January Camp - 2020, NT L4
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.

January Camp - 2020, NT L4
Cyclotomic polynomials

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.

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 $\varphi(n)$.

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

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

---

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 1. *We have also proved the formula $\sum_{d|n} \varphi(d) = n$.*

8. Find $\Phi_{81}(x)$.
9. Let $n > 1$ be an odd integer. Prove that $\Phi_{2n}(x) = \Phi_n(-x)$.

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

11. Polynomial $\Phi_n(x)$ is irreducible. Prove this statement if n is a prime number.

12. Let $\Phi_n(x) = \sum_{i=0}^{\varphi(n)} a_i x^i$ for any positive integer $n \geq 2$. Prove that $a_i = a_{\varphi(n)-i}$ for all $0 \leq k \leq \varphi(n)$.

13. Prove that $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$, where μ is the Mobius function, that is

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \dots p_k \\ 0 & n = p^2 m \end{cases}$$

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

Why is all of this in the number theory?

Lemma 1 (Key fact). *Let p be a prime, n a positive integer and a any integer. Suppose*

$$\Phi_n(a) \equiv 0 \pmod{p}.$$

Then either

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

---

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

15. Prove Lemma 1.

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

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

18. Let m and n be two positive integers and p a prime such that $p \nmid mn$. Then $\Phi_m(x)$ and $\Phi_n(x)$ cannot both be divisible by p for the same value of $x \in \mathbb{Z}$.

19. 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.

January Camp - 2020, NT L4
Cyclotomic polynomials II

Previous homework

1. 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.
2. Let $\Phi_n(x) = \sum_{i=0}^{\varphi(n)} a_i x^i$ for $n \geq 2$. Prove that $a_i = a_{\varphi(n)-i}$ for all $0 \leq k \leq \varphi(n)$.

Problems

1. Prove that $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$, where μ is the Mobius function, that is

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \dots p_k \\ 0 & n = p^2 m \end{cases}$$

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

Why is all of this in the number theory?

Lemma 1 (Key fact). *Let p be a prime, n a positive integer and a any integer. Suppose*

$$\Phi_n(a) \equiv 0 \pmod{p}.$$

Then either

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

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

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

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

7. Let m and n be two positive integers and p a prime such that $p \nmid mn$. Then $\Phi_m(x)$ and $\Phi_n(x)$ cannot both be divisible by p for the same value of $x \in \mathbb{Z}$.

8. 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

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