Algebraic number theory

Michael Luo

17 May 2026

Notes on algebraic number theory, focusing on cyclotomic polynomials. Prerequisites: basic modular arithmetic, orders, and finite fields.

Written for the last Math + Science Club lecture of the 2025–26 school year. Includes a particularly instructive proof that cyclotomic polynomials are irreducible.

Contents

§1 Motivation

Let $f(\theta) = \cos(\theta)\cos(2\theta)\cos(4\theta)$. You might already know the following.

Fact 1.1 (Morrie's law)**.** $f(20^\circ) = \frac{1}{8}$.

The proof of this is quite pretty: by three applications of sine double angle, we have

$$\begin{aligned}\cos(20^\circ)\cos(40^\circ)\cos(80^\circ) &= \frac{1}{\sin(20^\circ)}\sin(20^\circ)\cos(20^\circ)\cos(40^\circ)\cos(80^\circ)\\ &= \frac{1}{2}\cdot\frac{1}{\sin(20^\circ)}\sin(40^\circ)\cos(40^\circ)\cos(80^\circ)\\ &= \frac{1}{4}\cdot\frac{1}{\sin(20^\circ)}\sin(80^\circ)\cos(80^\circ)\\ &= \frac{1}{8}\cdot\frac{1}{\sin(20^\circ)}\sin(160^\circ)\\ &= \frac{1}{8}.\end{aligned}$$

Similarly, one can show

$$f(100^\circ) = f(140^\circ) = \frac{1}{8}.$$

Why do 20°, 100°, and 140° give the same values? Of course, the same argument works, but *why*?

We will answer this question by developing some basic algebraic number theory.

§2 Rings and fields

We'll need some basic abstract algebra. I promise it's useful.

Roughly, a field is a set where you can add, subtract, multiply, and divide (except by zero). A ring is a set where you can add, subtract, and multiply. For example, $\mathbb{Q}$, $\mathbb{C}$, and $\mathbb{Z}/67\mathbb{Z}$ are fields, and $\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$ are rings but not fields, since in both rings, you can't divide by 2 — $\frac{1}{2}$ is defined in neither $\mathbb{Z}$ nor $\mathbb{Z}/12\mathbb{Z}$. (However, $\frac{1}{2}$ is defined in $\mathbb{Z}/67\mathbb{Z}$: it's 34, since $2\cdot 34 \equiv 1 \pmod{67}$.)

If this doesn't make sense, here's the actual definition.

Definition 2.1. A *ring* is a set R along with two binary operations $R^2 \to R$, *addition* and *multiplication*, written $+$ and $\cdot$, respectively, such that the following hold:

- Addition and multiplication are commutative and associative.
- There exist two elements 0 and 1 such that $a + 0 = a$ and $a \cdot 1 = a$ for all $a \in R$.
- For any $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.
- For any $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

We often omit the multiplication symbol, writing ab instead of $a \cdot b$.

A *field* k is a ring where $0 \neq 1$ and for all $a \neq 0$, there exists $a^{-1} \in k$ such that $a \cdot a^{-1} = 1$.

Some authors say rings don't have to have commutative multiplication, instead calling what we just defined above "commutative rings." These people work with weird things like quaternions.

We can make rings from rings! For a ring R, let $R[x]$ be the smallest ring containing x. For example, $\mathbb{Z}[x]$ is the set of polynomials in x with integer coefficients, and

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

For a field K, let $K(x)$ be the smallest field containing x. For example, $\mathbb{Q}(x)$ is the set of quotients of polynomials with rational coefficients, and

$$\mathbb{Q}(\sqrt{3}) = \mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}.$$

Exercise 2.2. Verify $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}[\sqrt{3}]$ as above by showing $\mathbb{Q}[\sqrt{3}]$ is a field. You'll need to show $\frac{1}{\alpha} \in \mathbb{Q}[\sqrt{3}]$ for any $\alpha \in \mathbb{Q}[\sqrt{3}]$.

§3 Algebraic numbers

Definition 3.1. A number α is an *algebraic number* if it is a root of some polynomial P with rational coefficients. A number α is an *algebraic integer* if it is a root of some monic polynomial P with integer coefficients.

Here are some examples.

