Elementary Properties of Cyclotomic Polynomials

Yimin Ge
Vienna, Austria

Abstract

Elementary number theoretic properties of cyclotomic polynomials are a topic that has become very popular among olympiad mathematics and the discussions about and around several interesting olympiad problems. The purpose of this note is to give an introductory lesson about this issue and the structure behind it and to present some examples of how this knowledge can be used at olympiad problems.

1 Prerequisites

1.1 The Möbius Inversion

Definition 1. The *Möbius Function* $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is squarefree and } k \text{ is the number of prime divisors of } n \\ 0 & \text{else.} \end{cases}$$

Evidentially, μ is multiplicative, that is, $\mu(mn) = \mu(m)\mu(n)$ for all coprime positive integers m, n.

Theorem 1. *Let n be a positive integer. Then*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \geq 2. \end{cases}$$

Proof. The claim is obvious for $n = 1$.

Suppose that $n \geq 2$. Let T be the product of all prime numbers dividing n, that is,

$$T = \prod_{\substack{p \text{ prime} \\ p|n}} p.$$

Every divisor of n that does not divide T is not square-free and thus drops out of the sum. We hence obtain

$$\sum_{d|n} \mu(d) = \sum_{d|T} \mu(d).$$

Let p be any prime number dividing T. Then

$$\sum_{d|T} = \sum_{d|\frac{T}{p}} \mu(d) + \mu(pd) = \sum_{d|\frac{T}{p}} \mu(d) - \mu(d) = 0. \qquad \square$$

Notice that Theorem 1 also directly follows from the well-known fact that if f is a multiplicative function, then so is

$$F(n) = \sum_{d|n} f(d).$$

Theorem 1 also leads to one of the most important facts of the Möbius function, namely the *Möbius Inverison Formula*:

Theorem 2 (Möbius Inverison Formula)**.** *Suppose that $F, f : \mathbb{Z}^+ \to \mathbb{Z}^+$ are functions so that*

$$F(n) = \sum_{d|n} f(d).$$

Then

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Proof. We have

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{t|\frac{n}{d}} f(t).$$

Every divisor t of n/d is also a divisor n. We thus obtain

$$\sum_{d|n} \mu(d) \sum_{t|\frac{n}{d}} f(t) = \sum_{t|n} f(t) \sum_{\substack{d|n \\ t|\frac{n}{d}}} \mu(d) = \sum_{t|n} f(t) \sum_{d|\frac{n}{t}} \mu(d).$$

Notice that the last step follows from the fact that if d and t are divisors of n then d divides n/t if and only if t divides n/d. By Theorem 1, we however have

$$\sum_{d|\frac{n}{t}} \mu(d) = \begin{cases} 1 & \text{if } t = n \\ 0 & \text{else} \end{cases}$$

so it follows that

$$\sum_{t|n} f(t) \sum_{d|\frac{n}{t}} \mu(d) = f(n). \qquad \square$$

Theorem 2 is closely related to the following theorem which, in rudimentary terms, can be reduced to Theorem 2 by taking the logarithms:

Theorem 3. *Suppose that $F, f : \mathbb{Z}^+ \to \mathbb{Z}^+$ are functions so that*

$$F(n) = \prod_{d|n} f(d).$$

Then

$$f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)}.$$

Proof. The proof of this theorem goes exactly like the proof of Theorem 2 except that every sum is replaced by the product and every multiplication with the μ-function is replaced by its power:

$$\begin{aligned}\prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} &= \prod_{d|n}\left(\prod_{t|\frac{n}{d}} f(t)\right)^{\mu(d)} = \prod_{t|n} f(t)^{\sum_{d|n, t|\frac{n}{d}}\mu(d)} \\ &= \prod_{t|n} f(t)^{\sum_{d|\frac{n}{t}}\mu(d)} = f(n).\end{aligned}$$

□

Example 1. Suppose that φ is the Euler's Totient Function. Then for any positive integer n,

$$n = \sum_{d|n} \varphi(d).^1$$

Then the Möbius Inversion yields

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

1.2 Primitive Roots of Unity

Definition 2. Let n be a positive integer. A complex number ζ is called an *nth root of unity* if

$$\zeta^n = 1.$$

We know from high school mathematics that there are n nth roots of unity which are exactly the numbers

$$e^{\frac{2\pi i}{n}}, e^{\frac{2\pi i}{n}2}, \ldots, e^{\frac{2\pi i}{n}n}.$$

This directly follows from the polar form of complex numbers.

