TWO APPLICATIONS OF CYCLOTOMIC POLYNOMIALS

VLADIMIR DOTSENKO

Background

The n^{th} cyclotomic polynomial $\Phi_n(x)$ is defined as $\prod_\eta (x-\eta)$, where η runs over all primitive n^{th} roots of 1. Previously in class, we proved that this polynomial has integer coefficients and is irreducible over integers. It is also worth noting that 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 ± 1 for every n.

Dirichlet's theorem for primes $p \equiv 1 \pmod n$

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

The proof of this theorem relies on the following

Lemma. *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 Lemma to prove Theorem 1. 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 $c = A!p_1p_2\cdots p_m$. The number $k = \Phi_n(c)$ is relatively prime to c (since the constant term of Φ_n is ± 1), so it is not divisible by any of the primes $p_1, \ldots, p_m$, and has no divisors $d \le A$ 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 k by Nk for N large enough, so that Nk is greater than all the roots of the equation $\Phi_n(x) = \pm 1$, with everything else remaining the same.

Proof of Lemma. 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, $c^n \equiv 1 \pmod p$. 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 1 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).

Theorem 2. *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:

$$Z(R) = \{z \in R\colon zr = rz \text{ for all } r \in R\}.$$

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:

$$C_S(R) = \{z \in R\colon zs = sz \text{ for all } s \in S\}.$$

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 of Theorem 2. 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

$$q^n - 1 = q - 1 + \sum_{\substack{\text{non-central} \\ \text{conjugacy classes}}} \frac{q^n - 1}{q^{n_g} - 1}.$$

It is easy to see that $\frac{q^n-1}{q^{n_g}-1}$ is an integer only if n_g divides n (and that in general $\gcd(q^n - 1, q^k - 1) = q^{\gcd(n,k)} - 1$), so in fact not only $\frac{q^n-1}{q^{n_g}-1}$ is an integer but also $\frac{x^n-1}{x^{n_g}-1}$ is a polynomial with integer coefficients. As polynomials in x, $x^{n_g} - 1$ 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.

Remark. Irreducibility of cyclotomic polynomials, while of crucial importance for Galois Theory, is not really used in our proofs at all (contrary to what I might made you believe in class).