Cyclotomic Polynomials in Olympiad Number Theory

Lawrence Sun*
lala-sun@hotmail.com

February 17, 2013

Abstract

This is a paper discussing the powerful applications cyclotomic polynomials have in olympiad number theory. We first go over much of the theory, and then we prove the gigantic Zsigmondy's Theorem. Then we proceed to destroy a few olympiad problems.

*Thank you to Victor Reis for proofreading much of this article and Evan Chen for cleaning up the LaTeX.

Contents

1 Pre-Introduction

1.1 How to Best Use this Paper

I'll admit, cyclotomic polynomials are not the most useful things in the world. They are extremely interesting but can only be applied to destroy a medium subset of problems unlike other methods such as SoS which are applicable in many situations. They are unlike some topics where a firm understanding of the theory is not required to use them. In addition, the theory involved in cyclotomic polynomials is debatably much more complicated. The main gain from learning about cyclotomic polynomials is the intuition gained from their structure. Because of this, simply memorizing all the theorems is **strongly** discouraged. I would recommend the reader to try proving all the theorems inside this article first before glancing at the proofs given. Discovering the proof yourself will give you a more firm understanding of a concept than any proof given by anybody.

1.2 Some Motivation

Nothing is complete without some motivation. So we'll try to motivate the definition of a cyclotomic polynomial. It is well known that if ω denotes a nontrivial cubic root of unity then we have $\omega^2+\omega+1=0$. Thus the polynomial x^2+x+1 has a root at both the nontrivial cubic roots of unity. We also note that this polynomial is *irreducible*, i.e. that it cannot be factored into two nonconstant polynomials with integer coefficients. Thus it is the *minimal* polynomial of the nontrivial cubic root of unity, because it is the minimum degree integer polynomial which has ω as a root (can you prove that $P(x)$ is the minimal polynomial of α iff $P(x)$ is irreducible given $P(\alpha)=0$?)

Now let's move onto the fourth roots of unity. Let's define $\omega_n = \exp\left(\frac{2\pi i}{n}\right)$. Now note that $\omega_4 = i$. So what polynomial has a root at i? Due to the identity $i^2+1=0$, we have x^2+1 has a root at ω_4. It is easy to verify this polynomial is irreducible as well.

Now, are these polynomials interesting in any way? Is there a formula to generate them? It turns out they are *very* interesting and there do exist formulas to generate them, though admittedly they are not the easiest formulas to use in the world. We will be exploring these polynomials extensively throughout this article.

1.3 Notation

In this section we define notation that may not be familiar to the average Olympiad problem solver and are not defined anywhere else in the article.

- $\mathbb{Z}[x]$ denotes the set of polynomials with integer coefficients. In general, $R[x]$ denotes the same thing except with coefficients in the set R.
- $\mathbb{Q}[\omega_n]$ denotes the set of values which result from taking an arbitrary polynomial with rational coefficients and plugging in ω_n.
- $\mathbb{Z}_p$ denotes the set of remainders of integers taken modulo p, i.e. $0, 1, ..., p-1$.

2 Basics of Cyclotomic Polynomials

2.1 Definition

We shall define the notion of a *cyclotomic polynomial* very soon. However, first we must investigate the examples we did earlier a little more into how to construct them. Notice that the polynomial for 4 had a root at ω_4^1, ω_4^3 but not ω_4^2 or ω_4^4. Why is this the case? Perhaps its because $\gcd(1,4) = \gcd(3,4) = 1$ and $\gcd(2,4), \gcd(4,4) \neq 1$. Further small cases will yield similar analysis, that the minimal polynomial has a root at ω_n^k iff $\gcd(k,n) = 1$. This motivates us to define:

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \omega_n^k)$$

where we are denoting $\Phi_n(x)$ to be the n^{th} cyclotomic polynomial. Note that this definition is equivalent to defining $\Phi_n(x)$ to be the monic polynomial whose roots are all the roots of unity whose least positive power that equals 1 is n. To get a feeling of these, one can find $\Phi_1(x) = x-1, \Phi_2(x) = x+1, \Phi_3(x) = x^2+x+1, \Phi_4(x) = x^2+1, \Phi_5(x) = x^4+x^3+x^2+x+1$. This sequence seems highly random, however it turns out each term means quite a bit.

2.2 Basic Theorems

Theorem 2.1. *For any positive integer n we have* $\deg \Phi_n(x) = \varphi(n)$.

Proof. This follows almost directly from the definition of the phi function. □

Theorem 2.2. *For any positive integer n we have* $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Proof. This is simply a root counting argument. Remark that $x^n - 1 = (x - \omega_n)(x - \omega_n^2) \cdots (x - \omega_n^n)$.

Now, consider a term $x - \omega_n^k$. Let $g = \gcd(n,k)$. Then it is not hard to see ω_n^k is a root of $\Phi_{n/g}(x)$ because ω_n^k is a n/g^{th} primitive root of unity.

Thus it quickly follows each $x - \omega_n^k$ on the LHS shows up on the RHS.

Now to show no $x - \omega_n^k$ shows up twice on the RHS. Luckily, this is trivial because based on the definition of $\Phi_m(x)$ we have z is a root iff z is a primitive m^{th} root of unity.

As no number can be a primitive a^{th} and b^{th} root of unity at the same time when $a \neq b$, we are done. □

This gives us a general formula for the n^{th} cyclotomic polynomial. Unfortunately it is very hard to use, however using this we will prove more results which are more useful.

Corollary 2.3. *For any positive integer n we have* $\sum_{d|n} \varphi(d) = n$.

Theorem 2.4. *For any positive integer we have $\Phi_n(x) \in \mathbb{Z}[x]$. That is, $\Phi_n(x)$ is a polynomial with integer coefficients.*

Proof. We proceed by induction. As $\Phi_1(x) = x - 1$, the base case of $n = 1$ is clearly true.

Now suppose for all $k < n$ we have $\Phi_k(x)$ is a polynomial with integer coefficients. We want to show then that $\Phi_n(x)$ is as well. Define

$$P_n(x) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x).$$

By the inductive hypothesis we have $P_n(x)$ is a polynomial with integer coefficients. Clearly P_n is monic. Thus by the division algorithm we know there exists integer polynomials Q, R such that:

$$x^n - 1 = P_n(x)Q(x) + R(x)$$

where $\deg R < \deg P_n$ or $R(x) = 0$. Now plug in the $n - \varphi(n)$ roots of $P_n(x)$ into the above equation. It is easy to see $R(x)$ has at least $n - \varphi(n)$ roots.

