough to prove that any root of the cyclotomic polynomial is a root of the polynomial we want to be divisible by. Let ω be a primitive n-th root of unity. We must show $(1 + \omega)(1 + \omega^2) \ldots (1 + \omega^{n-1}) = 1$. The easiest way to prove it is

by applying $1+x=\frac{x^2-1}{x-1}$ to all terms of the product. Tnus, we need to prove:

$$(\omega-1)(\omega^2-1)\dots(\omega^{n-1}-1)=(\omega^2-1)(\omega^4-1)\dots(\omega^{2n-2}-1)$$

However this is clear as both sides equal $\prod(\omega_i-1)$ where ω_i are all n-th roots of unity except 1. This was enough to show that $n+1$ primes work, let us now show the other side.
First, clearly n must be even, as otherwise the left side, which equals $2^{n+1}-1$, would be divisible by 3, but the right side can't be. Now, let d be a divisor of $n+1$, and consider a prime divisor p of 2^d-1 modulo which the order of 2 is d, that exists by Zsigmondy's theorem, unless $d=6$, which is not possible as $n+1$ is odd. We see that by the claim we proved, $(1+2^{dk+1})(1+2^{dk+2})\dots(1+2^{dk+d-1})\equiv 1 \mod p$. Thus, repeatedly using this property we get that p divides $2^{\frac{n+1}{d}-1}-1$, however taking q to be the smallest prime divisor of $n+1$ and $d=\frac{n+1}{q}$, we obtain that the order of q which is $\frac{n+1}{q}$ divides $q-1$ which is not possible as $\frac{n+1}{q}>q-1$.

Now we will exhibit the idea behind proving the very useful Zsigmondy's Theorem. This is not a rigurous proof as we use some of the properties exposed in the beggining without proof. The way we prove it can be extended to integers easily also implies the result with a^n+b^n instead of a^n-b^n

Problem 2. *Zsigmondy's Theorem*
Let $a>b>0$ be coprime positive integers. Then for any integer $n>1$, there exists a prime number p such that

$$p \mid a^n-b^n \quad \text{and} \quad p \nmid a^k-b^k \ \text{ for all } \ 1\le k<n.$$

With the following exceptions:

- $a+b$ is a power of 2 and $n=2$.
- $(a,b,n)=(2,1,6)$

Solution: Consider the adaptation of the cyclotomic polynomials for two variables:

$$\Phi_d(a,b)=b^{\varphi(d)}\Phi_d(\frac{a}{b})$$

Call a divisor new if it divides a^n-b^n and no a^k-b^k for $k<n$, and old otherwise. Consider an n such that a^n-b^n has no new divisors. Assume $n\ge 3$, as else the solution is straightforward. The main property that still holds is: $\prod_{d|n}\Phi_d(a,b)=a^n-b^n$. Now, take a prime p dividing $\Phi_n(a,b)$. It must divide $a^k-b^k=\prod_{d|k}\Phi_d(a,b)$ for some $k<n$. Let x_p be the smallest number such that $\Phi_{x_p}(a,b)$ is divisible by p. By the gcd property in the beginning, we must have $n=p^\alpha x_p$. Clearly, $x_p\le p-1$ as $p \mid a^{p-1}-b^{p-1}$. By the form of n and as $p>x_p$, p is the largest prime divisor of n, meaning p is unique. So if there exists some prime dividing $\Phi_n(a,b)$, it is unique. Also,

$$p|\frac{a^n-b^n}{a^{\frac{n}{p}}-b^{\frac{n}{p}}}, \ \text{ but by Lifting the Exponent Lemma } \ v_p(\frac{a^n-b^n}{a^{\frac{n}{p}}-b^{\frac{n}{p}}})\le 1$$

If p is odd. If $p = 2$, n is a power of 2, and in this case either $n = 2$ or $a^{\frac{n}{2}} + b^{\frac{n}{2}}$ is a sum of squares so is 2 mod 4. Anyways, we get that there is at most one prime dividing $Phi_n(a, b)$. Let us now solve 2 cases:
$a)\Phi_n(a, b) = 1$.

In this case, by triangle inequality $|a - \zeta b| \geq |a| - |\zeta b| = |a| - |b|$ for a root of unity ζ. So:

$$|\Phi_n(a,b)| = |\prod_{(i;n)=1}(a - \zeta_i b)| \geq \prod_{(i;n)=1}(|a| - |\zeta_i b|) = \prod_{(i;n)=1}(|a| - |b|) = (a-b)^{\varphi(n)}$$

Where the product is taken through all primitive roots of unity ζ_i. It is only left to recall the triangle inequality equality case, that is: $|a| + |b| = |a + b|$ if and only if $\frac{a}{b} \in \mathbb{R}_+$ or one of a and b is zero, which means that there is no equality if $n > 1$. In the same way we can prove $\Phi_n(a, b) \leq (a+b)^{\varphi(n)}$, which we will use for the other case.

$a)\Phi_n(a, b) = p$ for some prime p.