- The numbers 5, $\sqrt{3}$ and $67i$ are algebraic integers, since they are roots of the polynomials $x - 5$, $x^2 - 3$, and $x^2 + 67^2$, respectively.
- The numbers $\frac{1}{2}$ and $\sqrt{\frac{6}{7}}$ are algebraic numbers, but not algebraic integers. They are roots of the polynomials $x - \frac{1}{2}$ and $7x^2 - 6$, respectively.
- The numbers π and e are not algebraic numbers, since they are not the root of any polynomial with rational coefficients. (They are still the root of the polynomials $x - \pi$ and $x - e$, though.) These numbers are called *transcendental*.

The set of algebraic numbers is denoted $\overline{\mathbb{Q}}$, and the set of algebraic integers is denoted $\overline{\mathbb{Z}}$. It is a fact that $\overline{\mathbb{Q}}$ is a field and $\overline{\mathbb{Z}}$ is a ring. That means the sum and product of two algebraic integers (resp. numbers) is an algebraic integer (resp. number), and the reciprocal of a nonzero algebraic number is an algebraic number.

We will now introduce the incredibly useful concept of a minimal polynomial.

Theorem 3.2 (Existence and uniqueness of minimal polynomial)

For an algebraic number α, there exists a unique polynomial (up to scaling) P_α of minimal degree such that $P_\alpha(\alpha) = 0$.

This P_α is called the *minimal polynomial* of α. The *degree* of α is the degree of P_α. For example, $P_{\sqrt{3}}(x) = x^2 - 3$.

As α is algebraic, some P_α of minimal degree exists. We need to prove P_α is unique. We will need the following.

Lemma 3.3

Suppose $P(\alpha) = 0$. Then $P_\alpha \mid P$.

Proof. By the division algorithm, let $P = qP_\alpha + r$ for polynomials q and r where $\deg r < \deg P_\alpha$. Plugging in α yields $0 = r(\alpha)$. Along with $\deg r < \deg P_\alpha$, this implies r is the zero polynomial. □

Now if there were two minimal polynomials P_α and Q_α, then $P_\alpha \mid Q_\alpha$, and $Q_\alpha \mid P_\alpha$. Yet this implies P_α and Q_α are constant multiples of each other, so the minimal polynomial is unique up to scaling.

Another fact about minimal polynomials is that they are irreducible.

Theorem 3.4

Let α be an algebraic number. If $P(\alpha) = 0$, then P is the minimal polynomial of α if and only if P is irreducible.

Proof. First suppose P is the minimal polynomial of α. If $P = AB$ where $\deg A, \deg B < \deg P$, then $A(\alpha) = 0$ or $B(\alpha) = 0$. But P is minimal, impossible.

Now suppose P is irreducible. Then $P_\alpha \mid P$, implying P_α is a constant multiple of P. □

In Exercise 2.2, we saw that by "rationalizing denominators," $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}[\sqrt{3}]$, since $\mathbb{Q}[\sqrt{3}]$ is a field. In general, the following is true.

Theorem 3.5

The ring $\mathbb{Q}[\alpha]$ is a field for any algebraic number α.

I'll justify this intuitively. I claim that the ring $\mathbb{Q}[\alpha]$ can be thought of as the set $\mathbb{Q}[x]/(P_\alpha(x))$. For example, $\mathbb{Q}[\sqrt{3}]$ can be thought of as $\mathbb{Q}[x]/(x^2-3)$. Wait, what does this notation mean? You know how $\mathbb{Z}/(5)$ is the integers modulo 5? In the same way, $\mathbb{Q}[x]/(x^2-3)$ is the set of polynomials with coefficients in $\mathbb{Q}$, "modulo x^2-3." This means we can add and subtract multiples of x^2-3 at will. For example, in $\mathbb{Q}[x]/(x^2-3)$, we may compute

$$x^3 = x^3 - x(x^2-3) = 3x.$$

Why is this the same concept as above? This is best explained with an example. Look at these two parallel calculations: the left is $\mathbb{Q}(\sqrt{3})$, and the right is $\mathbb{Q}[x]/(x^2-3)$.

$$\begin{aligned} &(3+\sqrt{3})(1-\sqrt{3}) \\ &= 3 - 2\sqrt{3} - \sqrt{3}^2 \\ &= 3 - 2\sqrt{3} - \sqrt{3}^2 + (\sqrt{3}^2 - 3) \\ &= -2\sqrt{3} \end{aligned} \qquad \begin{aligned} &(3+x)(1-x) \\ &= 3 - 2x - x^2 \\ &= 3 - 2x - x^2 + (x^2-3) \\ &= -2x. \end{aligned}$$

As you can see, x acts like $\sqrt{3}$. For the experienced reader, the relevant buzzword sequence is that there's an isomorphism $\mathbb{Q}(\sqrt{3}) \to \mathbb{Q}[x]/(x^2-3)$ given by $1 \mapsto 1$ and $\sqrt{3} \mapsto x$.

