This week, we shall discuss an important family of polynomials and their applications in algebra and number theory.

Recall that a complex number \( \xi \) is said to be a primitive \( n \)th root of 1, if \( \xi^n = 1 \), and \( \xi^k \neq 1 \) for \( 1 \leq k < n \). The \( n \)th cyclotomic polynomial \( \Phi_n(x) \) is the polynomial in \( \mathbb{C}[x] \) with leading coefficient 1 whose roots (with multiplicity 1) are all primitive \( n \)th roots of 1.

**Example.** We have \( \Phi_1(x) = x - 1 \), \( \Phi_2(x) = x + 1 \), \( \Phi_3(x) = x^2 + x + 1 = \frac{x^3 - 1}{x - 1} \), \( \Phi_4(x) = x^2 + 1 \).

Primitive \( n \)th roots of 1 are complex numbers of the form \( e^{\frac{2\pi ki}{n}} \), where \( 0 \leq k \neq n - 1 \) and \( \gcd(k, n) = 1 \). Clearly, the number of such \( k \) is equal to \( \phi(n) \), the number of positive integers not exceeding \( n \) and coprime to \( n \). We proved earlier in class that \( \sum_{d \mid n} \phi(d) = n \). In the similar fashion, we shall now prove a generalisation of this statement, namely we shall show that

\[
\prod_{d \mid n} \Phi_d(x) = x^n - 1.
\]

(It is a generalisation, since comparing the degrees of polynomials on the left and on the right, we see that \( \sum_{d \mid n} \phi(d) = n \)). Indeed, each root of the polynomial on the right is a complex number of the form \( e^{\frac{2\pi ki}{n}} \), where \( 0 \leq k \neq n - 1 \). If we bring the fraction \( \frac{k}{n} \) to lowest term, we shall get a primitive root of the degree equal to the denominator (which is a divisor of \( n \), and all primitive roots for all divisors appear like that.

The formula we just proved implies the following result.

**Lemma.** Cyclotomic polynomials have integer coefficients: \( \Phi_n(x) \in \mathbb{Z}[x] \) for all \( n \).

**Proof.** Induction on \( n \): if for all \( m < n \) the polynomials \( \Phi_m(x) \) have integer coefficients, then clearly

\[
\Phi_n(x) = \frac{x^n - 1}{\prod_{d \mid n, d < n} \Phi_d(x)}
\]

has integer coefficients as well. \( \square \)

Let us now prove a result on cyclotomic polynomials that is important for Galois theory.

**Theorem 1.** For each \( n \geq 1 \), the cyclotomic polynomial \( \Phi_n(x) \) is irreducible in \( \mathbb{Z}[x] \).

**Proof.** Let us show that this theorem can be deduced from the following statement (and then prove that statement):

Let \( g(x) \) be an irreducible divisor of \( \Phi_n(x) \) in \( \mathbb{Z}[x] \), and let \( \zeta \) be a complex root of \( g(x) \). Then for each prime \( p \) with \( \gcd(n, p) = 1 \), the complex number \( \zeta^p \) is also a root of \( g(x) \).

How to deduce the theorem from this statement? Let us take \( \zeta_0 = e^{\frac{2\pi i}{n}} \), it is clearly a primitive \( n \)th root of 1, so \( \zeta_0 \) is a root of \( \Phi_n(x) \), hence it is a root of some irreducible divisor \( g(x) \) of \( \Phi_n(x) \) in \( \mathbb{Z}[x] \). By the statement above, for any \( p_1 \) not dividing \( n \), the complex number \( \zeta_1 = \zeta_0^{p_1} \) is also a
root of $g(x)$. Furthermore, by the same statement, for any $p_2$ not dividing $n$, the complex number $\zeta_2 = \zeta_1^{p_2} = e^{\frac{2\pi i p_2}{n}}$ is also a root of $g(x)$, etc., so for any collection of (not necessarily different) primes $p_1, p_2, \ldots, p_k$ not dividing $n$, the complex number $\zeta_0 = e^{\frac{2\pi i p_1 p_2 \cdots p_k}{n}}$ is also a root of $g(x)$. But all primitive $n$th roots of 1 are of the form $\zeta_n^k$ with $\gcd(k, n) = 1$, so all primitive $n$th roots of 1 are roots of $g(x)$, and $g(x) = \Phi_n(x)$.