But then if R is nonzero, it has degree at least $n - \varphi(n)$. As $\deg P_n(x) = n - \varphi(n)$, we get a contradiction as $\deg R < \deg P$. Thus $R(x) = 0$ everywhere and thus $x^n - 1 = P_n(x)Q(x)$.

Remark that we know $x^n - 1 = P_n(x)\Phi_n(x)$. It immediately follows $Q(x) = \Phi_n(x)$, and thus $\Phi_n(x)$ is an integer polynomial as desired. □

Remark. One can also provide a proof by showing $\gcd(x^n - 1, x^m - 1) = x^{\gcd(n,m)} - 1$ and then directly applying **China TST 2009 Quiz 6 Problem 3**.

We have just proven a major result. Now we know the polynomials we have defined are indeed integer polynomials. So now you are probably expecting a proof that they are irreducible. Unfortunately, we do not yet have the tools to do this. However, we can perform a special case for the p^{th} cyclotomic polynomial quite easily.

Theorem 2.5. *For p a prime, we have $\Phi_p(x)$ is irreducible.*

Proof. To prove this it suffices to show $\Phi_p(x + 1)$ is irreducible. Note that

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + ... + \binom{p}{p-1}\end{aligned}$$

which is obviously irreducible by Eisenstein's Criterion and thus we are done. □

We finish the section with an interesting result.

Theorem 2.6. *For a positive integer n, write $\Phi_n(x) = \sum_{i=0}^{\varphi(n)} a_i x^i$. Then if $n \geq 2$ we have $a_{\varphi(n)-k} = a_k$ for all $0 \leq k \leq \varphi(n)$.*

Proof. This is essentially showing the polynomial is symmetric. Luckily, this is easy. Remark that the product of two symmetric polynomials is symmetric again. Now observe that $(x - \omega_n^k)(x - \omega_n^{n-k}) = x^2 - (\omega_n^k + \omega_n^{n-k}) + 1$ is symmetric. The result follows by pairing the roots up in conjugate pairs. □

2.3 A Very Interesting Question

Write out the first twenty or so cyclotomic polynomials. You'll notice all of their coefficients are either -1, 0 or 1. Does this hold for all cyclotomic polynomials? Can you prove it? This is left as an exercise to the reader. It is advised the reader reads section 3 first before attempting this, but this question is placed here for the readers who wish to try to unearth many of the interesting properties of cyclotomic polynomials only using the basic proofs given above. The author finds that this question is excellent in guiding one to learn more about the structure of cyclotomic polynomials.

3 Special Properties of Cyclotomic Polynomials

We begin with an easy theorem. Define $\mu(n)$ to be the unique function satisfying $\mu(1) = 1$ and for all $n > 1$ we have $\sum_{d|n} \mu(d) = 0$. On the planetmath page at [1] more can be found about this function.

Theorem 3.1. *For all positive integers n we have $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$*

Proof. This is true by the Moebius Inversion Formula. Basically take the proof in [1] and replace all the sums with products to get the desired result. □

This is a nice result and gives an efficient way to compute cyclotomic polynomials. I frequently use this formula to compute big cyclotomic polynomials. Before deriving some more nice identities, let's explore something interesting.

Theorem 3.2. *For any positive integer n, the sum of the primitive n^{th} roots of unity is $\mu(n)$.*

Proof. Define

$$f(n) = \sum_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} e^{2\pi i k/n}.$$

We will show f is multiplicative. So $f(m)f(n)$ has $\varphi(m)\varphi(n) = \varphi(mn)$ terms. Now suppose two terms are equal so $e^{2\pi i a/n} e^{2\pi i b/m} = e^{2\pi i c/n} e^{2\pi i d/m}$. But then $am+nb \equiv cm+dn \pmod{mn}$, which is absurd so multiplying $f(m)$ with $f(n)$ when $\gcd(m, n) = 1$ results in $\varphi(mn)$ distinct terms. Now why do these terms pop up in $f(mn)$? This is because $\gcd(am + bn, mn) = 1$ obviously when $\gcd(a, n) = \gcd(b, m) = 1$. Thus f is multiplicative.

Now it's easy to show that $f(p) = -1$ and $f(p^k) = 0$, hence $f(n) = \mu(n)$ for all x so we are done. □

Remark. A much shorter proof exists using Moebius Inversion, but I decided this proof in instructive because it displays the beauty of multiplicative functions in number theory.

Thus we can find the coefficient on the $x^{\varphi(n)-1}$ term in $\Phi_n(x)$. To my knowledge no simple formula exists for the terms other than this one, the leading coefficient, the constant one

and the x coefficient. However, I'd be very happy to learn that some other coefficients have a nice formula!

Now we prove a rather useful formula.

Theorem 3.3. *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 $\Phi_{np}(x) = \dfrac{\Phi_n(x^p)}{\Phi_n(x)}$.*

Proof. First let's do the case of $p \nmid n$. This is a simple root counting exercise. Using (2.1) we have the degrees in both sides of $\Phi_{np}(x) = \dfrac{\Phi_n(x^p)}{\Phi_n(x)}$ are equal. Thus it suffices to show every primitive pn^{th} root of unity is a root of the RHS.

Luckily, this is easy. Consider ω_{pn}^k where $\gcd(k, pn) = 1$. Then $(\omega_{pn}^k)^p = \omega_n^k$ and clearly we have $\gcd(k, n) = 1$. Thus it follows quickly that ω_{pn}^k is a root of the RHS and therefore we are done with this case.

The proof for the case of $p \mid n$ is identical so it is omitted. Therefore we are done. □

Corollary 3.4. *If n is an odd integer, we have $\Phi_{2n}(x) = \Phi_n(-x)$.*

The above theorem is very nice and I use this to compute cyclotomic polynomials normally. Note that it is essentially (3.1) in disguise.

Theorem 3.5. *If a, n are positive integers and $\gcd(a, n) = 1$, we have $\Phi_n(x^a) = \prod_{d \mid a} \Phi_{nd}(x)$.*

Proof. This theorem is simply another roots counting problem. Applying (2.1) we can easily prove both sides have equal degree. Thus it suffices to show every a^{th} root of a primitive n^{th} root of unity is a root of the RHS.

So a characterization of the roots on the LHS is ω_{an}^k whenever $\gcd(k, n) = 1$. So take a root ω_{an}^k. Let $g = \gcd(k, a)$. Then ω_{an}^k is a primitive an/g^{th} root of unity. It follows for $d = \frac{a}{g}$ we have ω_{an}^k is a root of $\Phi_{nd}(x)$. It immediately follows both sides are equal so we are done. □

4 A Brief Tangent

Before we get to the most powerful properties of these polynomials, we must first build up a little theory. None of the theorems in this section have complete proofs written here to add additional exercises for the interested reader. These theorems are highly disconnected with cyclotomic polynomials so their proofs won't give much intuition into cyclotomic polynomials. However, their proofs are provided in the appendix.