Now let me convince you that $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(P_\alpha(x))$ is a field. Note that $\mathbb{Z}/(5)$ is a field, since 5 is prime. Similarly, $P_\alpha(x)$ is "prime" in $\mathbb{Q}[x]$, as it's an irreducible polynomial. Therefore, $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(P_\alpha(x))$ is a field, just like $\mathbb{Z}/(5)$ is a field.

Remark. The above commentary was adapted from my handout "Demystifying finite fields."

Exercise 3.6. Show that an algebraic number α is an algebraic integer iff when P_α is scaled to be monic, it has integer coefficients.

The roots of P_α are called the *Galois conjugates* of α. A good general intuition to have is that it's often good to think of an algebraic number α in terms of its minimal polynomial P_α and its Galois conjugates. More bluntly, α is useless by itself. Bring in its brothers and sisters — its Galois conjugates — to fight with it.

Here are a few examples of Galois conjugates.

- The Galois conjugate of $\frac{6}{7}$ is $\frac{6}{7}$.
- The Galois conjugates of $6+\sqrt{7}i$ are $6\pm\sqrt{7}i$.
- The Galois conjugates of $\sqrt{2}$ and $\sqrt{3}$ are $\pm\sqrt{2}$ and $\pm\sqrt{3}$. The Galois conjugates of $\sqrt{2}-\sqrt{3}$ are $-\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, and $\sqrt{2}+\sqrt{3}$.
- The Galois conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, where ω is a primitive third root of unity.

With the language of algebraic numbers and integers, we can now begin to discuss cyclotomic polynomials.

§4 Cyclotomic polynomials

Some review: some complex number ζ is a *root of unity* if there exists some n such that $\zeta^n = 1$. The smallest such n is called the *order* of ζ, and ζ is called a *primitive nth root of unity*.

Definition 4.1. The nth cyclotomic polynomial Φ_n is the monic polynomial whose roots are the nth primitive roots of unity.

First of all, we have the following identity.

Proposition 4.2

For all $n \geq 1$,

$$\prod_{d|n} \Phi_d(x) = x^n - 1,$$

where the product is taken over divisors d of n.

This holds since both sides are monic polynomials whose roots are the nth roots of unity — every nth root of unity is a primitive dth root of unity for exactly one d dividing n. As shown in Figure 1, each 12th root of unity is either a primitive 1st, 2nd, 3rd, 4th, 6th, or 12th root of unity. Hence

$$x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x).$$

Proposition 4.2 allows us to compute the cyclotomic polynomials recursively via $\Phi_1(x) = x - 1$ and

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} \Phi_d(x)}.$$

Let's use this to compute the first 10 cyclotomic polynomials.

