

**Definition.** A real number is transcendental if it is not a root of a non-zero polynomial equation with integer coefficients.

**Definition.** A real number  $x$  is a Liouville number if for every possible integer  $n$ , there exist integers  $p$  and  $q > 1$ , such that  $0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}$ .

1. Prove that a Liouville number is transcendental.
2. Prove that the number  $\sum_{k=1}^{\infty} \frac{1}{(k!)^k}$  is transcendental.

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

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

**Theorem (Möbius Inversion Formula).** Suppose that  $F, H, f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  are functions such that  $F(n) = \sum_{d|n} f(d)$  and  $H(n) = \prod_{d|n} f(d)$ . Then,  $f(n) = \sum_{d|n} \mu(d)F(\frac{n}{d})$  and  $f(n) = \prod_{d|n} H(\frac{n}{d})^{\mu(d)}$ .

3. Prove Möbius Inversion Formula Theorem.

**Definition (Cyclotomic Polynomials).** Let  $\zeta_n$  be the complex number  $e^{\frac{2\pi i}{n}}$ . The  $n^{\text{th}}$  cyclotomic polynomial is

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

**Properties.** 1.  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ .

2.  $\Phi_n(x) \in \mathbb{Z}[x]$ .

3.  $\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$ .

4. Let  $p$  be a prime number and  $n$  be a positive integer. Then,  $\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p), & \text{if } p|n \\ \frac{\Phi_n(x^p)}{\Phi_n(x)}, & \text{if } p \nmid n \end{cases}$

5.  $\Phi_n(x)$  is irreducible in  $\mathbb{Z}[x]$ .

4. Prove Property 1.
5. a) Suppose that  $f(x)$  and  $g(x)$  are monic polynomials with rational coefficients. Then, if  $f \cdot g \in \mathbb{Z}[x]$  then  $f, g \in \mathbb{Z}[x]$ .
- b) Prove Property 2.
6. Prove Property 3.
7. Prove Property 4.
8. a) 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  $f(x) \in \mathbb{Z}[x]$  such that  $x^n - 1 \equiv (x - a)^2 f(x) \pmod{p}$ . Then  $p|n$ .
- b) Let  $n$  be a positive integer,  $d < n$  is a divisor of  $n$  and  $b$  is any integer. Suppose that  $p$  divides  $\Phi_n(b)$  and  $\Phi_d(b)$ , then  $p|n$ .
9. 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  $p|n$ .
10. Let  $a$  and  $b$  be positive integers. Suppose that  $x$  is an integer so that  $\gcd(\Phi_n(x), \Phi_m(x)) > 1$ . Then  $\frac{n}{m} = p^k$  for some prime number  $p$  and integer  $k$ .
11. Let  $n$  be a positive integer. Prove that there exist infinitely many prime numbers  $p$  with  $p \equiv 1 \pmod{n}$ .
12. For any positive integer  $n$  consider the polynomial  $f_n = x^{2n} + x^n + 1$ . Prove that for any positive integer  $m$  there is a positive integer  $n$  such that  $f_n$  has exactly  $m$  irreducible factors in  $\mathbb{Z}[x]$ .