Write a polynomial as $P(x) = \sum_{k \geq 0} a_k x^k$. Then define the *derivative* of P as:

$$P'(x) = \sum_{k \geq 1} k a_k x^{k-1}$$

The following statements are almost trivial to prove so their proofs are omitted. Proofs can be found in any standard calculus textbook. Note that as the following statements are identities in $\mathbb{R}[x]$, they hold as well in $\mathbb{Z}[x]$ but more importantly in $\mathbb{Z}_p[x]$ which we will be using heavily.

Proposition 4.1. *For any two polynomials f, g we have $(f(x) + g(x))' = f'(x) + g'(x)$.*

Proposition 4.2. *For any two polynomials f, g we have $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.*

Using these propositions, we can prove the following statement. However, it is left as an exercise to the reader as to how to prove it.

Theorem 4.3. *Let P be a polynomial over either $\mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x]$ or $\mathbb{Z}_p[x]$. Then there exists a nonconstant polynomial $m(x)$ such that $m(x)^2 \mid P(x)$ iff $\gcd(P(x), P'(x)) \neq 1$.*

Corollary 4.4. *The polynomial $x^n - 1$ has only roots of multiplicity 1 for all n.*

Remark. This results holds over any finite field or over any UFD with characteristic 0. It's ok if you don't understand what these terms mean, that's fine and this is simply an additional exercise for those with some abstract algebra knowledge.

Note that we already knew this corollary because we know all the roots of $x^n - 1$, but it shows the power of this theorem as we can show there exist no roots of multiplicity greater than 1 without knowing anything about the roots!

5 Order of an Element

5.1 Relations with Cyclotomic Polynomials

Given a prime p, define $\text{ord}_p(a)$ to be the least positive integer k such that $a^k \equiv 1 \pmod{p}$. Now, how come we can connect this with cyclotomic polynomials? That's simple. Remark that $\Phi_n(x)$ has a root at $\alpha \in \mathbb{C}$ iff the "order" of α in $\mathbb{C}$ is n. So does this hold over $\mathbb{Z}_p$? Numerical examples will say this is the case, which motivates the rest of this section. However, before we prove this statement we need a little help.

Proposition 5.1. *Let m, n be two positive integers and p a prime such that $p \nmid mn$. Then $\gcd(\Phi_m(x), \Phi_n(x)) = 1$ over $\mathbb{Z}_p[x]$.*

Proof. By (4.3) applied in $\mathbb{Z}_p[x]$ we have $x^{mn} - 1$ has no repeated factors. Now suppose $\gcd(\Phi_m(x), \Phi_n(x)) = g(x) \neq 1$. Then note that $g(x)^2 \mid (x^{mn} - 1)$, which is absurd so we are done. □

Corollary 5.2. *Let m, n be two positive integers and p a prime such that $p \nmid mn$. Then $\Phi_m(x), \Phi_n(x)$ cannot both be divisible by p for the same value of x.*

The following theorem is perhaps the most important theorem about cyclotomic polynomials.

Theorem 5.3. *Let p be a prime. Then for all positive integers n and integers a such that $\gcd(n,p)=1$ we have $p \mid \Phi_n(a) \iff \text{ord}_p(a)=n$.*

Proof. We proceed by induction. The base case of $n=1$ is trivial since $\Phi_1(x)=x-1$ has a root at $x \equiv 1 \pmod{p}$. Now suppose the hypothesis is true for all $k<n$. It suffices to show it is true for n.

Suppose a satisfies $\Phi_n(a) \equiv 0 \pmod{p}$. Then note that $a^n \equiv 1 \pmod{p}$. Suppose $\text{ord}_p(a)=k \neq n$. Then by the inductive hypothesis we have $\Phi_k(a) \equiv 0 \pmod{p}$. But then $\Phi_n(a) \equiv \Phi_k(a) \equiv 0 \pmod{p}$, a contradiction by (5.2).

Now suppose $\text{ord}_p(a)=n$. Then $a^n-1 \equiv 0 \pmod{p}$ so it follows a is a root of some $\Phi_k(x)$ where $k \mid n$. But then by the inductive hypothesis it cannot be any $k<n$ so it must be n. But then we are done! □

Remark. This result holds over any integral domain.

Corollary 5.4. *There is a primitive root modulo p, i.e. there exists some number a such that $\text{ord}_p(a)=p-1$.*

Proof. (Surprised this corollary has a proof? Its because the proof is nontrivial enough that it requires one.) Take $\Phi_{p-1}(x)$. Remark that $x^{p-1}-1 \equiv (x-1)(x-2)...(x-p+1) \pmod{p}$ so it follows $\Phi_{p-1}(x)$ fully factors into linear polynomials in $\mathbb{Z}_p[x]$. But then this follows it has some root a. By (5.3) $\text{ord}_p(a)=p-1$ so we are done. □

Now we prove a very powerful result. It is extremely useful and simple to use. It relates to the order of an element because it will aid us heavily in proving Zsigmondy's Theorem.

Theorem 5.5. *Let m,n be distinct positive integers and h an integer. Then if*

$$\gcd(\Phi_m(h),\Phi_n(h)) \neq 1$$

then it is a prime power p^z and we have $m/n=p^k$ for some integers z,k.

Proof. Let $\Phi_m(x) \equiv \Phi_n(x) \equiv 0 \pmod{p}$. Write $m=p^a b$ and $n=p^c d$ where b,d are not divisible by p. By (3.3) we have $\Phi_m(x) \equiv \Phi_b(x)^{p^{a-1}(p-1)} \pmod{p}$ and $\Phi_n(x) \equiv \Phi_d(x)^{p^{c-1}(p-1)} \pmod{p}$.

By (5.1) as $p \nmid bd$ we have $b=d$ is forced if both $\Phi_m(x), \Phi_n(x)$ both have a root at $x=h$. The fact that m/n is a power of p immediately follows. Now to prove the gcd is a prime power simply note that m/n is a prime power of every prime factor of their gcd, so the result follows. □

5.2 Proving the Infinitude of Certain Primes

A nice result of cyclotomic polynomials is to prove there are infinitely many primes $1 \pmod{n}$ for all positive integers n.