It remains to prove the statement above. Let $\Phi_n(x) = g(x)h(x)$, where $g(x)$ is irreducible according to our assumption. Suppose that the statement in question does not hold, so $\zeta$ is a root of $h(x)$. (Note that since $p$ does not divide $n$, the complex number $\zeta$ is a primitive $n$th root of 1). Thus, $\zeta$ is a root of the polynomial $h(x^p)$, so $g(x)$ and $h(x^p)$ have common divisors, therefore $h(x^p)$ is divisible by $g(x)$ since $g(x)$ is irreducible. Let us now consider all polynomials modulo $p$, and denote, for each polynomial $a(x)$, by $[a(x)]$ the same polynomial when considered in $\mathbb{F}_p[x]$. It is important to recall that $[h(x^p)] = [h(x)p] = [h(x)]^p$, because $h(x^p) \equiv (h(x))^p \pmod{p}$ [which relies on the Fermat’s Little Theorem $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{F}_p$, and the property $(a + b)^p \equiv a^p + b^p \pmod{p}$ following from the fact that all the binomial coefficients $\binom{p}{k}$ are divisible by $p$ for $0 < k < p$]. Let $[g_1(x)]$ be some irreducible divisor of $[g(x)]$ modulo $p$ (although $g(x)$ is irreducible in $\mathbb{Z}[x]$, we cannot be sure that it remains irreducible modulo $p$). Then $[h(x^p)] = [h(x)]^p$ is divisible by $[g_1(x)]$, hence is divisible by $g_1(x)$, so since $\mathbb{F}_p[x]$ is a UFD, we conclude that $[h(x)]$ is divisible by $g_1(x)$. Therefore, $[\Phi_n(x)] = [g(x)][h(x)]$ is divisible by $g_1(x)^2$, so $[x^n - 1]$ is divisible by $g_1(x)^2$. A polynomial is divisible by a square of another polynomial must have common divisors with its derivative (which is clear if we compute the derivative using the product rule), but the derivative of $x^n - 1$ is $nx^{n-1}$. Since $n$ is not divisible by $p$, the only factors of $[nx^{n-1}]$ are powers of $[x]$, which are not divisors of $[x^n - 1]$. The contradiction completes the proof.

Our next goal is to demonstrate how to use cyclotomic polynomials to prove the following result (a particular case of the celebrated Dirichlet’s theorem):

**Theorem 2.** For every integer $n$, there exist infinitely many primes $p \equiv 1 \pmod{n}$.

**Proof.** At the core of the proof of this theorem is the following statement

For every integer $n$, there exist a integer $A > 0$ such that all prime divisors $p > A$ of values of $\Phi_n(c)$ at integer points $c$ are congruent to 1 modulo $n$. In other words, prime divisors of values of the $n$th cyclotomic polynomial either are “small” or are congruent to 1 modulo $n$.

Let us explain how to use this statement to prove Theorem 2. Assume that there are only finitely many primes congruent to 1 modulo $n$; let $p_1, \ldots, p_m$ be those primes. Let us consider the number $c = Ap_1 p_2 \cdots p_m$. The number $k = \Phi_n(c)$ is relatively prime to $c$ (since $\Phi_n(x)$ divides $x^n - 1$, the constant term of $\Phi_n(x)$ divides the constant term of $x^n - 1$ and is hence equal to $\pm 1$ for every $n$), so it is not divisible by any of the primes $p_1, \ldots, p_m$, and has no divisors $d \leq A$ either. This almost guarantees that we can find a new prime congruent to 1 modulo $n$: take any prime divisor $p$ of $k$, and Lemma ensures that $p \equiv 1 \pmod{n}$. The only problem that may occur is that $k = \pm 1$, so it has no prime divisors. In this case, replace $c$ by $Nc$ for $N$ large enough, so that $Nc$ is greater than all the roots of the equation $\Phi_n(x) = 1$, with everything else remaining the same.

It remains to prove the statement we formulated. Let us consider the polynomial $f(x) = (x - 1)(x^2 - 1) \ldots (x^{n-1} - 1)$. The polynomials $f(x)$ and $\Phi_n(x)$ have no common roots, so their gcd in $\mathbb{Q}[x]$ is equal to 1, hence $a(x)f(x) + b(x)\Phi_n(x) = 1$ for some $a(x), b(x) \in \mathbb{Q}[x]$. Let $A$ denote the common denominator of all coefficients of $a(x)$ and $b(x)$. Then for $p(x) = Aa(x), q(x) = Ab(x)$ we have $p(x)f(x) + q(x)\Phi_n(x) = A$, and $p(x), q(x) \in \mathbb{Z}[x]$. Assume that a prime number $p > A$ divides $\Phi_n(c)$ for some $c$. Then $c$ is a root of $\Phi_n(x)$ modulo $p$, and consequently, $c^p \equiv 1 \pmod{p}$. Let us notice that $n$ is the order of $c$ modulo $p$. Indeed, if $c^k \equiv 1 \pmod{p}$ for some $k < n$, then $c$ is a
root of \( f(x) \) modulo \( p \), but the equality \( p(x)f(x) + q(x)\Phi_n(x) = A \) shows that \( f(x) \) and \( \Phi_n(x) \) are relatively prime modulo \( p \). Recall that \( c^{p-1} \equiv 1 \pmod{p} \) by Fermat’s Little Theorem, so \( p - 1 \) is divisible by \( n \), the order of \( c \), that is \( p \equiv 1 \pmod{n} \), and the lemma is proved.