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1
\end{aligned}$$

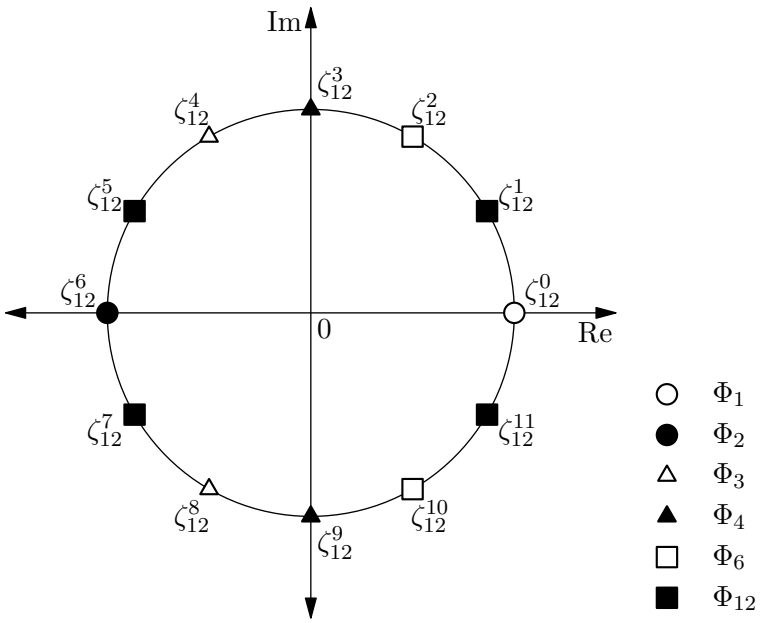


Figure 1: The 12th roots of unity. As shown, each 12th root of unity is either a primitive 1st, 2nd, 3rd, 4th, 6th, or 12th root of unity.

$$\begin{aligned}
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1 \\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1.
\end{aligned}$$

Here are some observations:

- The degree of the polynomial Φ_n is $\varphi(n)$, since that's the number of primitive nth roots of unity.
- The polynomial Φ_n is a *palindrome*: $\Phi_n(x) = x^{\varphi(n)}\Phi_n(x^{-1})$. Try proving this yourself.
- The coefficients of Φ_n seem to be in $\{-1, 0, 1\}$. Unfortunately, this is false: the x^7 and x^{41}-coefficients of Φ_{105} are -2. However, Φ_n always has integer coefficients.

  Here's a sketch: we claim that if P is a monic polynomial with integer coefficients and $P = AB$ is a factorization of P where A is a monic polynomial with integer coefficients, then B is a monic polynomial with integer coefficients. This is proved by backward induction on the coefficients of B. Now apply this claim inductively using $P(x) = x^n - 1$, $A(x) = \prod_{d|n, d<n} \Phi_d(x)$, and $B(x) = \Phi_n(x)$.
- The polynomial Φ_n is irreducible, which we will prove here.

Theorem 4.3

Cyclotomic polynomials are irreducible.

We present a proof due to Schur from https://www.lehigh.edu/~shw2/c-poly/several_proofs.pdf.

Proof. We will prove the following equivalent claim.

> **Claim** — Let n be a positive integer and $P, Q \in \mathbb{Z}[x]$ be polynomials such that $P(x)Q(x) = x^n - 1$. Then for all roots ζ of P and primes p not dividing n, ζ^p is a root of P as well.

Why is this claim sufficient? First, we'll need to invoke the following sledgehammer.

> **Theorem 4.4** (Dirichlet's theorem)
> There are infinitely many primes $p \equiv a \pmod{n}$ as long as $\gcd(a, n) = 1$.

This is hard to prove, but it is pretty intuitive. It would be really dumb if there were only, like, five $8 \pmod{13}$ primes. In particular, there is at least one prime p congruent to $a \pmod{n}$ for each a with $\gcd(a, n) = 1$.

If cyclotomic polynomials are irreducible, that means if a divisor P of $x^n - 1$ has a root at any primitive dth root of unity, P has a root at all $\varphi(d)$ primitive dth roots of unity. In the language of Figure 1, if P has one root of some shape, it must have all the roots of that shape. In the language of *The Three Musketeers*, "all for one and one for all." In the language of Chinese, 如果圆分多项式是不可约的，那么这意味着：若$x^n - 1$ 的一个因子P 在某个d 次本原单位根处有根，那么P 在所有$\varphi(d)$ 个d 次本原单位根处都有根.

> **Remark.** This joke was inspired by the excellent YouTube channel Sheafification of G.

Look at Figure 1. By Dirichlet's theorem, there is some prime p congruent to $a \pmod{n}$ for all a with $\gcd(a, n) = 1$. For any nth root of unity ζ, the roots of unity of the form ζ^p for primes p not dividing n are exactly those of the same shape as ζ — the ones with the same order.[1]

For example, take $n = 12$ and $\zeta := \zeta_{12}^5$. By Dirichlet's theorem, there are primes $p_1 \equiv 1 \pmod{12}$, $p_5 \equiv 5 \pmod{12}$, $p_7 \equiv 7 \pmod{12}$, and $p_{11} \equiv 11 \pmod{12}$. If ζ is a root of P, then $\zeta^{p_1} = \zeta_{12}^5$, $\zeta^{p_5} = \zeta_{12}^1$, $\zeta^{p_7} = \zeta_{12}^{11}$, and $\zeta^{p_{11}} = \zeta_{12}^7$ are all roots of P as well. These are exactly the primitive 12th roots of unity: if P has one primitive 12th root of unity as a root, all of them are roots of P. This is the "all for one and one for all" claim we described earlier.

