Mathematics Enrichment - Complex Numbers, Roots of 1 and Cyclotomic Polynomials

**Foundations**

Notation: $\boxed{e^{i\alpha} = \cos\alpha + i\sin\alpha}$ where $i$ is a complex number,$i^2 = -1$.

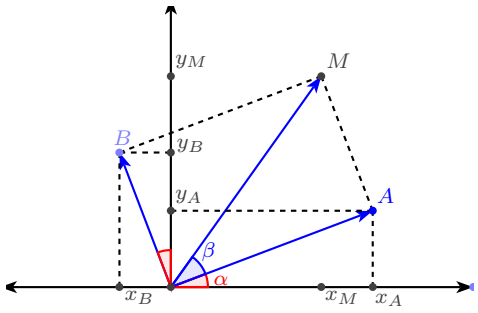
1) Properties: $\boxed{e^{i(\alpha+\beta)} = e^{i\alpha}e^{i\beta}}$ and hence $\boxed{e^{in\alpha} = (e^{i\alpha})^n}$.

The first property is equivalent to the formulae

$\boxed{\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta}$ and $\boxed{\sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta}$,

which can be proven using the diagram below as follows: Assume $|OM| = 1$.

a) Prove that the coordinates of $A$ are $(x_A, y_A) = (\cos\alpha\cos\beta, \sin\alpha\cos\beta)$.
b) Prove that the coordinates of $B$ are $(x_B, y_B) = (-\sin\alpha\sin\beta, \cos\alpha\sin\beta)$.
c) Prove that the coordinates of $M$ are $(x_M, y_M) = (x_A + x_B, y_A + y_B)$.




2) The roots of the polynomial $X^n - 1$ are of the form $e^{\frac{2\pi ik}{n}}$ with $k \in \{0, 1, ..., n-1\}$. These are also called $n$-th roots of unity. Thus

$$\boxed{X^n - 1 = \prod_{k=0}^{n-1}(X - e^{\frac{2\pi ik}{n}}) = \prod_{k=0}^{n-1}(X - \xi_n^k), \text{ where } \xi_n = e^{\frac{2\pi i}{n}}}.$$

3) The $n$-th roots of unity $e^{\frac{2\pi ik}{n}}$ such that $\gcd(k, n) = 1$ are called *primitive*. There are $\varphi(n)$ such roots. Define

$$\boxed{\Phi_n(X) := \prod_{k\ ;\ \gcd(k,n)=1}(X - e^{\frac{2\pi ik}{n}})},$$

the $n$-th cyclotomic polynomial.

a) Prove: $\prod_{k;\gcd(k,n)=a}(X - e^{\frac{2\pi ik}{n}})$ is a cyclotomic polynomial.
b) Prove: $\boxed{n = \sum_{d|n}\varphi(d)}$ and $\boxed{X^n - 1 = \prod_{d|n}\Phi_d(X)}$.

4) $\Phi_n(X)$ is irreducible as a polynomial with integer coefficients.

Let $P(X)$ be any polynomial with integer coefficients. Then

$$\Phi_n(X)|P(X) \Longleftrightarrow P(\xi_n) = 0, \text{ where } \xi_n = e^{\frac{2\pi i}{n}}.$$

**Problems**

Q1. Use the factorizations of the polynomials $X^n - 1$ to calculate the cyclotomic polynomials $\Phi_n(X)$ for $n \in \{1, 2, ..., 14\}$.

Q2. Let $p$ be an odd prime and $k$ be a positive integer. Calculate each of the following, and write them in polynomial form:

$$\text{(i) } \Phi_p(X); \quad \text{(ii) } \Phi_{2p}(X); \quad \text{(iii) } \Phi_{p^k}(X).$$

Q3. Let $p$ be a prime $p \neq 3$. Prove the following formula for $\Phi_{3p}(X)$ and use it to write each of $\Phi_{15}(X)$, $\Phi_{21}(X)$, $\Phi_{33}(X)$ in polynomial form.

$$\Phi_{3p}(X) = \frac{X^{2p} + X^p + 1}{X^2 + X + 1}.$$

Q4. Let $p$ be a prime and $n, k$ positive integers.

- If $p|n$, prove that $\Phi_{pn}(X) = \Phi_n(X^p)$. More generally, $\Phi_{p^k n}(X) = \Phi_n(X^{p^k})$.
- If $\gcd(p, n) = 1$, prove that $\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}$ and $\Phi_{p^k n}(X) = \frac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})}$.

If $n$ is an odd integer, we have $\Phi_{2n}(x) = \Phi_n(-x)$.

Q5. Write each of the following polynomials as a product of polynomials:

a) $X^4 + X^2 + 1$;
b) $X^{10} + X^5 + 1$.
c) $X^{10} - X^5 + 1$.
d) $X^8 + X^6 + X^4 + X^2 + 1$.

Q6. (BMO). Prove that there are no prime numbers in the infinite sequence

$$10001, 100010001, 1000100010001, ...$$

Q7. (WOOT). Let $n$ be a positive integer. Prove that the number

$$2^{2^n} + 2^{2^{n-1}} + 1$$

can expressed as the product of no less than $n$ prime factors (not necessarily different).

Q8. Prove that $\Phi_n(X)$ is a symmetric polynomial, i.e. the coefficients found at equal distance from the middle are equal.

Q9. Given positive integers $a_1 < ... < a_n$, consider the polynomials $P(X) = \prod_{i>j}(X^{a_i - a_j} - 1)$ and $Q(X) = \prod_{i>j}(X^{i-j} - 1)$. By factorising into cyclotomic polynomials, prove that $Q(X)$ divides $P(X)$. Conclude that $\prod_{i<j} \frac{a_i - a_j}{i-j}$ is always an integer.

Q10. Let $\xi$ be an $n$-th primitive root of 1. In what follows, $i$ and $j$ take all values in the set $\{0, 1, .., n-1\}$. Define $\Delta := \prod_{i<j}(\xi^i - \xi^j)^2 = \pm \prod_{i \neq j}(\xi^i - \xi^j)$. Prove that $\Delta = \pm n^n$.