[1] This can be easily verified by considering the fractions $1/n, \ldots, n/n$ when written in lowest terms and observing that for any $d \mid n$ there are exactly $\varphi(d)$ fractions having d as their denominator. Another (rather untypical) proof of this fact is given in section 2.1.

Definition 3. Let n be a positive integer and ζ be an nth root of unity. Then the smallest positive intege k that satisfies $\zeta^k = 1$ is called the *order* of ζ and is denoted by $\mathrm{ord}(\zeta)$.

Lemma 1. *Let n be a positive integer and ζ be an nth root of unity. Then for every integer k, $\zeta^k = 1$ if and only if $\mathrm{ord}(\zeta) \mid k$. In particular, $\mathrm{ord}(\zeta) \mid n$.*

Proof. Let $d = \mathrm{ord}(\zeta)$. If $d \mid k$, then obviously $\zeta^k = 1$. On the other hand, suppose that $\zeta^k = 1$. By the integer division algorithm there exist integers q, r with $0 \leq r \leq d-1$ so that $k = qd + r$. Then

$$1 = \zeta^k = \zeta^{qd+r} = \zeta^r.$$

But $0 \leq r < d$ and d is the smallest positive integer satisfying $\zeta^d = 1$, so $r = 0$. □

Corollary 1. *Let n be a positive integer and ζ be an nth root of unity. Then for any integers k and l, $\zeta^k = \zeta^l$ if and only if $k \equiv l \pmod{\mathrm{ord}(\zeta)}$. In particular, if $1 \leq k, l \leq \mathrm{ord}(\zeta)$, then $\zeta^k = \zeta^l$ if and only if $k = l$.*

Proof. $\zeta^k = \zeta^l$ if and only if $\zeta^{k-l} = 1$. The claim follows now from Lemma 1. □

Definition 4. Let n be a positive integer and ζ be an nth root of unity. Then ζ is called a *primitive nth root of unity* if $\mathrm{ord}(\zeta) = n$.

Notice that if ζ is an nth root of unity and $d = \mathrm{ord}(\zeta)$, then ζ is a primitive dth root of unity.

Lemma 2. *Suppose that ζ is a primitive nth root of unity. Then the set*

$$\{\zeta, \zeta^2, \ldots, \zeta^n\}$$

is the set of all nth roots of unity.

Proof. For every integer k, ζ^k is an nth root of unity since $\zeta^{kn} = 1$. By the definition of a primitive nth root of unity, the numbers

$$\zeta, \ldots, \zeta^n$$

are distinct. But since there only exist n nth roots of unity, the claim follows. □

Since the numbers

$$e^{\frac{2\pi i}{n}}, \ldots, e^{\frac{2\pi i}{n}n} = 1$$

are all distinct, we see that in particular $e^{\frac{2\pi i}{n}}$ is a primitive nth root of unity.

Lemma 3. *Let n, k be positive integers and ζ be a primitive nth root of unity. Then ζ^k is a primitive nth root of unity if and only if $\gcd(k, n) = 1$.*

Proof. Let $d = \mathrm{ord}(\zeta^k)$. Then $\zeta^{kd} = 1$. It follows from Lemma 1 that $n \mid kd$.

If $\gcd(k, n) = 1$, then $n \mid kd$ implies $n \mid d$. But d also divides n, so $d = n$, thus ζ^k is primitive.

If $\gcd(k, n) \neq 1$ then

$$\zeta^{k\frac{n}{\gcd(k,n)}} = 1,$$

so $d < n$. Thus, ζ^k is not primitive. □

Corollary 2. *Let n be a positive integer. Then there exist exactly $\varphi(n)$ primitive nth roots of unity.*

2 Cyclotomic Polynomials

2.1 Definition and Elementary Properties

Definition 5. Let n be a positive integer. Then the *nth cyclotomic polynomial*, denoted as Φ_n, is the (monic) polynomial having exactly the primitive nth root of unity as roots, that is,

$$\Phi_n(X) \equiv \prod_{\substack{\zeta^n=1 \\ \mathrm{ord}(\zeta)=n}} (X-\zeta).$$

Since there are exactly $\varphi(n)$ primitive nth roots of unity, the degree of Φ_n is $\varphi(n)$.

In the following, I will present some elementary properties of cyclotomic polynomials which can also be very useful at competitions.

