Cyclotomic polynomials

Introduction

1. Polynomials $A(x)$, $B(x)$, $C(x)$, $D(x)$ satisfy the equation

$$A(x^5) + xB(x^5) + x^2C(x^5) = (1 + x + x^2 + x^3 + x^4)D(x) \quad \text{for all } x \in \mathbb{R}.$$

   Find all possible values of $A(1)$.

2. A sequence $a_1, a_2, \ldots, a_n$ is called k-balanced if

$$a_1 + a_{k+1} + \ldots = a_2 + a_{k+2} + \ldots = \ldots = a_k + a_{2k} + \ldots$$

   Suppose the sequence $a_1, a_2, \ldots, a_{50}$ is k-balanced for $k = 3, 5, 7, 11, 13, 17$. Prove that a_i are all zeros.

Definition 1. *A complex number z is called a* **primitive nth root of unity** *if $z^n = 1$ and $z^k \neq 1$ for $k = 1, 2, \ldots, n-1$.*

In other words, z^n is the first power which is equal to 1.

Definition 2. *The n***th cyclotomic polynomial** *is the monic polynomial $\Phi_n(x)$ whose roots are exactly primitive nth roots of unity, that is*

$$\Phi_n(x) = \prod_{\gcd(n,k)=1, 1 \leqslant k \leqslant n} (x - e^{\frac{2\pi k}{n} i})$$

Problems

1. Find all primitive roots of unity (see Definition 1) if a) $n = 1$, b) $n = 2$, c) $n = 3$, d) $n = 4$, e) $n = 6$.
2. Prove that the number of primitive nth roots of unity is $\varphi(n)$.
3. Find cyclotomic polynomials (see Definition 2) $\Phi_1(x)$, $\Phi_2(x)$, $\Phi_3(x)$, $\Phi_4(x)$, $\Phi_6(x)$.
4. Prove that the degree of $\Phi_n(x)$ is even for any $n > 2$.
5. Find the degree of $\Phi_n(x)$.
6. Find $\Phi_p(x)$ if p is a prime number.

7. Prove that for any positive integer n
$$\prod_{d|n} \Phi_d(x) = x^n - 1. \tag{1}$$
Remark. We have also proved that $\sum\limits_{d|n} \varphi(d) = n$.

8. Prove that $\Phi_n(x)$ is a polynomial with integer coefficients.

9. Let $\Phi_n(x) = \sum\limits_{i=0}^{\varphi(n)} a_i x^i$ for $n \geq 2$. Prove that $a_i = a_{\varphi(n)-i}$ for all $0 \leq i \leq \varphi(n)$.

10. Find $\Phi_{81}(x)$.

11. Let $n > 1$ be an odd integer. Prove that $\Phi_{2n}(x) = \Phi_n(-x)$.

12. Polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. Prove that $\Phi_p(x)$ is irreducible over $\mathbb{Z}$ if p is a prime number.

    Remark. Note that $\Phi_n(x)$ can be reducible over $\mathbb{Z}_p$ for some prime numbers p. Give an example.

13. Determine whether there exists a polynomial $P(x)$ with integer coefficients such that $P(x)$ is irreducible over $\mathbb{Z}$, but reducible over $\mathbb{Z}_p$ for any prime p.

14. Prove that $\Phi_n(x) = \prod\limits_{d|n}(x^d - 1)^{\mu(n/d)}$, where μ is the Mobius function, that is
$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \dots p_k \\ 0 & n = p^2 m \end{cases}$$

15. For any positive integer n, the sum of all primitive nth roots of unity is $\mu(n)$.

Closer to number theory

Lemma 1 (Key fact). *Let p be a prime, n a positive integer and a any integer. Suppose*
$$\Phi_n(a) \equiv 0 \pmod{p}.$$
Prove that either

- *p divides n, or*
- *n divides $p - 1$ (moreover, n is the order of a modulo p).*

16. What does Lemma 1 say if $n = 4$?

17. Prove Lemma 1.

18. Let x be an integer and $p > 3$ a prime such that $p \mid x^2 - x + 1$. Prove that $p = 1 \pmod{6}$.

19. Let a and b be integers such that $a^4 + b^4$ is divisible by 1001. Prove that both a and b are divisible by 1001.

20. Let m and n be distinct positive integers and p a prime such that $p \nmid mn$. Then $\Phi_m(a)$ and $\Phi_n(a)$ cannot both be divisible by p for $a \in \mathbb{Z}$.

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

22. Prove that for any prime number p there always exists a primitive root, i.e. there exists a positive integer a such that $a, a^2, \ldots, a^{p-1}$ are all different modulo p. *Hint.* You may use the following identity

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1)) \pmod{p}.$$

23. Prove that for any positive integer n there exist infinitely many primes congruent to 1 modulo n.

24. Let p be a prime number. Prove that there exists a prime number q such that for every integer n, the number $n^p - p$ is not divisible by q.

Homework

1. For any positive integer n, let $\tau(n)$ be the number of positive factors of n (for example, $\tau(5) = 2$, $\tau(6) = 4$) . Prove that

$$\sum_{d \mid n} \tau(n/d)\mu(d) = 1.$$