Clearly, $a - b = 1$ as else the inequality applied above would again finish. If $a - b = 1$, write $n = p^\alpha x_p$ as before. If $\alpha \geq 2$ then

$$p \geq \Phi_n(a,b) = \Phi_{px_p}\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right) \geq \left(a^{p^{\alpha-1}} - b^{p^{\alpha-1}}\right)^{\varphi(px_p)} \geq a^p - b^p = pb^{p-1} + \cdots + 1$$

where in the last = sign we used Newton's Binomial for $(b+1)^p - b^p$. Thus $\alpha = 1$, so $n = px_p$ and the inequality rewrites as:

$$p \geq \Phi_n(a,b) = \frac{\Phi_{x_p}(a^p, b^p)}{\Phi_{x_p}(a,b)} \geq \left(\frac{a^p - b^p}{a+b}\right)^{\varphi(x_p)} \geq \frac{\sum_{i=1}^{b}((i+1)^p - i^p)}{a+b} \geq \frac{b(2^p-1)}{2b+1} \geq \frac{2^p-1}{3}.$$

And for the last inequality to hold, we need $p \leq 3$ for which we can find $a = 2$, thus $b = 1$.

4.5 Polynomial Divisibility and a Divisibility Lemma

In what follows, we exhibit a lemma which is not hard to prove, neither to understand, or to apply, but is frequently met in all types of contests. **Lemma:** If $a_1, a_2 \ldots a_p$ is a complete residue class modulo a prime p, meaning that all a_i are distinct mod p than $x^{a_1} + x^{a_2} + \ldots x^{a_p}$ is divisible by $x^{p-1} + x^{p-2} + \cdots + x + 1$. The proof is also rather easy. Consider a root ζ of $\zeta^p - 1$ which is not 1, and it is clear that:

$$\sum_{i=1}^{p} \zeta^{a_i} = \sum_{i=0}^{p-1} \zeta^i = 0$$

Let's see the lemma in action:

Problem 1. *Moldova TST 2022 P1*
Show that for every integer $n \geq 2$, the number

$$a = n^{5n-1} + n^{5n-2} + n^{5n-3} + n + 1$$

is a composite number.

Solution: Observe that the exponents leave distinct residues modulo 5 so by our lemma $x^{5n-1} + x^{5n-2} + x^{5n-3} + x + 1$ is divisible by $x^4 + x^3 + x^2 + x + 1$. And if $x = n$, they are clearly not equal, so the number is composite.

The following problem has a solution that is hard to motivate. A reasonable way to get the idea is to try to see when $x + 1$ and $x^2 + 1$ are factors.

Problem 2. *Moldova TST 2019 P5*
Let $n, \in \mathbb{N}^*, n \geq 3$ Prove that the polynomial $f(x) = \frac{X^{2^n-1}-1}{X-1} - X^n$ has a divisor of form $X^p + 1$ where $p \in \mathbb{N}^*$

Solution:
Consider $g(x) = x^{2^{v_2(n+1)}} + 1$. We will show that it divides the given polynomial. Indeed, it is again enough to prove $g(x)$ divides $f(x)$ in $\mathbb{R}(x)$ as g is monic. For a root r of $g(x)$, $r^{2^n-1} = \frac{1}{r}$ so $\frac{r^{2^n-1}-1}{r-1} = \frac{-1}{r}$ and in the same way $r^n = \frac{-1}{r}$, so r is also a root of this polynomial.

4.6 Problems to Work on

- **Lebesgue** Show that the equation $x^n - 1 = y^2$ has no solutions for $n > 1$ except $(1, 0)$.
- **Folklore** Parameterize the solutions of the equation $a^2 + b^2 = c^3$ for coprime a and b.
- **Folklore** Parameterize the solutions of the equation $a^2 + b^2 = c^2$ for coprime a and b.
- **BMO 1998** Solve in integers $x^2 + 4 = y^5$.
- **RMM 2023 N1** Let n be a positive integer. Let S be a set of ordered pairs (x, y) such that $1 \leq x \leq n$ and $0 \leq y \leq n$ in each pair, and there are no pairs (a, b) and (c, d) of different elements in S such that $a^2 + b^2$ divides both $ac + bd$ and $ad - bc$. In terms of n, determine the size of the largest possible set S.
- **St.Petersburg, P4 Grade 11, 2013** Find all pairs (p, q) of prime numbers, such that $2p - 1$, $2q - 1$, $2pq - 1$ are perfect squares.

5 Bibliography

The articles listed in the bibliography are not necessarily sources of direct inspiration for the authors, nor do most of them contain problems identical or closely related to those presented in this handout. The primary purpose for which they are mentioned is to provide readers with additional explanations and perspectives on the general topics discussed herein, should further clarification be needed. The references are arranged in order of increasing difficulty.

References

[1] R. Earl, *Complex Numbers*, 2004.
Provides a clear and accessible introduction to the concept of complex numbers.

[2] stuck, *Roots of Unity Filter*, 2008.
Explains the roots of unity filter in a concise and comprehensible manner.

[3] A. Kessler, *Complex Numbers*, 2009.
Serves as a good continuation of the introductory material, familiarizing the reader with standard notations and operations.

[4] K. Conrad, *The Gaussian Integers*.
Offers a well-structured introduction to the Gaussian integers and their basic properties.

[5] L. Sun, *Cyclotomic Polynomials in Olympiad Number Theory*, 2013.
Presents the key properties of cyclotomic polynomials and provides intuitive, proof-oriented explanations relevant to Olympiad number theory.

[6] PISOLVE, *The Zsigmondy Theorem*, 2011.
Contains a detailed proof of Zsigmondy's theorem along with several related training problems.