Theorem 4. *Let n be a positive integer. Then*

$$X^n - 1 \equiv \prod_{d|n} \Phi_d(X).$$

Proof. The roots of $X^n - 1$ are exactly the nth roots of unity. On the other hand, if ζ is an nth root of unity and $d = \mathrm{ord}(\zeta)$, then ζ is a primitive dth root of unity and thus a root of $\Phi_d(X)$. But $d \mid n$, so ζ is a root of the right hand side. It follows that the polynomials on the left and right hand side have the same roots and since they are both monic, they are equal. □

Notice that comparing degrees of the polynomials yields another proof of

$$n = \sum_{d|n} \varphi(d).$$

Lemma 4. *Suppose that $f(X) \equiv X^m + a_{m-1}X^{m-1} + \ldots + a_0$ and $g(X) \equiv X^n + b_{n-1}X^{n-1} + \ldots + b_0$ are polynomials with rational coefficients. If all coefficients of the polynomial $f \cdot g$ are integers, then so are the coefficients of f and g.*

Proof. Let M and N respectively be the smallest positive integers so that all coefficients of $Mf(X)$ and $Ng(X)$ are integers (that is, M and N are the least common multiples of the denominators of $a_0, \ldots, a_{m-1}$ and $b_0, \ldots, b_{n-1}$ respectively, when written in lowest terms). Let $A_i = Ma_i$ (for $i = 0, \ldots, m-1$), $B_j = Nb_j$ (for $j = 0, \ldots, n-1$) and $A_m = M, B_n = N$. Then

$$MNf(X)g(X) \equiv A_m B_n X^{m+n} + \ldots + A_0 B_0.$$

Since $f(X)g(X) \in \mathbb{Z}[X]$, all coefficients of $MNf(X)g(X)$ are divisible by MN.

Suppose that $MN > 1$ and let p be a prime divisor of MN. Then there exists an integer $i \in \{0, \ldots, m\}$ so that $p \nmid A_i$. Indeed, if $p \nmid M$ then $p \nmid A_m$ and if $p \mid M$, then $p \mid A_i$ for all $i \in \{0, \ldots, m\}$ would imply that $A_i/p = (M/p)a_i \in \mathbb{Z}$, yielding a contradiction to the

minimality of M. Similary, there exists an integer $j \in \{0, \ldots, n\}$ so that $p \nmid B_j$. Let I and J be the greatest integers among these numbers i and j respectively. Then the coefficient of X^{I+J} in $MNf(X)g(X)$ is

$$A_I B_J + p \cdot R$$

where R is an integer, so in particular, it is not divisible by p which contradicts the coefficients of $MNf(X)g(X)$ being divisible by MN. □

Corollary 3. *Let n be a positive integer. Then the coefficients of Φ_n are integers, that is, $\Phi_n(X) \in \mathbb{Z}[X]$.*

Proof. The proof goes by induction on n. The statement is true for $n = 1$ since $\Phi_1(X) = X - 1$.

Suppose that the statement is true for all $k < n$. Then from Theorem 4 we obtain

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d \neq n} \Phi_d(X)},$$

so the coefficients of $\Phi_n(X)$ are rational and thus by Lemma 4 integers. □

We can also use the Möbius Inversion to obtain a direct formula for the cyclotomic polynomials:

Theorem 5. *Let n be a positive integer. Then*

$$\Phi_n(X) = \prod_{d|n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

Proof. This immediately follows from the Theorems 3 and 4. □

Lemma 5. *Let p be a prime number and n be a positive integer. Then*

$$\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & \text{if } p \mid n \\ \dfrac{\Phi_n(X^p)}{\Phi_n(X)} & \text{if } p \nmid n. \end{cases}$$

Proof. Suppose first that $p \mid n$. Then

$$\begin{aligned} \Phi_{pn}(X) &= \prod_{d|pn} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} \\ &= \left(\prod_{d|n} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \left(\prod_{\substack{d|pn \\ d \nmid n}} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \\ &= \Phi_n(X^p) \prod_{\substack{d|pn \\ d \nmid n}} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}. \end{aligned}$$

However, $d \mid pn$ and $d \nmid n$ implies that $p^2 \mid d$ (since $p \mid n$), so d is not squarefree and thus $\mu(d) = 0$. Thus,

$$\prod_{\substack{d|pn \\ d\nmid n}} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} = 1$$

and hence, $\Phi_{pn}(X) = \Phi_n(X^p)$.