Proposition 5.6. *If $p \nmid n$ and there is an integer a such that $p \mid \Phi_n(a)$, then $p \equiv 1 \pmod{n}$.*

Proof. This is an immediate consequence of (5.3). By (5.3) we know $\text{ord}_p(a)=n$. But then it follows $n \mid (p-1)$, so $p \equiv 1 \pmod{n}$ and we are done. □

Theorem 5.7. *There are infinitely many primes* $1 \pmod{n}$ *for any positive integer* n*.*

Proof. By a well-known result, given a non-constant integer polynomial $P(x)$ then there exist infinitely many primes p such that there exists an integer a such that $p \mid P(a)$. Applying this on $\Phi_n(x)$ and then applying (5.5) on each of these primes gives the desired result. □

A much more complex theorem is that there are infinitely many primes $a \pmod{n}$ whenever $a^2 \equiv 1 \pmod{n}$. It uses cyclotomic polynomials but utilizes the field of p^2 elements. Can you find it?

6 Zsigmondy's Theorem

This theorem is normally regarded as very difficult to prove and nonelementary. However, with the tool of cyclotomic polynomials we can make mincemeat out of it!

Theorem 6.1 (Zsigmondy's Theorem)**.** *Let* a *and* n *be integers greater than* 1*. There exists a prime divisor* q *of* $a^n - 1$ *such that* q *does not divide* $a^j - 1$ *for all* j*,* $0 < j < n$*, except exactly in the following cases:*

(1) $n = 2, a = 2^s - 1$ *where* $s \geq 2$*, and*

(2) $n = 6, a = 2$*.*

This is not the form which you are probably familiar with that involves $a^n \pm b^n$. I only deal with the case of $a^n - 1$ and leave generalizing it as an exercise to the reader as it turns out the generalization is quite easy.

So first we translate this theorem into a better form. It effectively states for all integers $a, n > 1$ we can find a prime p such that $\text{ord}_p(a) = n$. Given (5.3), we instantly jump to the conclusion that it is a good decision to consider $\Phi_n(a)$. Indeed, this turns out to be the biggest insight needed. From there its simply details.

Proposition 6.2. *Let* $a, n > 1$ *be integers. Suppose all prime factors of* $\Phi_n(a)$ *are divisors of* n*. Then* $\Phi_n(a)$ *is a prime which divides* n*, or* $n = 2$*.*

This proposition seems bizarre. What is the motivation for it? The motivation for it is basically if you play around the concept of the givens in the theorem this is not a hard corollary.

Proof. Take any prime $p \mid \Phi_n(a)$. Clearly $\gcd(p, a) = 1$ because the constant term of $\Phi_n(x)$ is 1. Now, let $k = \text{ord}_p(a)$.

Remark that then by (5.3) we have $p \mid \Phi_k(a)$. By (5.5) we have $n/k = p^t$ for some positive integer t (note this implies $p \mid n$). Now write

$$x^n - 1 = \Phi_n(x) \cdot Q(x).$$

for some polynomial Q. It is easy to see $(x^{n/p} - 1) \mid Q(x)$. By Lifting the Exponent Lemma in [2], we have if p is an odd prime that $v_p(a^n - 1) = v_p(a^{n/p} - 1) + 1$ because clearly $k \mid n/p$

as $\gcd(k,p)=1$ clearly. It immediately follows $v_p(\Phi_n(a))=1$. Now take two distinct primes $p,q \mid n$. Let $n=p^{a_1}k_1=q^{a_2}k_2$ where $k_1=\mathrm{ord}_p(a)$ and $k_2=\mathrm{ord}_q(a)$.

Observe that $\frac{n}{p^{a_1}} \mid p-1$ and $\frac{n}{q^{a_2}} \mid q-1$. But then it follows $q \mid (p-1)$ and $p \mid (q-1)$, implying $q \leq p-1, p \leq q-1$ which is absurd! Thus it follows n has at most one prime factor and it has it with multiplicity 1 if it is odd.

Suppose $2 \mid \Phi_n(a)$. Then clearly $k=1$ so it follows $n=2^t$. But then $\Phi_n(a)=a^{2^{n-1}}+1 \equiv 2 \pmod 4$ whenever $n \neq 2$. Thus when $n \neq 2$ we have $4 \nmid \Phi_n(a)$, thus the result follows. □

Proposition 6.3. *Let $a,n>1$ be integers. Write $n=p^kr$ where $p \nmid r$. Then we have $\Phi_n(a) > (b^{p-2}(b-1))^{\varphi(r)}$ where $b=a^{q^{k-1}}$.*

Proof. By (3.3) we have:

$$\Phi_n(a)=\frac{\Phi_r(b^p)}{\Phi_r(b)}$$

It is easy to show that $\Phi_r(b^p) > (b^p-1)^{\varphi(r)}$ because b^p is at least b^p-1 away from any of the roots of $\Phi_r(x)$. Similarly one can show $\Phi_r(b) < (b+1)^{\varphi(r)}$. It follows that:

$$\Phi_n(a) \geq \left(\frac{b^p-1}{b+1}\right)^{\varphi(r)}$$

Now use $b^p-1 \geq b^{p-2}(b^2-1)$ to get the desired result. □

Remark. This bound may seem unmotivated. It sort of is, but the thing is there are tons of ways to bound $\Phi_n(a)$. This is just a very strong bound that eliminates any small case checking.

Proof of Theorem . It is easy to check the counterexamples fail, so it suffices to prove everything else works. If $n=2$ the theorem is easy to check so assume $n>2$. Then we have by 6.2 that $\Phi_n(a)=p$ for some prime. Write $n=p^kr$. By (5.2) we have:

$$p > (b^{p-2}(b-1))^{\varphi(r)}$$

where $b=a^{q^{k-1}}$. If $p \geq 5$ we have $b^{p-2} > p$ for all integers b so it suffices to take $p=3$. But then $a=2, k=1, r=1$ or 2 is forced. This gives us the case of $n=3$ or $n=6$. $n=3$ clearly works while we assumed we were not in the case of $a=2, n=6$. Thus it follows the theorem holds for a,n so we are done. □

Proving this theorem was hard work. So here is an olympiad problem which is normally hard but this theorem makes trivial:

Mini Exercise: (Japan) Find all of quintuple of positive integers (a,n,p,q,r) such that $a^n-1=(a^p-1)(a^q-1)(a^r-1)$.

7 Irreducibility and its Implications

7.1 Proving the Irreducibility

This proof is famous for being nontrivial. It turns out it is very "simple" and short. However, coming up with these arguments is very difficult. It is highly recommended the reader spend at least a good chunk of time thinking about this before reading the solution.

Theorem 7.1. *The n^{th} cyclotomic polynomial is irreducible over $\mathbb{Z}[x]$.*

Proof. The idea for this proof is fairly simple. We first show that if ζ is a primitive n^{th} root of unity and p is a prime such that $\gcd(p, n) = 1$ then we have ζ^p is a root of the minimum polynomial of ζ.