Now we will actually prove the above claim. For algebraic integers d and n, we say d *divides* n as algebraic integers if $\frac{n}{d}$ is an algebraic integer. First, we will show the discriminant Δ of $x^n - 1$ is $\pm n^n$ for some choice of sign.

> **Remark** (Wait, what's the discriminant?)**.** You probably think the discriminant Δ of a quadratic $P(x) = ax^2 + bx + c$ is $b^2 - 4ac$. WRONG! In this handout, we use the convention that the discriminant of a polynomial P with roots $r_1, \ldots, r_n$ is
> $$\prod_{i<j} (r_i - r_j)^2.$$

[1] For the experienced reader, the action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on the set of dth primitive roots of unity with $d \mid n$ by $\zeta \mapsto \zeta^p$ is transitive. This is since the group of nth roots of unity is isomorphic to the cyclic group of order n, and the action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on $\mathbb{Z}/n\mathbb{Z}$ by multiplication has orbits $\{a \mid \gcd(a, n) = d\}$ for each $d \mid n$.

So the discriminant of a quadratic $P(x) = a(x - r_1)(x - r_2) = ax^2 + bx + c$ is actually

$$(r_1 - r_2)^2 = (r_1 + r_2)^2 - 4r_1r_2 = \frac{b^2 - 4ac}{a^2}.$$

We compute

$$\begin{aligned}
\Delta &= \prod_{i<j}(\zeta_n^i - \zeta_n^j)^2 \\
&= \pm\prod_{i\neq j}(\zeta_n^i - \zeta_n^j) \\
&= \pm\prod_{i\neq j}\zeta_n^i(1 - \zeta_n^{j-i}) \\
&= \pm\prod_{i}\zeta_n^{i(n-1)}\prod_{d\neq 0}(1 - \zeta_n^d) \\
&= \pm\zeta_n^{(n-1)^2n/2}\prod_{i} n \\
&= \pm n^n,
\end{aligned}$$

where index variables are assumed to run over $\{0, 1, \ldots, n-1\}$.

Now let P and Q be as in the claim. As $x^n - 1$ is monic, P and Q are either both monic or both have leading coefficient -1. Without loss of generality, suppose P and Q are both monic. Since the roots of P are a subset of those of $x^n - 1$, we have $P(x) = (x - \xi_1)\ldots(x - \xi_k)$ for some distinct nth roots of unity $\xi_1, \ldots, \xi_k$.

Now suppose by way of contradiction $P(\zeta) = 0$ but $P(\zeta^p) \neq 0$ for some prime $p \nmid n$. Then the quotient of $\Delta = \prod_{i<j}(\zeta_n^i - \zeta_n^j)^2$ with

$$P(\zeta^p) = (\zeta^p - \xi_1)\ldots(\zeta^p - \xi_k)$$

is an algebraic integer, since it is the product of differences of nth roots of unity, and the sum and product of algebraic integers is an algebraic integer. Hence $P(\zeta^p)$ divides Δ.

For a ring R, let its characteristic $\operatorname{char}(R)$ be the smallest positive integer n such that $n = 0$. (Here, n is defined as $1 + \cdots + 1$, where there are n ones and 1 is the multiplicative identity.) If no such n exists, we say $\operatorname{char}(R) = 0$. Examples of characteristic 0 rings include $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}[x]/(6x - 7)$. The rings $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ and $\mathbb{F}_{p^2}$ have characteristic p, while the ring $\mathbb{Z}/p^2\mathbb{Z}$ has characteristic p^2.

Let p be a prime and suppose R is a ring of characteristic p. Observe that R has a copy of $\mathbb{F}_p$ inside it formed by $\{0, \ldots, p-1\}$. Let $\sigma : R \to R$ be the Frobenius endomorphism defined by $\sigma(r) = r^p$ for all $r \in R$. From "Demystifying finite fields," $\sigma(P(x)) = P(\sigma(x))$ for any $P \in \mathbb{F}_p[x]$ in any finite field with characteristic p. Similarly, in R, $\sigma(P(x)) = P(\sigma(x))$. (The proof is exactly the same.)