Suppose now that $p \nmid n$. Then

$$\begin{aligned}
\Phi_{pn}(X) &= \prod_{d|pn} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} \\
&= \left(\prod_{d|n} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \left(\prod_{d|n} \left(X^{\frac{pn}{pd}} - 1\right)^{\mu(pd)}\right) \\
&= \left(\prod_{d|n} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \left(\prod_{d|n} \left(X^{\frac{n}{d}} - 1\right)^{-\mu(d)}\right) \\
&= \frac{\Phi_n(X^p)}{\Phi_n(X)}.
\end{aligned}$$

□

From this we instantly infer

Corollary 4. *Let p be a prime number and n, k be positive integers. Then*

$$\Phi_{p^k n}(X) = \begin{cases} \Phi_n(X^{p^k}) & \text{if } p \mid n \\ \dfrac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})} & \text{if } p \nmid n. \end{cases}$$

Proof. From Lemma 5, we have

$$\Phi_{p^k n}(X) = \Phi_{p^{k-1} n}(X^p) = \ldots = \Phi_{pn}(X^{p^{k-1}}) = \begin{cases} \Phi_n(X^{p^k}) & \text{if } p \mid n \\ \dfrac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})} & \text{if } p \nmid n. \end{cases}$$

□

Lemma 6. *Let p be a prime number. Suppose that the polynomial $X^n - 1$ has a double root modulo p, that is, there exists an integer a and a polynomial $f(X) \in \mathbb{Z}[X]$ so that*

$$X^n - 1 \equiv (X - a)^2 f(X) \pmod{p}.$$

Then $p \mid n$.

Proof. [2] Obviously, $p \nmid a$. Substituting $y = X - a$, we get

$$(y + a)^n - 1 \equiv y^2 f(y + a) \pmod{p}.$$

[2] We can also prove Lemma 6 with calculus modulo p by introducing the familiar rules for computing the derivative (and showing that they are consistent). The fact that a double root of a function is a root of its derivative remains invariant modulo p. The derivative of $X^n - 1$ is nX^{n-1}, so $na^{n-1} \equiv 0 \pmod{p}$. But $p \nmid a$, so $p \mid n$.

Comparing coefficients, we see that the coefficient of y on the right hand side is 0. By the binomial theorem, the coefficient of y on the left hand side is na^{n-1}. It follows that $na^{n-1} \equiv 0 \pmod{p}$. But $p \nmid a$, so $p \mid n$. □

Corollary 5. *Let n be a positive integer, $d < n$ a divisor of n and x an integer. Suppose that p is a common prime divisor of $\Phi_n(x)$ and $\Phi_d(x)$. Then $p \mid n$.*

Proof. By Theorem 4,

$$x^n - 1 = \prod_{t|n} \Phi_t(x),$$

so $x^n - 1$ is divisible by $\Phi_n(x)\Phi_d(x)$. It follows that the polynomial $X^n - 1$ has a double root at $X = x$, so by Lemma 6, $p \mid n$. □

Theorem 6. *Let n be a positive integer and x be any integer. Then every prime divisor p of $\Phi_n(x)$ either satisfies $p \equiv 1 \pmod{n}$ or $p \mid n$.*

Proof. Let p be a prime divisor of $\Phi_n(x)$. Notice that $p \nmid x$ because $p \mid \Phi_n(x) \mid x^n - 1$. Let $k = \mathrm{ord}_n(x)$. Since $p \mid x^n - 1$, we have $x^n \equiv 1 \pmod{p}$, so $k \mid n$.

If $k = n$, then it follows that $n \mid p - 1$, that is, $p \equiv 1 \pmod{n}$ since $x^{p-1} \equiv 1 \pmod{n}$ by Eulers theorem.