Let the minimum polynomial for ζ be $f(x)$. Now as $\Phi_n(\zeta) = 0$, we know that $f \mid \Phi_n$ so there exists some polynomial integer polynomial $g(x)$ such that $\Phi_n(x) = f(x) \cdot g(x)$. Suppose for the sake of contradiction ζ^p was not a root of $f(x)$, so $g(\zeta^p) = 0$. Let the minimum polynomial for ζ^p be $h(x)$ so write $g(x) = h(x) \cdot k(x)$.

Then we have $\Phi_n(x^p) = f(x^p) \cdot h(x^p) \cdot k(x^p)$. Remark that $h(x^p)$ has a root of ζ, so it follows $f(x) \mid h(x^p)$. Let $h(x^p) = f(x) \cdot \ell(x)$ so we have $\Phi_n(x^p) = \ell(x) \cdot k(x^p) \cdot f(x) \cdot f(x^p)$. Reducing modulo p:

$$\Phi_n(x)^p \equiv f(x)^{p+1} \cdot k(x)^p \cdot \ell(x) \pmod{p}$$

where here we have used the famous identity that $f(x^p) \equiv f(x)^p \pmod{p}$ for a polynomial f. To prove this identity, it is a simple corollary of that fact that $(a+b)^p \equiv a^p + b^p \pmod{p}$ for polynomials a, b which is true by using the binomial theorem. Now take an irreducible divisor $\pi(x)$ of $f(x)$ in $\mathbb{Z}_p[x]$. Remark that $\pi(x)$ must divide $\Phi_n(x)$ more than once then or else the RHS would only be divisible by $\pi(x)$ p times. However, this is a contradiction by applying (4.3) so our original assumption was incorrect and thus ζ^p is the root of f.

Note a key aspect we have above: we had no restrictions on ζ and almost no restrictions on p. We have enough to show the irreducibility of $\Phi_n(x)$ now! By using the above result we know if p is prime and relatively prime then the minimum polynomial of ω_n has the rook ω_n^p. We can then show for any pq where p, q are not necessarily distinct primes not dividing n we have ω_n^{pq} is a root. By applying induction, we can show all numbers k relatively prime to n we have ω_n^k is a root. But this polynomial is $\Phi_n(x)$. Thus it follows $\Phi_n(x)$ is the minimum polynomial of ω_n, implying it it irreducible and thus we are done. □

7.2 Applications

Unfortunately, there aren't many applications without going into more advanced topics. However, I will attempt to keep the discussion as elementary as possible.

Let's say you have a field R, i.e. a set where addition and multiplication defined over it that satisfy commutativity, associativity and distributivity. In addition, there is 0 and 1 which act as additive/multiplicative identities. Every element has both a (unique) multiplicative and additive inverse except 0 which lacks a multiplicative inverse. There are also things called rings where are the same as above but lack multiplicative inverses, but they are uglier than fields in certain senses so we will stick with fields mostly.

Examples. $\mathbb{Z}_p, \mathbb{Q}, \mathbb{R}, \mathbb{Q}_p, \mathbb{Z}[x]/\pi(x)$ where $\pi(x)$ is an irreducible polynomial over $\mathbb{Z}[x]$. All of these are rings also, while $\mathbb{Z}$ and $\mathbb{Z}[i]$ are rings but not fields.

Now, certain rings are "isomorphic". What does this mean? Two rings R and Q are *isomorphic* if there exists a function $f : R \to Q$ such that $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a) \cdot f(b)$ for all a, b in R. Additionally, f must be bijective. Note that the existence of a function f going from R to Q satisfying those properties also guarantees a function going from Q to R satisfying them as well (just consider f^{-1}). R is isomorphic to Q is normally denoted $R \cong Q$.

Examples. We have $\mathbb{Z}_2 \cong \mathbb{Z}[i]_{1+i}, \mathbb{Z}_5 \cong \mathbb{Z}[i]_{2+i}, \mathbb{Z}[i] \cong \mathbb{Z}[x]_{x^2+1}, \mathbb{Z}_5[x]_{x^2+2} \cong \mathbb{Z}_5[x]_{x^2+3}$.

Now, something we are interested in is the functions from a field to itself which make it isomorphic to itself. These functions are *automorphisms*. Note that the identity function is always trivially an automorphism. Most people are more familiar with the term of *conjugation*. The automorphism mapping from $\mathbb{C}$ to $\mathbb{C}$ that flips the sign of i is an automorphism. If one wishes to learn about automorphisms in depth, one is suggested to study Galois Theory. The author suggests using Artin's *Algebra* to study Galois Theory. However, in this section we will only study them very superficially.

Now, consider the field $\mathbb{Q}[\omega_n]$. One question is why is this even a field? To prove this is rather simple. Using the analog of Bezout's Identity in the rational numbers, we know given relatively prime polynomials P, Q with rational coefficients there exists polynomials with rational coefficients A, B such that $P(x)A(x) + Q(x)B(x) = 1$. Now consider a nonzero element $\alpha = \sum_{k=0}^{\varphi(n)-1} a_k \omega_n^k$ (do you see why we can stop at $\varphi(n) - 1$? Additionally, note that as the minimum polynomial of ω_n has degree $\varphi(n)$ by 7.1 we know $\alpha = 0$ iff $a_0 = a_1 = ... = a_{\varphi(n)-1} = 0$) in $\mathbb{Q}[\omega_n]$. Let $P(x) = \sum_{k=0}^{\varphi(n)-1} a_k x^k$. Then applying Bezout's Identity on $P(x), \Phi_n(x)$ we quickly see that $P(\omega_n)A(\omega_n) = 1$ so it is a field.

Now, note that in the case of $n = 4$ an automorphism in this field is the conjugation we are familiar with because $\omega_4 = i$. Notice that this automorphism permutes the roots of $\Phi_4(x)$. We shall prove that in general an automorphism permutes the roots of an irreducible polynomial.

Theorem 7.2. *Let $\pi(x)$ be an irreducible polynomial over $\mathbb{Q}[x]$ and let its roots be $r_1, r_2, ..., r_n$. Let R be a ring which contains $r_1, r_2, .., r_n$ and f be an arbitrary automorphism over R. Then f permutes the roots of π.*

Proof. First we prove that $f(a) = a$ for any rational number a.