Remark. Most available proofs of Theorem 2 that use cyclotomic polynomials use a different proof of Lemma. The main point that is being made by our proof is that it seems to accumulate the key ideas of elementary number theory: the Euclidean algorithm and its applications, the relationship between \( \mathbb{Q}[x] \) and \( \mathbb{Z}[x] \), the techniques based on the reduction modulo \( p \), and the multiplicative group of integers modulo \( p \) (through Fermat’s Little Theorem).

Let us outline another application of cyclotomic polynomials, Wedderburn’s Little Theorem.

Theorem 3. Every finite division ring is commutative.

By a ring we mean a set \( R \) with two operations (sum and product) satisfying the usual axioms. The product does not have to be commutative, e.g. square matrices of the given size form a ring, and quaternions form a ring too. By a division ring we mean a ring where every nonzero element is invertible, e.g. quaternions. Thus, the theorem states that if \( R \) is a finite division ring, then it in fact is a field.

Let us recall several definitions from ring theory that we need in this proof.

For a ring \( R \), its centre \( Z(R) \) consists of all elements that commute with all elements from \( R \):

\[
Z(R) = \{ z \in R : zr = rz \text{ for all } r \in R \}.
\]

The centre of a ring is closed under sum and product, and so forms a subring of \( R \). If \( R \) is a division ring, then \( Z(R) \) is a field, and \( R \) is a vector space over this field.

More generally, if \( S \subset R \), the centraliser of \( S \) is defined as the set of all elements that commute with all elements from \( S \):

\[
C_S(R) = \{ z \in R : zs = sz \text{ for all } s \in S \}.
\]

The centraliser of every subset is a subring of \( R \), and in the case of a division ring, a field. Clearly, \( C_R(R) = Z(R) \).

The last ingredient of the proof we need is the class formula for finite groups. Let \( G \) be a finite groups. For \( g \in G \), denote by \( C(g) \) the conjugacy class of \( g \), that is the set of all elements of the form \( h^{-1}gh \), where \( h \in G \). Then \( G \) is a disjoint union of conjugacy classes. We have \( \#C(g) = \frac{\#G}{\#C_g} \), where \( C_g \) is the centraliser subgroup (consisting, as in the case of rings, of all elements that commute with \( g \)).

Proof. Our goal is to prove that \( Z(R) = R \). Let \( q = \#Z(R) \). Since \( R \) is a vector space over \( Z(R) \), we have \( \#R = q^n \), where \( n \) is the dimension of this vector space. Since \( R \) is a division ring, the set \( G = R \setminus \{0\} \) is a group. Applying the class formula to this group, we obtain

\[
q^n - 1 = \sum_{\text{conjugacy classes}} \#C(g) = \sum_{\text{conjugacy classes}} \frac{q^n - 1}{\#C_g}.
\]

Let us look closer at this sum. It contains terms corresponding to conjugacy classes consisting of a single element (these are conjugacy classes of nonzero elements from the centre) and all other conjugacy classes. Every centraliser \( C_g \) of such a conjugacy class, with the zero element adjoined to it, forms a subring of \( R \) containing \( Z(R) \), that is a vector space over \( Z(R) \). Let \( n_g \) be the dimension of that vector space, \( n_g < n \). We have

\[
q^n - 1 = q - 1 + \sum_{\text{non-central conjugacy classes}} \frac{q^n - 1}{q^{n_g} - 1}.
\]
It is easy to see that $\frac{q^n-1}{\phi(q^n-1)}$ is an integer only if $n_q$ divides $n$ (and that in general $\gcd(q^n-1,q^k-1) = q^{\gcd(n,k)} - 1$), so in fact not only $\frac{q^n-1}{\phi(q^n-1)}$ is an integer but also $\frac{x^n-1}{\phi(x^n-1)}$ is a polynomial with integer coefficients. As polynomials in $x$, $x^{n_q} - 1$ and $\Phi_n(x)$ are coprime, so $x^n - 1$ is divisible by their product. This means that in our equality above all terms except for the term $q - 1$ are divisible by $\Phi_n(q)$. Thus $q - 1$ is divisible by $\Phi_n(q)$. But the latter is impossible for $n > 1$: $|q - \eta| > |q - 1|$ for all roots of unity $\eta \neq 1$, so $|\Phi_n(q)| = \prod_{\eta} |q - \eta| > |q - 1|$. This completes the proof. □