Suppose now that $k < n$. Since

$$0 \equiv x^k - 1 = \prod_{d|k} \Phi_d(x) \pmod{p},$$

there exists a divisor d of k so that $p \mid \Phi_d(x)$. But $d \mid k \mid n$ and $d < n$, so it follows from Corollary 5 that $p \mid n$. □

Corollary 6. *Let p be a prime number and x be an integer. Then every prime divisor q of $1 + x + \ldots + x^{p-1}$ either satisfies $q \equiv 1 \pmod{p}$ or $q = p$.*

Proof. Let q be a prime divisor of $1 + x + \ldots + x^{p-1}$. Since

$$1 + x + \ldots + x^{p-1} = \frac{x^p - 1}{x - 1} = \frac{x^p - 1}{\Phi_1(x)},$$

we have $1 + x + \ldots + x^{p-1} = \Phi_p(x)$. It follows from Theorem 6 that $q \equiv 1 \pmod{p}$ or $q \mid p$, that is, $q = p$. □

Lemma 7. *Let a and b be positive integers and x be an integer. Then*

$$\gcd(x^a - 1, x^b - 1) = |x^{\gcd(a,b)} - 1|.$$

Proof. Let $T = \gcd(x^a - 1, x^b - 1)$ and $t = \gcd(a, b)$. Since $x^t - 1 \mid x^a - 1$ and $x^t - 1 \mid x^b - 1$, we have $x^t - 1 \mid T$.

Obviously, $\gcd(x, T) = 1$. Let $d = \mathrm{ord}_T(x)$. Then $T \mid x^d - 1$ and since $x^a \equiv x^b \equiv 1 \pmod{T}$, we have $d \mid a$ and $d \mid b$, so $d \mid t$. Thus $x^d - 1 \mid x^t - 1$, so $T \mid x^t - 1$.

It follows from $x^t - 1 \mid T$ and $T \mid x^t - 1$ that $T = |x^t - 1|$. □

Theorem 7. *Let a and b be positive integers. Suppose that $\gcd(\Phi_a(x), \Phi_b(x)) > 1$ for some integer x. Then a/b is the integral power of a prime number, that is, $a/b = p^k$ for a prime number p and an integer k.*

Proof. Suppose that p is a common prime divisor of $\Phi_a(x)$ and $\Phi_b(x)$. We will show that a/b must be a power of p.

Suppose that $a = p^\alpha A$ and $b = p^\beta B$ where $\alpha, \beta \geq 0$ are integers and A, B are positive integers not divisible by p. We shall show that $A = B$.

Since $p \mid \Phi_a(x) \mid x^a - 1$, we have $p \nmid x$.

We shall first show that $p \mid \Phi_A(x)$. This is trivial if $\alpha = 0$. Otherwise, if $\alpha > 1$, it follows from Corollary 4 that

$$0 \equiv \Phi_a(x) = \frac{\Phi_A(x^{p^\alpha})}{\Phi_A(x^{p^{\alpha-1}})} \pmod{p},$$

so $\Phi_A(x^{p^\alpha}) \equiv 0 \pmod{p}$. But $x^{p^\alpha} \equiv x \cdot x^{p^\alpha - 1}$ and since $p^\alpha - 1$ is divisible by $p-1$, it follows from Eulers theorem that $x^{p^\alpha - 1} \equiv 1 \pmod{p}$ and thus, $x^{p^\alpha} \equiv x \pmod{p}$. Hence,

$$0 \equiv \Phi_A(x^{p^\alpha}) \equiv \Phi_A(x) \pmod{p}.$$

Similary, $p \mid \Phi_B(x)$.

Suppose that $A > B$. Let $t = \gcd(A, B)$. Then $t < A$. We know that $p \mid \Phi_A(x) \mid x^A - 1$ and $p \mid \Phi_B(x) \mid x^B - 1$, so $p \mid \gcd(x^A - 1, x^B - 1)$. But from Lemma 7, it follows that

$$\gcd(x^A - 1, x^B - 1) = |x^t - 1|,$$

so $p \mid x^t - 1$. But

$$0 \equiv x^t - 1 = \prod_{d \mid t} \Phi_d(x) \pmod{p},$$

thus there exists a divisor d of t so that $p \mid \Phi_d(x)$. But $d \mid t \mid A$, $d < A$ and $p \mid \Phi_A(x)$, so by Corollary 5, we have $p \mid A$, a contradiction since we assumed that $p \nmid A$. □

2.2 Applications

A common application of cyclotomic polynomials is the proof of a special case of Dirichlets Theorem.

Theorem 8 (Dirichlet)**.** *Let n be a positive integer. Then there exist infinitely many prime numbers p with $p \equiv 1 \pmod{n}$.*

Proof. We will only deal with $n > 1$ since $n = 1$ is trivial.