Note that $f(1) = f(1)^2$ implying $f(1) = 0, 1$ because the only roots of $x^2 - x = 0$ are $0, 1$. Let a be the element of R such that $f(a) = 0$. Then note that $f(0 \cdot a) = f(a) \cdot f(0) \implies f(0) = 0$, thus $f(1) = 1$ as f is bijective. But then $f(1+1+...+1) = f(1)+f(1)+...+f(1)$ implying $f(n) = n$ for all positive integer n. Now remark that $1 = f(1) = f(n) \cdot f(1/n)$, implying $f(1/n) = 1/n$ for all positive integers n. But then $f(a/b) = f(a) \cdot f(1/b)$ so $f(a/b) = a/b$ for all positive rationals a/b. Now note that $f(1) = f(-1)^2$, thus $f(-1) = -1$. It

immediately follows $f(n) = n$ for all rationals n. This means that all automorphisms on a ring which contains $\mathbb{Q}$ *fixes* the rationals Now why is this useful? Let $\pi(x) = a_0 + a_1 x + ... + a_n x^n$. Then as $\pi(r_i) = 0$ for all i, we have $f(\pi(r_i)) = 0$. But then:

$$\begin{aligned} 0 &= f(a_0 + a_1 r_i + ... + a_n r_i^n) \\ &= f(a_0) + f(a_1 r_i) + ... + f(a_n r_i^n) \\ &= a_0 + a_1 f(r_i) + a_2 f(r_i)^2 + ... + a_n f(r_i)^n \\ &= \pi(f(r_i)) \end{aligned}$$

Thus $f(r_i) \in \{r_1, r_2, ..., r_n\}$. Combined with the fact f is bijective and the roots of P are distinct (try proving this using (4.3)) the result follows. □

Now, let f be an automorphism over $\mathbb{Q}[\omega_n]$. Note that specifying where ω_n goes defines the automorphism everywhere because every element of $\mathbb{Q}[\omega_n]$ can be written as a linear combination of $1, \omega_n, \omega_n^2, ..., \omega_n^{\varphi(n)-1}$. Hence it suffices there are at most $\varphi(n)$ automorphisms over $\mathbb{Q}[\omega_n]$, and all possible suspects are $\omega_n \mapsto \omega_n^k$ where $\gcd(k, n) = 1$. It is left as an (easy) exercise to the reader that each of these are automorphisms. Now, what is the power of this theorem? Here is an example problem:

Exercise. Let $\zeta_1, \zeta_2, \zeta_3, \zeta_4$ be four primitive n^{th} roots of unity. Find all solutions to

$$\zeta_1 + \zeta_2 + \zeta_3 + \zeta_4 = 1$$

for all values of n.

Solution. Let f_k denote the automorphism over $\mathbb{Q}[\omega_n]$ mapping ω_n to ω_n^k. Let S denote the set of residues modulo n which are relatively prime to n. Then remark that:

$$\begin{aligned} \sum_{k \in S} f_k(LHS) &= \sum_{k \in S} f_k(RHS) \\ 4 \sum_{k \in S} \omega_n^k &= \sum_{k \in S} 1 \\ 4\mu(n) &= \varphi(n) \end{aligned}$$

where we have used (3.2) to simplify the LHS. Now, remark that this forces $\varphi(n) = 4$ and $\mu(n) = 1$. The only solutions to $\varphi(n) = 4$ are $n = 5, 8, 10, 12$. Of these the only one with $\mu(n) = 1$ is $n = 10$. Thus the only solution is $n = 10$ and it is easy to see that $\zeta_1 = \omega_{10}, \zeta_2 = \omega_{10}^3, \zeta_3 = \omega_{10}^7, \zeta_4 = \omega_{10}^9$ is the only solution then so we are done. □

8 Worked Out Problems

This section is to help the reader see how Cyclotomic polynomials can be used to kill olympiad problems.

Problem 1 (British Math Olympiad)**.** Prove that there are no prime numbers in the infinite sequence

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

Solution. Note that $10001 = 73 \cdot 173$. Now I claim that for $n \geq 3$ we have $1 + 10^4 + 10^8 + ... + 10^{4n}$ is not prime (which is clearly equivalent to the problem).

Clearly if $(m+1) \mid (n+1)$ then $(1+10^4+...+10^{4m}) | (1+10^4+...+10^{4n})$. Thus it suffices to take $n+1$ prime. Then $1+10^4+10^8+...+10^{4n} = \Phi_{n+1}(10^4) = \Phi_{n+1}(10) \cdot \Phi_{4n+4}(10)$ (this identity is derived via (3.5)) so it is not prime and thus we are done. □

Remark. This problem did not even really need Cyclotomic polynomials, and can be solved by using various identities. However, the Cyclotomic approach is highly motivated and allows one to quickly solve this.

Problem 2 (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).

Solution. $2^{2^n} + 2^{2^{n-1}} + 1 = \Phi_3(2^{2^{n-1}}) = \prod_{d|2^{n-1}} \Phi_{3d}(2)$ by applying (3.5). Remark that this already gives us n prime factors because we have factored this into n numbers greater than one (use a simple bounding argument to establish greater than one). However, we will prove a stronger result of at least n distinct prime factors.

Note that $\Phi_{3d}(2) > 1$ obviously and $\gcd(\Phi_{3d}(2), \Phi_{3d'}(2)) = 1$ for $d, d' | 2^n$ because by (5.5) their gcd must be a prime power of the same prime d/d' is a prime power of (if it is one). Since d/d' is a power of 2, the gcd must be a power of 2, which is absurd since neither of the expressions are divisible by 2 due to $\Phi_n(x)$ having a constant term of ± 1 for all n. It follows all of those factors in the product are relatively prime, so the expression has at least n prime factors. □

Remark. This problem did not need Cyclotomic polynomials either, but in this case they allow for a quick solve because the expression given in the problem immediately reminds us of $\Phi_3(x^k)$.

Now we approach a problem which requires either Cyclotomic Polynomials or some much trickier approach.

Problem 3. Prove that there exist infinitely many positive integers n such that all prime divisors of $n^2 + n + 1$ are not greater than $\sqrt{n}$.

Solution. Because we only need to show this is true for infinitely many n, we can look at very specific n. We look at perfect powers of $n = k^m$, where $\gcd(m, 3) = 1$. By (3.5) we have $\Phi_a(x^n) = \prod_{d|n} \Phi_{ad}(x)$ when $\gcd(a, n) = 1$.

We notice $n^2 + n + 1 = \Phi_3(k^m)$, thus:

$$n^2 + n + 1 = \prod_{d|m} \Phi_{3d}(k)$$

It is obvious that $(k+1)^{\varphi(3n)} > \Phi_{3n}(k)$ for all n since k is at most $k+1$ away from each primitive $3n^{th}$ root of unity. Thus we seek to show for some k, there exists an m such that $(k+1)^{\varphi(3m)} < k^{m/2}$ and then the result would follow because each term in the product is at most $\sqrt{n}$, implying the existence of no prime divisors greater than $\sqrt{n}$.