Now the ring $R := \overline{\mathbb{Z}}/p\overline{\mathbb{Z}}$ has characteristic p, hence $P(\zeta^p) = P(\zeta)^p$ in R. But $P(\zeta) = 0$ by assumption, so $P(\zeta^p) = 0$ in R, implying p divides $P(\zeta^p)$ as algebraic integers. So this would imply $p \mid P(\zeta^p) \mid \Delta = \pm n^n$. But this is impossible since by assumption $p \nmid n$, so $\frac{n^n}{p}$ is not an algebraic integer! So we're finally done. □

Since cyclotomic polynomials are irreducible, this implies Φ_n is the minimal polynomial of the primitive nth roots of unity. So the Galois conjugates of a primitive nth root of unity are all the primitive nth roots of unity, and a primitive nth root of unity has degree $\deg \Phi_n = \varphi(n)$.

Now we can finally resolve the mystery of Morrie's law from Section 1. If

$$f(\theta) = \cos(\theta)\cos(2\theta)\cos(4\theta),$$

we may apply the multiple-angle identities for cos to write

$$f(\theta) = g(\cos(\theta))$$

for some degree-7 polynomial g. Explicitly,

$$\cos(2\theta) = 2\cos^2(\theta) - 1 \quad \text{and} \quad \cos(4\theta) = 2(2\cos^2(\theta) - 1)^2 - 1,$$

so

$$g(x) = x(2x^2 - 1)(2(2x^2 - 1)^2 - 1).$$

We have $g(\cos(20^\circ)) = \frac{1}{8}$, and we want to know why $g(\cos(100^\circ)) = g(\cos(140^\circ)) = \frac{1}{8}$ as well.

We claim the minimal polynomial of $\cos(20^\circ)$ is $P(x) := 4x^3 - 3x - \frac{1}{2}$. First, observe that $\cos(20^\circ)$ is a root of P, as

$$P(\cos(20^\circ)) = 4\cos^3(20^\circ) - 3\cos(20^\circ) - \frac{1}{2} = \cos(60^\circ) - \frac{1}{2} = 0,$$

by the triple-angle identity $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$. Similarly, $\cos(100^\circ)$ and $\cos(140^\circ)$ are roots of P, as

$$P(\cos(100^\circ)) = \cos(300^\circ) - \frac{1}{2} = 0 \quad \text{and} \quad P(\cos(140^\circ)) = \cos(420^\circ) - \frac{1}{2} = 0.$$

Now there are two ways to observe that P is the minimal polynomial of $\cos(20^\circ)$. The first is specialized to this case, while the second is more general.

- Observe that the roots of P, which are $\cos(20^\circ)$, $\cos(100^\circ)$, and $\cos(140^\circ)$, are all irrational. If a cubic has no rational roots, it is irreducible. Hence P is irreducible and hence the minimal polynomial of $\cos(20^\circ)$.
- Let $\zeta = \operatorname{cis}(20^\circ)$. Then as ζ is a primitive 18th root of unity, it has degree $\varphi(18) = 6$. Now $\cos(20^\circ) = \frac{1}{2}(\zeta + \zeta^{-1})$. As $P(\cos(20^\circ)) = P(\frac{1}{2}(\zeta + \zeta^{-1})) = 0$, we have

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

  Fully expanding and multiplying by ζ^3, we see ζ is the root of some degree-6 polynomial with rational coefficients. This is fine, since the degree of ζ is 6, but if instead the minimal polynomial $P_{\cos(20^\circ)}$ had a smaller degree $d < 3$, plugging $\cos(20^\circ) = \frac{1}{2}(\zeta + \zeta^{-1})$ would show ζ is the root of some degree-$2d$ polynomial with rational coefficients. Yet the degree of ζ is 6, so this is impossible.

Now consider the polynomial $h(x) := g(x) - \frac{1}{8}$. Since h has rational coefficients and has $\cos(20^\circ)$ as a root, $P(x) \mid h(x)$. Now this implies the other roots of P are roots of h as well, so $h(\cos(100^\circ)) = h(\cos(140^\circ)) = 0$. So $f(100^\circ) = f(140^\circ) = \frac{1}{8}$, as desired!