Suppose that there exist only finitely many prime numbers p with $p \equiv 1 \pmod{n}$. Let T be the product of these primes and all prime numbers diving n. Obviously $T > 1$. Let k be a sufficiently large positive integer so that $\Phi_n(T^k) > 1$ (since Φ_n is a nonconstant monic polynomial, such a k exists) and let q be a prime divisor of $\Phi_n(T^k)$. Because q divides $T^{kn} - 1$, q does not divide T, so $q \not\equiv 1 \pmod{n}$ and $q \nmid n$, a contradiction to Theorem 6. □

Another nice application is a generalisation of a problem from the IMO Shortlist 2002:

Problem 1 (IMO Shortlist 2002)**.** *Let $p_1, p_2, \ldots, p_n$ be distinct primes greater than 3. Show that $2^{p_1 p_2 \cdots p_n} + 1$ has at least 4^n divisors.*

The official solution comments that using cyclotomic polynomials, it can be shown that $2^{p_1 p_2 \cdots p_n} + 1$ has at least $2^{2^{n-1}}$ divisors (which is much more than 4^n when n is large). We are going to prove this generalisation now.

Problem 2. *Let $p_1, p_2, \ldots, p_n$ be distinct primes greater than 3. Show that $2^{p_1 p_2 \cdots p_n} + 1$ has at least $2^{2^{n-1}}$ divisors.*

Solution. It is sufficient to prove that $2^{p_1 \cdots p_n} + 1$ has at least 2^{n-1} pairwise coprime divisors and hence at least 2^{n-1} distinct prime divisors.

We know that

$$\begin{aligned}(2^{p_1 \cdots p_n} - 1)\,(2^{p_1 \cdots p_n} + 1) = 2^{2p_1 \cdots p_n} - 1 &= \prod_{d \mid 2p_1 \ldots p_n} \Phi_d(2) \\ &= \left(\prod_{d \mid p_1 \ldots p_n} \Phi_d(2) \right) \left(\prod_{d \mid p_1 \ldots p_n} \Phi_{2d}(2) \right) \\ &= (2^{p_1 \cdots p_n} - 1) \left(\prod_{d \mid p_1 \ldots p_n} \Phi_{2d}(2) \right)\end{aligned}$$

and hence,

$$2^{p_1 \cdots p_n} + 1 = \prod_{d \mid p_1 \ldots p_n} \Phi_{2d}(2).$$

From Theorem 7, we know that if $\Phi_a(2)$ and $\Phi_b(2)$ are not coprime, then a/b must be a prime power. We thus have to prove that there exists a set of 2^{n-1} divisors of $p_1 \ldots p_n$ so that no two of them differ by exactly one prime number. But this is obvious because we can take the divisors of $p_1 \ldots p_n$ which have an even number of prime divisors and since there are equally many divisors having an even number of prime divisors and divisors having an odd number of prime divisors, there exist exactly 2^{n-1} of them. □

Problem 3 (IMO Shortlist 2006)**.** *Find all integer solutions of the equation*

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

Solution. The equation is equivalent to

$$1 + x + \ldots + x^6 = (y - 1)(1 + y + \ldots + y^4).$$

We know from Corollary 6 that every prime divisor p of $1 + x + \ldots + x^6$ either satisfies $p = 7$ or $p \equiv 1 \pmod 7$. This implies that every divisor of $1 + x + \ldots + x^6$ is either divisible by

7 or congruent to 1 modulo 7. Thus, $(y-1) \equiv 0 \pmod 7$ or $(y-1) \equiv 1 \pmod 7$, that is, $y \equiv 1 \pmod 7$ or $y \equiv 2 \pmod 7$. If $y \equiv 1 \pmod 7$ then $1+y+\ldots+y^4 \equiv 5 \not\equiv 0,1 \pmod 7$, a contradiction and if $y \equiv 2 \pmod 7$ then $1+y+\ldots+y^4 \equiv 31 \equiv 3 \not\equiv 0,1 \pmod 7$, also a contradiction. Hence, this equation has no integer solutions. □

References

[1] Yves Gallot, *Cyclotomic Polynomials and Prime Numbers*, `http://perso.orange.fr/yves.gallot/papers/cyclotomic.pdf`

[2] Mathlinks, *Cyclotomic Property*, `http://www.mathlinks.ro/Forum/viewtopic.php?t=126566`

[3] Mathlinks, *IMO Shortlist 2002*, `http://www.mathlinks.ro/Forum/viewtopic.php?t=15588`

[4] Mathlinks, *IMO Shortlist 2006, N5*, `http://www.mathlinks.ro/Forum/viewtopic.php?p=780855`