As $\frac{\varphi(n)}{n}$ can get arbitrarily close to 0, choose an $n > 1000$ such that $\frac{\varphi(n)}{n} < 0.01$. Then letting $m = n$ we have $(k+1)^{\varphi(3m)} < (k+1)^{2 \cdot 0.01 \cdot m}$. Clearly for some k we have then that $(k+1)^{2 \cdot 0.01 \cdot m} < k^{m/2}$ by making k arbitrarily large, so we are done. □

Remark. This problem almost requires Cyclotomic polynomials, and they lead to a very neat and straightforward solution.

Here is a very difficult to approach problem if knowledge of Cyclotomic Polynomials is minimal. However, with the tools we have developed it is of no trouble.

Problem 4 (Online Math Open)**.** ω is a complex number such that $\omega^{2013} = 1$ and $\omega^m \neq 1$ for $m = 1, 2, \ldots, 2012$. Find the number of ordered pairs of integers (a, b) with $1 \leq a, b \leq 2013$ such that

$$\frac{(1 + \omega + \cdots + \omega^a)(1 + \omega + \cdots + \omega^b)}{3}$$

is the root of some polynomial with integer coefficients and leading coefficient 1. (Such complex numbers are called *algebraic integers*.)

Solution. We start with a lemma.

Lemma 8.1. *Given a positive integer $n > 1$, we have $\Phi_n(1) = 1$ if n is not a prime power and if n is a prime power of p we have $\Phi_n(1) = p$.*

Proof. We proceed by induction. The base case of $n = 1$ is obvious, so now let's suppose the lemma is true for all $k < n$ so it suffices to show it holds for n. Remark that:

$$x^{n-1} + x^{n-2} + ... + 1 = \prod_{\substack{d|n \\ d \neq 1}} \Phi_d(x)$$

Thus by plugging in $x = 1$:

$$n = \prod_{\substack{d|n \\ d \neq 1}} \Phi_d(1)$$

If n is a prime power of p, simply by applying (4.3) it is easy to show $\Phi_n(1) = p$. So WLOG n is not a prime power and factorize it as $n = p_1^{e_1} ... p_m^{e_m}$. Then by looking at $\Phi_{p_i^j}(1)$ for $1 \leq i \leq m$ and $1 \leq j \leq e_i$ we get a product which amounts to n on the RHS via the inductive hypothesis. It immediately follows $\Phi_n(1) = 1$ as desired so we are done. □

Let f_k denote the automorphism that sends ω_{2013} to ω_{2013}^k when $\gcd(k, 2013) = 1$ and let $t = \frac{(1 + \omega + \cdots + \omega^a)(1 + \omega + \cdots + \omega^b)}{3}$. Remark that by considering the field $\mathbb{Q}[\omega]$, the number in the problem lies in this field so by (7.2) we have $f_k(t)$ is a root of the minimum polynomial of t and thus is an algebraic integer. Let S be the set of residues modulo 2013 which are relatively prime to 2013. Remark that $\prod_{k \in S} f_k(t)$ is an algebraic integer (and by some Galois Theory it is in fact a power of the constant term of the minimum polynomial of t, but proving this is not needed for the problem). Thus t is an algebraic integer would force $\prod_{k \in S} f_k(t)$ to be an algebraic integer.

Now, remark that $1-\omega$ is a unit in $\mathbb{Z}[\omega]$ because by applying 8.1 we get $(1-\omega)\cdot d = 1$ for some $d \in \mathbb{Z}[\omega]$. Thus t is an algebraic number iff $\dfrac{(1-\omega^{a+1})(1-\omega^{b+1})}{3}$ is an algebraic integer because multiplying by a unit obviously does not change being an algebraic integer or not. Now remark that

$$\prod_{k\in S} f_k(1-\omega^{a+1}) = \Phi_n(1)^{\varphi(2013)/\varphi(n)} \quad \text{where} \quad n = \frac{2013}{\gcd(2013, a+1)}.$$

Using (8.1), it immediately follows that

$$\prod_{k\in S} f_k\left(\frac{(1-\omega^{a+1})(1-\omega^{b+1})}{3}\right) = \frac{\Phi_n(1)^{\varphi(2013)/\varphi(n)} \cdot \Phi_{n'}(1)^{\varphi(2013)/\varphi(n')}}{3^{1200}}$$

(where $n = \dfrac{2013}{\gcd(2013, a+1)}, n' = \dfrac{2013}{\gcd(2013, b+1)}$) is integral iff

$$\frac{2013}{\gcd(a+1, 2013)} = \frac{2013}{\gcd(b+1, 2013)} = 3$$

or one of the gcd's is 2013 because the denominator of the product becomes 3^{1200} and the only way to expel that is to have both gcd's equal to $\dfrac{2013}{3}$ or one of them 2013 by using above formulas (note that we have already shown the product is rational, and for the product to be an algebraic integer it must be integral then). For these cases the problem obviously holds after a little work of computing the actual expressions so it follows the answer is $2013 \cdot 2 - 1 + 2 \cdot 2 = \boxed{4029}$. □

Remark. The above solution looks somewhat convoluted, as one should not expect such a "weak" method to give a sufficient and necessary condition for the expression to be an algebraic integer. However, using some very deep theory it becomes very motivated but this is out of the scope of this paper. The interested reader can search up on valuations in the ring of algebraic numbers. A shadier (but still valuable in some ways) intuition as to why this should work is that the constant term is the most "vulnerable" to becoming nonintegral when you divide an algebraic integer by an integer, so it is often a good idea to check it.

9 Exercises

Note that these problems are not in order of difficulty.

1. Prove the statements in Section 4.
2. Generalize Zsigmondy's Theorem to $a^n - b^n$ and $a^n + b^n$.
3. Do the problem in Section 2.3.
4. Let $p_1, p_2, ..., p_n$ be distinct odd primes. Prove that $2^{p_1 p_2 \cdots p_n} + 1$ has at least $2^{2^{n-1}}$ divisors.

5. Prove that $\cos\left(\frac{2\pi}{n}\right)$'s irreducible polynomial has degree $\frac{\varphi(n)}{2}$.

6. Let n be a positive integer. Call a k-gon in a plane *balanced* if the weights on the vertices make the figure balance at its center. Suppose we have an n-gon which is balanced.

   a. Suppose $n = p^k$ where p is a prime and k is a positive integer. Characterize all balanced n-gons in a nontrivial manner.

   b. Do a., except for $n = p^a q^b$ where p, q are primes.

7. If you did the problem in 2.3 you'll be frustrated by this. Prove that all integers are the coefficients of some Cyclotomic Polynomial.