Exercise 4.5 (ARML 2025/I8)**.** The polynomial f has integer coefficients, and

$$f(\sqrt{20} + \sqrt{2} + 5) = 2025.$$

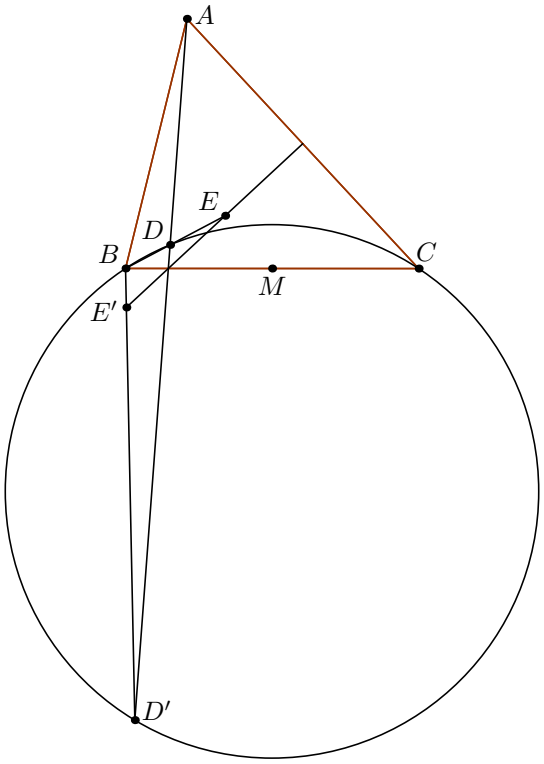
Compute the least possible positive value of $f(1)$.

§5 Geometry

We end with a surprising application to geometry. Consider the following problem.

Problem 5.1 (USAMO 2024/5)**.** Point D is selected inside acute $\triangle ABC$ so that $\angle DAC = \angle ACB$ and $\angle BDC = 90^\circ + \angle BAC$. Point E is chosen on ray BD so that $AE = EC$. Let M be the midpoint of BC.

Show that line AB is tangent to the circumcircle of triangle BEM.



The condition that $\angle DAC = \angle ACB$ encodes that D lies on some line ℓ, and the condition that $\angle BDC = 90^\circ + \angle BAC$ encodes that D lies on some circle Γ. The intersection of this line and this circle determines two points: D (inside $\triangle ABC$) and D' (outside $\triangle ABC$). Let E and E' be the intersections of lines BD and BD' with the perpendicular bisector of $\overline{AC}$.

Looking at the diagram, one sees that not only is (BEM) tangent to line AB, but $(BE'M)$ is as well! Why?

We will complex bash. Let (ABC) be the unit circle and let a, b, and c be the free variables. The line ℓ has the form $\overline{A}z + A\overline{z} + B = 0$ for some $A, B \in \mathbb{Q}(a, b, c)$ with $A \neq 0$.[2] The circle Γ has the form $z\overline{z} - \overline{C}z - C\overline{z} + D = 0$, for $C, D \in \mathbb{Q}(a, b, c)$. Substituting the formula for $\overline{z}$ from the equation for ℓ into the equation for Γ yields $P(z) = 0$ for some quadratic $P \in \mathbb{Q}(a, b, c)[z]$. The roots of this quadratic are the points d and d'.

Take for granted that P is irreducible over $\mathbb{Q}(a, b, c)$. So P is the minimal polynomial of d over $\mathbb{Q}(a, b, c)$, and d cannot be expressed as a rational function in a, b, and c.

Since the problem is true, line AB is tangent to circle (BEM). Since e is a function of d, this can be stated in terms of complex numbers as $Q(d) = 0$ for some polynomial $Q \in \mathbb{Q}(a, b, c)[x]$ (since $a, b, m \in \mathbb{Q}(a, b, c)$). As P is the minimal polynomial of d, we have $P \mid Q$. Since P has d' as a root, Q has d' as a root as well. So the problem is true if D was replaced with D', as desired!

[2] Here, $\mathbb{Q}(a, b, c)$ denotes the field of rational functions in a, b, and c.