8. Find all positive integer triplets (l, m, n) such that $\sin^2\frac{\pi}{n} + \sin^2\frac{\pi}{m} = \sin^2\frac{\pi}{l}$

9. Let p be a prime and write $n = p^a b$ where $p \nmid b$. Prove that $\Phi_n(x)$ factorizes into irreducible polynomials of degree $\text{ord}_b(p)$ in $\mathbb{Z}_p[x]$.

10. Let a be an integer and k a positive integer. Show that there are infinitely many primes $p \equiv 1 \pmod{k}$ such that a is a perfect k^{th} power modulo p.

11. Show that $\mathbb{Q}[\omega_m] \cap \mathbb{Q}[\omega_n] = \mathbb{Q}[\omega_{\gcd(m,n)}]$

12. (IMO) If p is a prime number, show that there is another prime number q such that $n^p - p$ is not a multiple of q for any natural number n.

13. (Kronecker's Theorem) Given a monic polynomial $P(x)$ with integer coefficients all of whose roots have modulus 1, show that $P(x)$'s roots are roots of unity.

14. (Valentine Day Set, reworded) Characterize all monic integer polynomials $P(x)$ such that $P(x)$ divides $P(x^k)$ for a fixed integer k.

15. (Valentine Day Set, reworded) Considering covering the positive integers with disjoint arithmetic progressions. Prove that if one of the progressions used has difference ≥ 60, then at least one of the arithmetic progressions has starting term ≥ 19. Show that furthermore if we change it to > 60 then we can strengthen it to ≥ 21.

10 Appendix

The point of this section is to prove the results in section 4 as well as give hints to the exercises.

10.1 Hints to Exercises

Most of these hints give almost nothing, however take warning that some of them may potentially give away too much and will spoil the problem.

1. The first two propositions are basic sum manipulation. For the last one, take an irreducible divisor $\pi(x)$ of $P(x)$. What happens to it when you take a derivative?

2. Try using $\Phi_n(b/a)$ in some way.

3. The results in section 3 shows it is sufficient to check $\Phi_n(x)$ when n is squarefree. Work from here.

4. Remark that $2^{p_1p_2\cdots p_n}+1 = \Phi_2(2^{p_1p_2\cdots p_n})$. How can we factor this with the theorems we have proven?

5. $\cos\left(\frac{2\pi}{n}\right) = \frac{\omega_n + \omega_n^{-1}}{2}$ will be helpful.

6. This problem requires the notion of a vector space. Let the solution set be our vector space, now what is the minimal spanning set?

7. Let $p_1, ..., p_k$ be distinct odd primes such that $p_1 < p_2 < ... < p_k$. Now try computing $\Phi_{p_1p_2\cdots p_k}(x) \pmod{x^{p_k+1}}$ and put some restrictions on the p_i to get what we want.

8. $\sin^2\frac{\pi}{n}$ is ugly. Put it into something that relates to cyclotomics better.

9. Find a k such that $(x^n-1)|(x^{p^k}-x)$. Then what can you deduce?

10. Is it clear why the k^{th} Cyclotomic Polynomial is relevant?

11. Go play around a little with automorphisms to get the desired result.

12. Clearly $q \equiv 1 \pmod{p}$. What's a good way to generate these primes?

13. What's a natural way to determine if a polynomial's roots are roots of unity?

14. Is it clear why the previous exercise makes this problem relevant to this article?

15. Arithmetic progressions tie into polynomials through what method?

10.2 Proofs of Results in Section 4

Proof of Proposition 4.1: Write $f(x) = \sum_{k\geq 0} a_k x^k$ and $g(x) = \sum_{k\geq 0} b_k x^k$. Then $(f(x)+g(x))' = \sum_{k\geq 1} k(a_k+b_k)x^{k-1} = \sum_{k\geq 1} ka_kx^{k-1} + \sum_{k\geq 1} kb_kx^{k-1} = f'(x)+g'(x)$ so we are done. $\square$

Proof of Proposition 4.2: In the notation of the proof of (4.1), we have

$$f(x) \cdot g(x) = \sum_{k \geq 0} x^k \sum_{i=0}^{k} a_i b_{k-i}.$$

Thus:

$$\begin{aligned}
(f(x) \cdot g(x))' &= (f(x) \cdot g(x))' = \sum_{k \geq 1} k x^{k-1} \sum_{i=0}^{k} a_i b_{k-i} \\
&= (f(x) \cdot g(x))' = \sum_{k \geq 1} x^{k-1} \sum_{i=0}^{k} (i \cdot a_i b_{k-i} + (k-i) \cdot a_i b_{k-i}) \\
&= f'(x) \cdot g(x) + f(x) \cdot g'(x)
\end{aligned}$$

as desired. □

To prove (4.3), first we need a lemma.

Lemma 10.1. *In the sets in* (4.3)*, an irreducible nonconstant polynomial* $\pi(x)$ *cannot have derivative* 0*.*

Proof. For $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ this is obvious because a polynomial has derivative 0 iff it is constant so we are done with those cases.

For $\mathbb{Z}_p[x]$, suppose $f(x) = \sum_{k \geq 0} a_k x^{pk}$ is irreducible and has derivative 0. But then note that $f(x) \equiv \left(\sum_{k \geq 0} a_k x^k \right)^p \pmod{p}$, contradiction so f is not irreducible and we are done. □

Now we can prove the result.

Proof of 4.3. If $m(x)^2 | P(x)$, then $m(x) | P'(x)$ obviously so it suffices to show $\gcd(P(x), P'(x)) \neq 1 \implies P$ has some repeated factor.

Let $\pi(x)$ be an irreducible factor of $\gcd(P(x), P'(x))$. Then write $P(x) = \pi(x) \cdot Q(x)$. Taking the derivative and we get: $P'(x) = \pi(x) \cdot Q'(x) + \pi'(x) \cdot Q(x)$.

Note that $\pi(x)$ must divide thus. Therefore it follows $\pi(x) | \pi'(x) \cdot Q(x)$. As we have $\deg \pi' < \deg \pi$ and by (10.1) $\pi'(x)$ is nonzero so $\pi(x)$ does not divide $\pi'(x)$, thus we need $\pi(x) \mid Q(x)$. But then it is clear that $\pi(x)^2 \mid P(x)$ so we are done. □

References

[1] Michael Slone, Kimberly Lloyd, Pedro Sanchez. "Mobius function."
`http://planetmath.org/encyclopedia/MobiusFunction.html`

[2] Amir Hossein Parvardi. "Lifting the Exponent Lemma."
`http://www.artofproblemsolving.com/Resources/Papers/LTE.pdf`